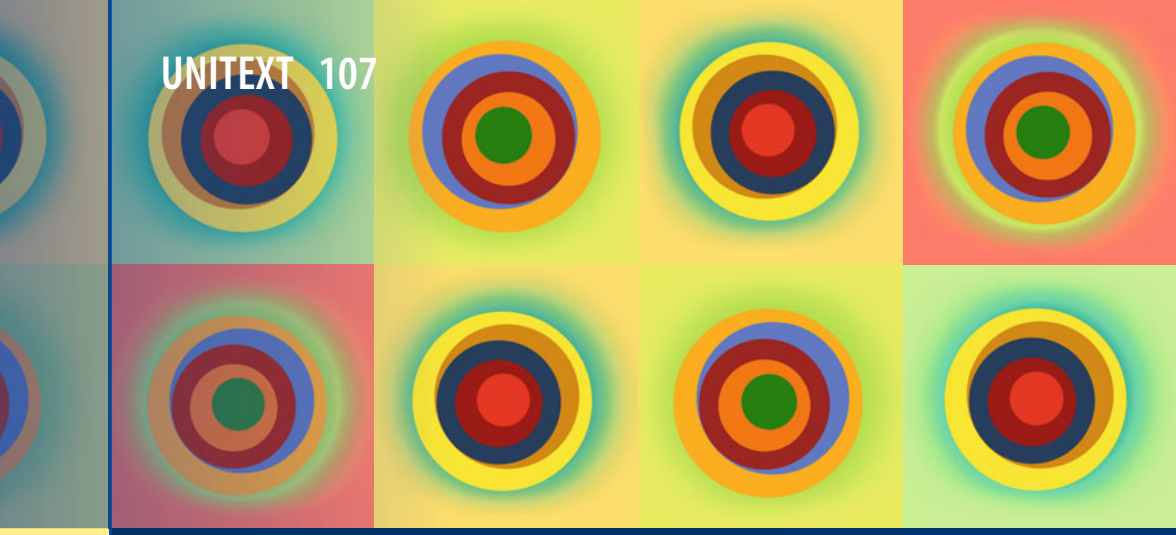


UNITEXT 107

Rocco Chirivì · Ilaria Del Corso
Roberto Dvornicich

Esercizi scelti di Algebra

Volume 1

Springer

UNITEXT – La Matematica per il 3+2

Volume 107

www.springer.com/series/5418

Rocco Chirivì • Ilaria Del Corso •
Roberto Dvornicich

Esercizi scelti di Algebra

Volume 1

Springer

Rocco Chirivì
Dipartimento di Matematica e Fisica
University of Salento
Lecce, Italy

Roberto Dvornicich
Dipartimento di Matematica
University of Pisa
Pisa, Italy

Ilaria Del Corso
Dipartimento di Matematica
University of Pisa
Pisa, Italy

ISSN versione cartacea: 2038-5722
ISSN versione elettronica: 2532-3318
UNITEXT – La Matematica per il 3+2
ISBN 978-88-470-3960-5
ISBN 978-88-470-3961-2 (eBook)
DOI 10.1007/978-88-470-3961-2

Immagine di copertina: "Quadrati, cerchi e simmetrie" di Rocco Chirivì © (2017)

Questa edizione è pubblicata da SpringerNature
La società registrata è Springer-Verlag Italia Srl.

Ad Andrea, che sa cos'è la matematica

Rocco

A Francesca, con l'augurio che sappia scoprire e coltivare le proprie passioni

Ilaria

Ai giovani che già amano o che potrebbero amare la matematica

Roberto

Prefazione

Questo è un libro di esercizi di algebra, comprensivo delle note di teoria necessarie quale riferimento per la soluzione dei testi proposti. È basato sull'esperienza di vari decenni di insegnamento dell'algebra all'Università di Pisa e raccoglie i testi e le relative soluzioni degli esercizi proposti agli esami negli anni.

Un motivo che ci ha portato alla preparazione di questo libro è l'idea che la matematica si possa imparare solo *reinventandola*, e per fare ciò non c'è modo migliore che elaborare le soluzioni degli esercizi. Altro forte impulso al nostro lavoro è stata la convinzione che gli esercizi presentati abbiano delle caratteristiche che li rendono diversi da tutti gli altri. La prima è la non serialità: non esistono esercizi "ripetuti", ossia esercizi che si differenziano fra loro solo per la variazione di alcuni parametri, ma il cui metodo di soluzione è essenzialmente lo stesso. La seconda, e forse fondamentale, è quella che non proponiamo esercizi che si possano affrontare con semplici strumenti di routine: ogni esercizio, per essere risolto, ha bisogno di un'idea.

Chiunque si sia cimentato con la matematica sa come questo cambi completamente, da una parte, il livello di difficoltà di un esercizio, e, dall'altra, il suo interesse intrinseco. Il progresso culturale che deriva dal risolvere un esercizio che richiede delle idee è incomparabilmente superiore a quello della soluzione di un esercizio per cui basta la mera applicazione di tecniche apprese. Abbiamo inoltre l'ambizione di ritenere che le idee necessarie per risolvere i nostri esercizi si differenzino abbastanza nettamente l'una dall'altra, e che questo aspetto sia uno dei motivi di maggiore interesse del libro. Da questo punto di vista, potremmo descrivere il nostro come un libro di *problemi di algebra* piuttosto che un libro di esercizi.

In virtù della storia dell'Università di Pisa, che ha tra i suoi studenti anche quelli della Scuola Normale Superiore, è possibile che gli esercizi proposti in questo libro siano a volte più difficili rispetto alla media degli esercizi proposti nei testi di esame nelle università italiane. Tuttavia, lo scopo di questo libro è di stimolare il ragionamento e preparare gli studenti, nel modo migliore, allo studio dell'algebra. Il nostro consiglio importantissimo ai lettori è quindi: non cadete *mai* nella tentazione di guardare la soluzione senza aver provato abbastanza a lungo a risolvere un esercizio. Studiare una soluzione già pronta, anche se si tratta di una soluzione elegante, non porta ad una vera crescita; come dicevamo sopra, per imparare la matematica

bisogna *fare* la matematica. È infatti la ricerca di una soluzione che arricchisce e fa scoprire i legami fra le cose, legami che sono estremamente importanti nello studio. Inoltre, speriamo in questo modo di incuriosire gli studenti all'approfondimento dei temi tracciati nelle poche righe del testo di un problema.

L'organizzazione del libro segue lo sviluppo storico dell'insegnamento dell'algebra nei primi anni del corso di laurea in matematica dell'Università di Pisa. Dopo un periodo in cui lo studio era concentrato in un corso che si svolgeva interamente il primo anno, con il passaggio alla differenziazione fra laurea triennale e laurea magistrale il corso è stato diviso in due parti, una chiamata Aritmetica e una chiamata, in un primo momento, Strutture Algebriche e successivamente Algebra 1. Esse corrispondono esattamente all'organizzazione di questo libro in due volumi.

La parte di Aritmetica riguarda essenzialmente lo studio di strumenti di base, quali l'induzione, alcuni elementi di calcolo combinatorio, i numeri interi e le congruenze. A ciò segue un'introduzione allo studio delle proprietà basilari delle strutture algebriche: i gruppi abeliani, gli anelli, i polinomi e le loro radici, le estensioni dei campi e i campi finiti. Nel secondo volume, relativo a Strutture Algebriche e Algebra 1, si approfondiscono la teoria dei gruppi, gli anelli commutativi con particolare riferimento alla fattorizzazione unica, le estensioni dei campi e si introducono le nozioni fondamentali della teoria di Galois.

Ciascuna parte è accompagnata da richiami teorici riguardanti la materia oggetto degli esercizi. Tale parte teorica, benché esaustiva non ha comunque la pretesa di sostituire un libro di testo di algebra e, in particolare, i risultati richiamati non hanno dimostrazione. (Per ogni approfondimento il lettore può consultare, ad esempio, il volume "Algebra" di I.N. Herstein, Editori Riuniti, oppure "Algebra" di M. Artin, Bollati Boringhieri.)

Il libro contiene inoltre una serie di esercizi preliminari. Essi dovrebbero essere affrontati per primi in quanto le loro conclusioni sono spesso usate nelle soluzioni degli esercizi successivi. Vogliamo infine sottolineare che tutte le soluzioni qui proposte usano *solo* gli strumenti teorici richiamati e gli esercizi preliminari. L'utilizzo di teoremi più avanzati permetterebbe di risolvere in modo più agevole, o in alcuni casi renderebbe banali, gli esercizi; ma ciò è del tutto contrario allo spirito con cui questo libro è stato scritto.

Ringraziamenti. Vogliamo ringraziare Ciro Ciliberto per il suo sostegno, la dottoressa Francesca Bonadei di Springer Italia per il prezioso aiuto e, in particolar modo, gli studenti che negli anni hanno seguito le nostre lezioni e affrontato gli esercizi qui proposti agli esami.

Aggiornamenti. Invitiamo i lettori a farci avere le loro impressioni e a segnalarci eventuali errori, quasi inevitabili in un libro con dettagliate soluzioni di oltre 250 esercizi, via posta elettronica a `rocco.chirivi@unisalento.it`, `ilaria.delcorso@unipi.it` o `roberto.dvornicich@unipi.it`.

Per aggiornamenti e errata corrige è possibile consultare la pagina web http://www.dmf.unisalento.it/~chirivi/libroEserciziAlgebra.html.

Pisa e Lecce, Italia
giugno 2017

Rocco Chirivì
Ilaria Del Corso
Roberto Dvornicich

The nice thing about mathematics is doing mathematics

Pierre Deligne

Indice

1 Richiami di teoria 1
1.1 Nozioni fondamentali 1
1.1.1 Gli insiemi 1
1.1.2 Le applicazioni 3
1.1.3 Le relazioni 5
1.1.4 Il principio di induzione 7
1.1.5 Le operazioni 8
1.1.6 I numeri 9
1.2 Combinatoria 11
1.3 I numeri interi 15
1.3.1 La divisibilità tra interi 15
1.3.2 Le congruenze 17
1.3.3 L'aritmetica modulare 20
1.4 I gruppi 23
1.4.1 Definizione e prime proprietà 23
1.4.2 Sottogruppi 24
1.4.3 Prodotto di sottogruppi 26
1.4.4 Classi laterali di un sottogruppo 26
1.4.5 Sottogruppi normali 27
1.4.6 Il gruppo simmetrico 29
1.4.7 Omomorfismi di gruppi 29
1.4.8 Prodotto diretto di gruppi 32
1.5 Gli anelli 33
1.5.1 Definizione e prime proprietà 33
1.5.2 Sottoanelli, ideali e quozienti 35
1.5.3 Anelli di polinomi 36
1.5.4 Divisibilità tra polinomi 39
1.5.5 Fattorizzazione di polinomi 40
1.5.6 Quozienti di anelli di polinomi 42
1.6 I campi 44

1.6.1 Caratteristica di un campo 44
1.6.2 Gruppo moltiplicativo 45
1.6.3 Estensioni di campi 45
1.6.4 Campo di spezzamento 48
1.6.5 Campi finiti 49
1.7 Esercizi preliminari 51

2 Esercizi 69
2.1 Successioni 69
2.2 Combinatoria 71
2.3 Congruenze 77
2.4 Gruppi 83
2.5 Anelli e campi 91

3 Soluzioni 97
3.1 Successioni 97
3.2 Combinatoria 103
3.3 Congruenze 130
3.4 Gruppi 166
3.5 Anelli e campi 191

Indice analitico 223

Capitolo 1
Richiami di teoria

1.1 Nozioni fondamentali

1.1.1 Gli insiemi

Il concetto di *insieme* è una nozione primitiva; non tenteremo di definirla e non presenteremo una trattazione assiomatica della teoria degli insiemi. Da un punto di vista ingenuo, che noi adotteremo, un insieme è una collezione di oggetti, i suoi elementi. L'unica proprietà di un insieme X è la possibilità di decidere se un elemento x è o meno appartenente all'insieme X: nel primo caso scriveremo $x \in X$ e diremo che x *appartiene* all'insieme X, se invece x non è un elemento di X scriveremo $x \notin X$, da leggersi x *non appartiene* ad X. In particolare due insiemi X e Y sono *uguali* se e solo se contengono gli stessi elementi. Vi è un solo insieme che non contiene alcun elemento, l'*insieme vuoto*, indicato con $\varnothing$.

Un insieme X è un *sottoinsieme* di un insieme Y se ogni elemento di X è un elemento di Y, in tale caso scriviamo $X \subseteq Y$; con $X \nsubseteq Y$ intendiamo invece che X non è un sottoinsieme di Y. L'insieme vuoto è un sottoinsieme di ogni insieme X, in simboli $\varnothing \subseteq X$, e ovviamente vale anche $X \subseteq X$. La famiglia di tutti i sottoinsiemi di X si indica con $\mathcal{P}(X)$ ed è detta *insieme delle parti* di X; due particolari elementi di $\mathcal{P}(X)$ sono quindi $\varnothing$ e X stesso.

Spesso un sottoinsieme X di un insieme Y è definito per mezzo di una proprietà p; scriveremo

$$X \doteq \{y \in Y \mid p(y)\}$$

per indicare che X è l'insieme di tutti gli elementi di Y per cui la proprietà p è vera.

L'*unione* $X \cup Y$ dei due insiemi X e Y è l'insieme i cui elementi sono tutti e soli gli elementi che appartengono ad X o ad Y: abbiamo cioè

$$x \in X \cup Y \quad \text{se e solo se} \quad x \in X \text{ oppure } x \in Y.$$

Si noti che, a differenza dell'uso nel linguaggio comune della congiunzione "oppure" un elemento dell'unione può appartenere ad entrambi gli insiemi X e Y; l'alternativa è da intendersi quindi nel senso della congiunzione latina *vel*.

R. Chirivì et al., *Esercizi scelti di Algebra, Volume 1*,
UNITEXT – La Matematica per il 3+2 107, DOI 10.1007/978-88-470-3961-2_1

L'*intersezione* $X \cap Y$ è l'insieme che ha per elementi gli elementi che appartengono ad X e ad Y

$$x \in X \cap Y \quad \text{se e solo se} \quad x \in X \text{ e } x \in Y.$$

L'unione e l'intersezione si possono definire per un numero qualsiasi di insiemi: se $\mathcal{F}$ è una famiglia di insiemi allora

$$x \in \bigcup_{X \in \mathcal{F}} X \quad \text{se e solo se} \quad \text{esiste } X \text{ in } \mathcal{F} \text{ per cui } x \in X$$

e allo stesso modo

$$x \in \bigcap_{X \in \mathcal{F}} X \quad \text{se e solo} \quad \text{per ogni } X \text{ in } \mathcal{F} \text{ si ha } x \in X.$$

Proposizione 1.1 *L'unione e l'intersezione sono distributive una rispetto all'altra*: *se X, Y e Z sono tre insiemi allora*

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z) \quad e \quad X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z).$$

Due insiemi X, Y che non hanno alcun elemento in comune, cioè tali che $X \cap Y = \varnothing$, si dicono *disgiunti*. Ogni sottoinsieme X di Y è disgiunto dal suo *complementare* $Y \setminus X$ definito come l'insieme degli elementi di Y che non sono in X. Se X e Y sono insiemi disgiunti allora a volte scriviamo $X \sqcup Y$ per l'unione di X e Y e diciamo che l'unione è *disgiunta*.

Le operazioni sugli insiemi hanno un diretto legame con le operazioni logiche sulle proposizioni come chiarito dalla seguente

Proposizione 1.2 *Se $X = \{z \in Z \mid p(z)\}$ e $Y = \{z \in Z \mid q(z)\}$ sono sottoinsiemi di Z allora*

(i) $X \cup Y = \{z \in Z \mid p(z)\ o\ q(z)\}$,
(ii) $X \cap Y = \{z \in Z \mid p(z)\ e\ q(z)\}$,
(iii) $Z \setminus X = \{z \in Z \mid non\ p(z)\}$,
(iv) $X \subseteq Y$ *se e solo se* p *implica* q.

Proposizione 1.3 *Se X e Y sono sottoinsiemi di un insieme Z allora valgono le Leggi di de Morgan*

$$Z \setminus (X \cup Y) = (Z \setminus X) \cap (Z \setminus Y) \quad e \quad Z \setminus (X \cap Y) = (Z \setminus X) \cup (Z \setminus Y);$$

cioè il passaggio al complementare scambia l'unione con l'intersezione.

L'insieme delle coppie di elementi (x, y) con x in X e y in Y si indica con $X \times Y$ e si chiama *prodotto cartesiano* di X e Y. La stessa costruzione è possibile con un numero qualsiasi di insiemi: $X_1 \times X_2 \times \cdots \times X_n$ è l'insieme delle n–uple ordinate $(x_1, x_2, \ldots, x_n)$ con $x_1 \in X_1$, $x_2 \in X_2$, $\ldots$, $x_n \in X_n$. Indichiamo, per brevità, con X^n il prodotto cartesiano di X con se stesso n volte.

1.1.2 Le applicazioni

Un'*applicazione* da X in Y è una legge che ad ogni elemento di X associa uno e un solo elemento di Y. Ciò può essere formalizzato definendo un'applicazione f da X in Y come un sottoinsieme del prodotto cartesiano $X \times Y$ con la proprietà che per ogni $x \in X$ esiste un unico $y \in Y$ con $(x, y) \in f$; l'insieme X è detto il *dominio* di f e Y è il *codominio* di f. Per indicare che $f \subseteq X \times Y$ è un'applicazione da X in Y scriveremo $f : X \longrightarrow Y$ o anche $X \xrightarrow{f} Y$ e useremo sempre la notazione funzionale scrivendo $f(x) = y$ o $f : x \longmapsto y$ o anche $x \xmapsto{f} y$ invece di $(x, y) \in f$.

Se $f(x) = y$ allora diremo indifferentemente che y è l'*immagine* di x, che f *manda* x in y, che ad x *corrisponde* y e che y *viene raggiunto* da x tramite f. Il sottoinsieme $\mathrm{Im}(f) = \{f(x) \mid x \in X\} \subseteq Y$ degli elementi di Y raggiunti da qualche elemento x di X tramite f è detto *immagine* di f. Osserviamo che dalla definizione segue che due applicazioni f e g sono uguali se hanno lo stesso dominio e codominio e se $f(x) = g(x)$ per ogni x nel dominio.

Se A è un sottoinsieme di X allora $f(A)$, l'*immagine* di A tramite f, è l'insieme degli elementi $f(a)$ al variare di a in A. Se invece B è un sottoinsieme di Y allora $f^{-1}(B)$, la *controimmagine* di B tramite f, è l'insieme degli x in X tali che $f(x) \in B$. L'immagine e la controimmagine godono di alcune compatibilità con l'unione e l'intersezione come chiarito dalla seguente

Proposizione 1.4 *La controimmagine commuta con l'unione e intersezione*

$$f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B), \quad f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$$

mentre l'immagine commuta solo con l'unione

$$f(A \cup B) = f(A) \cup f(B)$$

e vale

$$f(A \cap B) \subseteq f(A) \cap f(B).$$

In generale, però, $f(A \cap B)$ può essere un sottoinsieme proprio di $f(A) \cap f(B)$.

Se $X \xrightarrow{f} Y$ e $Y \xrightarrow{g} Z$ sono due applicazioni, l'applicazione *composta* $g \circ f$ è definita come

$$X \ni x \xmapsto{g \circ f} g(f(x)) \in Z.$$

Proposizione 1.5 *Per la composizione vale la* legge associativa: *se f, g e h sono applicazioni per cui sono definite le composizioni $g \circ f$ e $h \circ g$ allora $h \circ (g \circ f) = (h \circ g) \circ f$.*

Un'applicazione per cui elementi distinti di X corrispondono ad elementi distinti di y è detta *iniettiva*. Per evidenziare che un'applicazione è iniettiva si scrive

$X \hookrightarrow Y$. Un'applicazione per cui ogni y di Y è raggiunto viene detta *suriettiva*; equivalentemente f è suriettiva se $\mathrm{Im}(f) = Y$. Un'applicazione suriettiva si indica con $X \twoheadrightarrow Y$. Se f è iniettiva e suriettiva allora diremo che f è *biiettiva*, ciò è indicato a volte con $f : X \xrightarrow[\sim]{} Y$.

Proposizione 1.6 *La composizione di applicazioni iniettive è iniettiva e la composizione di applicazioni suriettive è suriettiva. In particolare, la composizione di applicazioni biiettive è biiettiva.*

Se X è un sottoinsieme di Y allora è definita l'applicazione *inclusione* $X \ni x \overset{i_X}{\longmapsto} x \in Y$; si tratta chiaramente di un'applicazione iniettiva. In particolare l'inclusione di X in X è detta *identità* e si indica con Id_X, o semplicemente Id quando non vi è ambiguità; essa è un'applicazione biiettiva.

Se X è un sottoinsieme di Y e f è un'applicazione da Y nell'insieme Z, si chiama *restrizione* di f ad X l'applicazione $X \ni x \overset{f_{|X}}{\longmapsto} f(x) \in Z$; chiaramente si ha $f_{|X} = f \circ i_X$.

Se f è un'applicazione da X in Y allora un'*inversa* per f è un'applicazione $Y \xrightarrow{g} X$ tale che $g \circ f = \mathrm{Id}_X$ e $f \circ g = \mathrm{Id}_Y$. Un'applicazione per cui esiste un'inversa è detta *invertibile*. Non tutte le applicazioni ammettono inversa, abbiamo infatti

Proposizione 1.7 *Un'applicazione è invertibile se e solo se è biiettiva. Inoltre, se un'applicazione è invertibile essa ammette un'unica inversa.*

Per un'applicazione invertibile possiamo quindi definire f^{-1} come l'unica inversa di f.

Se $X \xrightarrow{f} X$ è un'applicazione di X in sé indichiamo con X^f l'insieme dei *punti fissi* per f, cioè $X^f = \{x \in X \mid f(x) = x\}$; useremo anche la notazione $\mathrm{Fix}(f)$ per l'insieme dei punti fissi.

Un'applicazione biiettiva di un insieme X in sé è detta *permutazione* e l'insieme di tutte le permutazioni di X è indicato con $\mathsf{S}(X)$. Tale insieme avrà una notevole importanza per il nostro studio dell'Algebra. In generale, l'insieme di tutte le applicazioni $X \longrightarrow Y$ è indicato con Y^X.

Un diagramma di insiemi e applicazioni è detto *commutativo* se tutti i cammini con la stessa partenza e arrivo danno il medesimo risultato per composizione. Ad esempio, il seguente diagramma

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h} \\ A & \xrightarrow{i} & B \end{array}$$

è commutativo se e solo se $(h \circ f)x = (i \circ g)x$ per ogni elemento x in X.

1.1.3 Le relazioni

Sia X un insieme e R un sottoinsieme del prodotto cartesiano $X \times X$, ad R è associata la *relazione* $\sim_R$, o semplicemente $\sim$ se non vi è ambiguità, su X definita come: $x \sim_R y$ se e solo se $(x, y) \in R$. Di fondamentale importanza sono le relazioni di equivalenza: una relazione $\sim$ è di *equivalenza* se valgono le seguenti tre proprietà

(i) proprietà riflessiva: $x \sim x$ per ogni $x \in X$,
(ii) proprietà simmetrica: se $x \sim y$ allora $y \sim x$,
(iii) proprietà transitiva: se $x \sim y$ e $y \sim z$ allora $x \sim z$.

Si osservi che la relazione di uguaglianza è una relazione di equivalenza; può essere utile pensare intuitivamente le relazioni di equivalenza come delle versioni "deboli" dell'uguaglianza. Dato un elemento $x \in X$ si chiama *classe di equivalenza* di x l'insieme $\mathcal{C}\ell(x)$ di tutti gli elementi $y \in X$ con $x \sim y$. Due distinte classi di equivalenza non si intersecano e l'unione di tutte le classi di equivalenza è tutto l'insieme X.

Introduciamo ora un nuovo linguaggio strettamente legato alle relazioni. Una *partizione* di un insieme X è una famiglia $\mathcal{P}$ di sottoinsiemi non vuoti di X con le seguenti proprietà

(i) due distinti insiemi di $\mathcal{P}$ sono disgiunti,
(ii) l'unione di tutti i sottoinsiemi di $\mathcal{P}$ è X.

Vi è una perfetta corrispondenza tra relazioni di equivalenza e partizioni come chiarito dal seguente

Teorema 1.8 *Se $\sim$ è una relazione di equivalenza su X allora la famiglia delle classi di equivalenza per $\sim$ è una partizione di X. Viceversa se $\mathcal{P}$ è una partizione di X allora la relazione definita da*

$$x \sim y \quad \textit{se e solo se} \quad \textit{esiste } C \in \mathcal{P} \textit{ con } x, y \in C$$

è una relazione di equivalenza su X; inoltre $\sim$ ha per classi di equivalenza gli insiemi C della partizione $\mathcal{P}$.

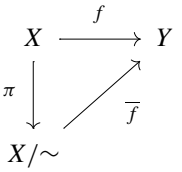
La famiglia delle classi di equivalenza per una relazione è detta *insieme quoziente*, indicato con $X/\sim$, inoltre, l'applicazione

$$X \ni x \overset{\pi}{\longmapsto} \mathcal{C}\ell(x) \in X/\sim$$

che ad un elemento x associa la sua classe di equivalenza è detta *proiezione al quoziente*.

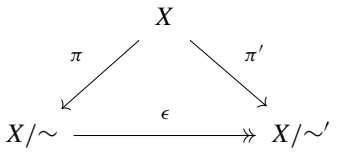
Un'applicazione $X \xrightarrow{f} Y$ è *compatibile* con la relazione di equivalenza $\sim$ su X se $f(x) = f(y)$ ogni volta che $x \sim y$. Se così è, esiste ed è unica un'applicazione $\overline{f}$

per cui $f = \overline{f}\pi$; in altri termini, $\overline{f}$ rende il seguente diagramma



commutativo. Ciò si esprime anche dicendo che f *passa* al quoziente. Definiremo a volte direttamente un'applicazione $\overline{f}$ come $\mathcal{C}\ell(x) \longmapsto f(x)$; in tal caso bisognerà controllare che la definizione sia *ben posta*, cioè che f sia compatibile con $\sim$.

Se abbiamo due relazioni $\sim$ e $\sim'$ su un insieme X e succede che $x \sim y$ implichi $x \sim' y$ allora la partizione $\mathcal{P}$ indotta da $\sim$ è *più fine* della partizione $\mathcal{P}'$ indotta da $\sim'$: cioè per ogni classe $C \in \mathcal{P}$ esiste una classe $C' \in \mathcal{P}'$ tale che $C \subseteq C'$. La corrispondenza $C \longmapsto C'$ è un'applicazione suriettiva ϵ che rende commutativo il diagramma



Un *insieme di rappresentanti* $\mathcal{R}$ per una relazione di equivalenza è un sottoinsieme di X con la proprietà che la proiezione ristretta ad $\mathcal{R}$ è una biiezione con $X/\sim$; abbiamo cioè scelto per ogni classe di equivalenza un rappresentante in X.

Un'altra importante classe di relazioni che useremo spesso è data dalle relazioni d'ordine: una relazione *d'ordine* su un insieme X è una relazione $\leq$ con le seguenti proprietà

(i) proprietà riflessiva: $x \leq x$ per ogni $x \in X$,
(ii) proprietà antisimmetrica: se $x \leq y$ e $y \leq x$ allora $x = y$,
(iii) proprietà transitiva: se $x \leq y$ e $y \leq z$ allora $x \leq z$.

Si noti che non chiediamo che tutti gli elementi di X siano tra loro confrontabili, può infatti essere che $x \leq y$ e $y \leq x$ siano entrambe false. Se invece per ogni coppia di elementi $x, y \in X$ si ha $x \leq y$ o $y \leq x$ allora la relazione si dice d'ordine *totale*. A volte, per evidenziare che una relazione d'ordine può non essere di ordine totale diremo che è una relazione d'ordine *parziale*.

Una relazione d'ordine *stretto* è invece una relazione $<$ su X che verifica le proprietà

(i) proprietà irriflessiva: per nessun $x \in X$ si ha $x < x$,
(ii) proprietà transitiva: se $x < y$ e $y < z$ allora $x < z$.

Ad ogni relazione d'ordine è associata una relazione d'ordine stretto e viceversa. Infatti se $\leq$ è una relazione d'ordine allora definendo $x < y$ se $x \leq y$ e $x \neq y$, abbiamo una relazione d'ordine stretto e, se $<$ è d'ordine stretto allora definendo

$x \leq y$ se $x < y$ o $x = y$, abbiamo una relazione d'ordine. Questa associazione tra $\leq$ e $<$ verrà assunta tacitamente nel seguito.

1.1.4 Il principio di induzione

Indichiamo l'insieme dei numeri naturali $\{0, 1, 2, \ldots\}$ con $\mathbb{N}$; nel seguito assumeremo note le proprietà elementari dei naturali e non daremo una loro definizione assiomatica. Ricordiamo solo che una possibile definizione formale è quella di Giuseppe Peano di cui riportiamo, data la sua fondamentale importanza, solo il quinto assioma detto *Principio d'Induzione*.

Assioma 1.9 (Principio di Induzione) *Sia $p(n)$ una proprietà dipendente da un naturale n tale che*: *$p(0)$ è vera e, per ogni naturale m, si ha che $p(m)$ implica $p(m+1)$. Allora $p(n)$ è vera per ogni n.*

Nell'uso del Principio di Induzione la verifica che $p(0)$ è vera è spesso chiamata *passo base* e la dimostrazione che $p(m)$ implica $p(m+1)$ *passo induttivo*. Il Principio di Induzione può essere enunciato in varie forme equivalenti. Ad esempio

Proposizione 1.10 (Seconda forma del Principio di Induzione) *Sia $p(n)$ una proprietà dipendente da un naturale n tale che*: *$p(0)$ è vera e, per ogni naturale m, si ha che $p(m+1)$ segue da $p(0)$, $p(1)$, $\ldots$, $p(m-1)$, $p(m)$. Allora $p(n)$ è vera per ogni n.*

Con la seconda forma dell'induzione possiamo assumere la verità di $p(0)$, $p(1)$, $\ldots$, $p(m)$ per dimostrare $p(m+1)$ nel passo induttivo.

Un'ulteriore utile forma equivalente è il cosiddetto *Principio del Minimo* o *del Buon Ordinamento*

Proposizione 1.11 (Principio del Minimo) *Se A è un sottoinsieme non vuoto di $\mathbb{N}$ allora A ammette minimo, esiste cioè un elemento $a \in A$ tale che $a \leq b$ per ogni $b \in A$.*

Chiamiamo *successione* in X una applicazione $\mathbb{N} \longrightarrow X$, indichiamo una successione con $(a_n)_n$ invece di $n \longmapsto a_n$.

Vogliamo definire una successione $(a_n)_n$ in X fissando il valore iniziale $a_0 = x \in X$ e imponendo che per ogni n, il termine a_{n+1} si possa ricavare in qualche modo dai termini precedenti $a_0, a_1, \ldots, a_{n-1}, a_n$. Siano quindi $f_n : X^n \longrightarrow X$, con $n \geq 1$, delle applicazioni e richiediamo $a_{n+1} = f_{n+1}(a_0, a_1, \ldots, a_{n-1}, a_n)$ per ogni n. In questa situazione diciamo che la successione $(a_n)_n$ è definita per *ricorsione*. La fondatezza di tale modo di procedere è un'altra forma equivalente del Principio d'Induzione.

Proposizione 1.12 (Principio di Definizione Ricorsiva) *Sia X un insieme, x un elemento di X e supponiamo data, per ogni $n \in \mathbb{N}$, un'applicazione $f_n : X^n \longrightarrow X$. Allora esiste un'unica successione $(a_n)_n$ per cui $a_0 = x$ e $a_{n+1} = f_{n+1}(a_0, a_1, \ldots, a_{n-1}, a_n)$ per ogni $n \in \mathbb{N}$.*

Un esempio di definizione ricorsiva è dato dalla successione $(F_n)_n$ dei *numeri di Fibonacci*: essi sono definiti da $F_0 = 0$, $F_1 = 1$ e, per ogni $n \geq 1$, $F_{n+1} = F_n + F_{n-1}$. I primi elementi di tale successione sono

$$0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots.$$

Questa definizione rientra nello schema della proposizione precedente prendendo $X = \mathbb{N}$, $x = 0$, $f_1(a_0) = 1$ e $f_{n+1}(a_0, a_1, a_2, \ldots, a_n) = a_{n-1} + a_n$ per ogni $n \geq 1$.

1.1.5 Le operazioni

Il principale oggetto del nostro studio dell'algebra sono gli insiemi su cui possono essere definite, in modo naturale, delle operazioni con determinate proprietà. Un'*operazione* su un insieme X è un'applicazione dal prodotto cartesiano $X \times X$ in X. Di solito, per le operazioni non usiamo la notazione funzionale ma, indicata, ad esempio, con $\circ$ un'operazione su X, l'immagine attraverso $\circ$ della coppia (x, y) di elementi X è indicata con $x \circ y$; l'operazione stessa è quindi

$$X \times X \ni (x, y) \overset{\circ}{\longmapsto} x \circ y \in X.$$

Diciamo anche che $x \circ y$ è la *composizione* di x e y mediante l'operazione $\circ$.

L'operazione $\circ$ è detta *associativa* se $(x \circ y) \circ z = x \circ (y \circ z)$ per ogni $x, y, z \in X$. Dati n elementi $x_1, x_2, \ldots, x_n$ di X, se $\circ$ è un'operazione associativa è possibile definire un significato non ambiguo alla composizione $x_1 \circ x_2 \circ \cdots \circ x_n$; infatti possiamo associare tra loro a due a due gli elementi in qualsiasi modo senza cambiare il risultato finale.

Un'operazione $\circ$ è detta *commutativa* se $x \circ y = y \circ x$ per ogni $x, y \in X$. Se un'operazione è commutativa e associativa allora la composizione $x_1 \circ x_2 \circ \cdots \circ x_n$ non dipende dall'ordine degli elementi.

Un *elemento neutro* e per un'operazione $\circ$ è un elemento di X per cui $e \circ x = x \circ e = x$ per ogni $x \in X$. È facile provare che se un elemento neutro esiste allora esso è unico.

Se un'operazione $\circ$ ammette un elemento neutro e allora diciamo che un elemento x ha per *inverso sinistro* un elemento y se $y \circ x = e$. Allo stesso modo un *inverso destro* per x è un elemento y per cui $x \circ y = e$ e, infine, un *inverso* è un inverso sinistro che è contemporaneamente un inverso destro.

Se $\circ$ è un'operazione sull'insieme X e Y è un sottoinsieme di X, allora diciamo che Y è *chiuso* rispetto a $\circ$ se per ogni coppia di elementi y_1, y_2 di Y si ha $y_1 \circ y_2 \in Y$. Se Y è chiuso per $\circ$ allora possiamo *restringere* l'operazione

$\circ$ ad un'operazione di Y definendo $Y \times Y \ni (y_1, y_2) \longmapsto y_1 \circ y_2 \in Y$. Di solito l'operazione ristretta di Y si indica con lo stesso simbolo dell'operazione di X.

Date due operazioni $\circ$ e $+$ su un insieme X diciamo che $\circ$ è *distributiva* rispetto a $+$ se per ogni $x, y, z \in X$ vale: $(x + y) \circ z = (x \circ z) + (y \circ z)$ e $x \circ (y + z) = (x \circ y) + (x \circ z)$.

1.1.6 I numeri

Nel seguito faremo uso di vari insiemi numerici, soprattutto come esempi di strutture algebriche. Essi sono tutti costruiti a partire dai naturali visti nella Sezione 1.1.4. Così, ad esempio, gli interi $\mathbb{Z}$ sono i "naturali con segno" e possono essere definiti come le coppie in $\mathbb{N} \times \mathbb{N}$ modulo la relazione di equivalenza $(n, m) \sim (h, k)$ se $n + k = m + h$; la classe di equivalenza di (n, m) è l'intero $n - m$. L'addizione e la moltiplicazione con i naturali possono essere estese agli interi. Con i naturali possiamo risolvere l'equazione $x + a = b$ se solo se $a \leq b$, con gli interi invece la stessa equazione è sempre risolubile e si ha la soluzione $b - a$.

In modo analogo si costruisce l'insieme $\mathbb{Q}$ dei numeri razionali come $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ modulo la relazione di equivalenza $(n, m) \sim (h, k)$ se $nk = mh$; la classe di equivalenza di (n, m) è il numero razionale n/m. Anche in questo caso possiamo estendere le operazioni di $\mathbb{Z}$. Mentre con gli interi l'equazione $ax = b$ è risolubile se e solo se b è un multiplo di a, con i razionali ciò è sempre possibile se $a \neq 0$ e si ha la soluzione b/a.

Esistono però delle equazioni che non hanno alcuna soluzioni in numeri razionali, ad esempio $x^2 - 2 = 0$; si opera un'ulteriore estensione introducendo i numeri reali. La costruzione dell'insieme $\mathbb{R}$ dei numeri reali è però alquanto più complicata. Benché già i greci ne avessero compreso alcune proprietà con ciò che loro chiamavano "teoria dei rapporti delle lunghezze", solo verso la fine del XIX secolo si arrivò ad una precisa definizione formale. Qui ricordiamo soltanto che si possono seguire varie strade; ad esempio usare le successioni di Cauchy in razionali o le sezioni di Dedekind. In entrambi i casi, si tratta di "completare" $\mathbb{Q}$ aggiungendo quelle quantità che possono essere approssimate con numeri razionali ma che non sono in $\mathbb{Q}$. In $\mathbb{R}$ abbiamo, ad esempio, il numero $\sqrt{2}$ che è una soluzione dell'equazione $x^2 - 2 = 0$ vista prima. Ma non abbiamo ancora finito, infatti l'equazione $x^2 + 1 = 0$ non ha alcuna soluzione in numeri reali; infatti il quadrato di un numero reale è sempre non negativo.

Spendiamo ora qualche parola riguardo al passo successivo, i numeri complessi; essi non presentano nessuna seria difficoltà, una volta che siano stati costruiti i numeri reali. Chiamiamo numero complesso ogni coppia (a, b) di numeri reali; come è tradizione indichiamo la coppia (a, b) con $a + ib$, dove i è un simbolo detto *unità immaginaria*, inoltre a è la *parte reale* e b è la *parte immaginaria*. Definiamo la somma e la moltiplicazione per i numeri complessi come

$$\begin{aligned}(a + ib) + (c + id) &= (a + c) + i(b + d)\\ (a + ib)(c + id) &= (ac - bd) + i(ad + bc).\end{aligned}$$

Considerando i numeri complessi del tipo $a + i \cdot 0$, troviamo subito che i numeri reali sono naturalmente un sottoinsieme dei numeri complessi. È inoltre immediato provare che le operazioni così definite sull'insieme $\mathbb{C}$ dei numeri complessi estendono quelle dei numeri reali. Il motivo per cui abbiamo definito la moltiplicazione tra numeri complessi nel modo appena visto è che ora vale: $i^2 = (0 + i \cdot 1)^2 = -1$; anche -1 ha una radice quadrata. Altrimenti detto, l'equazione $x^2 + 1 = 0$ ha le due soluzione complesse $\pm i$.

Un numero complesso $0 + ib$ viene detto *immaginario puro*. Può risultare utile pensare ai numeri complessi come ai punti di un piano, detto *piano complesso*, in cui l'asse delle ascisse è l'asse dei numeri reali, corrispondente al coefficiente a, e l'asse delle ordinate è l'asse dei numeri immaginari puri, corrispondente al coefficiente b nella scrittura $a + ib$. In questa rappresentazione l'origine degli assi è il numero complesso $0 = 0 + i \cdot 0$, l'elemento neutro per la somma. Quella che abbiamo finora introdotto si chiama *forma algebrica* dei numeri complessi.

Dato un numero complesso $z = a + ib$ chiamiamo $\overline{z} = a - ib$ il *coniugato* di z. Il coniugato di z è il simmetrico di z rispetto alla retta reale. La distanza del punto z dall'origine è $|z| = \sqrt{a^2 + b^2}$ detta *modulo* di z, osserviamo che $|z|^2 = z \cdot \overline{z}$. Da questa identità otteniamo la formula $1/z = \overline{z}/|z|^2$ per l'inverso di un numero complesso non nullo. In particolare, per i numeri complessi di modulo 1, cioè per i punti della circonferenza unitaria nel piano complesso, si ha $z^{-1} = \overline{z}$.

Se $z \neq 0$, indichiamo con θ l'*argomento* di z, cioè l'angolo formato dalla semiretta reale positiva e la congiungente l'origine 0 con il punto z; allora vale

$$z = |z|(\cos\theta + i \sin\theta).$$

Vi è una fondamentale formula che lega l'esponenziale complesso e le funzioni trigonometriche, è la Formula di Eulero

$$e^{i\theta} = \cos\theta + i \sin\theta;$$

usando questa formula possiamo esprimere un numero complesso z nella sua *forma polare*

$$z = |z|e^{i\theta}.$$

Per $z = 0$ l'argomento θ è indefinito, mentre, se $z \neq 0$, la forma polare è unica a meno di multipli di 2π per θ. Si noti come al variare di θ il numero complesso $|z|e^{i\theta}$ si muova sulla circonferenza di centro 0 e raggio $|z|$. In particolare, grazie alla Formula di Eulero, l'applicazione $\theta \longmapsto e^{i\theta}$ parametrizza i punti della circonferenza unitaria.

La forma polare è particolarmente adatta per il calcolo delle potenze di un numero complesso; si ha infatti subito che se $z = |z|e^{i\theta}$ e n è un intero, allora

$$z^n = |z|^n e^{in\theta},$$

o, in altri termini, il modulo di z^n è $|z|^n$ e l'argomento è $n\theta$. Analogamente possiamo calcolare le radici n–esime di z, cioè quei numeri complessi ζ per cui $\zeta^n = z$; esse

sono date da

$$\sqrt[n]{|z|}e^{i\frac{\theta+2k\pi}{n}}, \quad \text{con } k = 0, 1, 2, \ldots, n-1.$$

Si osservi che se $z \neq 0$ abbiamo n radici n–esime distinte. Ponendo $z = 1$, questa formula si specializza al caso, per noi particolarmente interessante, delle *radici n–esime dell'unità*

$$e^{2\pi ik/n} = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \quad \text{con } k = 0, 1, 2, \ldots, n-1.$$

Inoltre, fissando $\zeta_n = e^{2\pi i/n}$, tutte le radici n–esime dell'unità si ottengono come $1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$.

Concludiamo questa breve introduzione ai vari tipi di numeri osservando che ogni equazione

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0,$$

con $a_0, a_1, \ldots, a_{n-1}, a_n$ complessi e $a_n \neq 0$, ha una soluzione in $\mathbb{C}$ se $n > 0$; non c'è più bisogno di estendere l'insieme dei numeri per risolvere le equazioni. In seguito studieremo in dettaglio le equazioni polinomiali, concentrandoci sul meccanismo di estensione tramite soluzioni che in questa sezione abbiamo più volte incontrato in modo informale.

Osserviamo che le usuali operazioni di addizione e moltiplicazione tra interi, razionali, reali e complessi sono associative e commutative, hanno per elementi neutri 0 e 1 rispettivamente, l'inverso dell'intero a rispetto all'addizione è $-a$ e, infine, la moltiplicazione è distributiva rispetto all'addizione.

1.2 Combinatoria

Un insieme X si dice *finito* se ha un numero finito di elementi, tale numero si chiama la *cardinalità* di X e si indica con $|X|$. Se X non è finito allora diremo che è *infinito* e che la sua cardinalità è infinita. Due insiemi hanno la stessa cardinalità finita se e solo se possono essere messi in biiezione tra loro. In particolare, X è finito di cardinalità n se e solo se esiste una biiezione tra $\{1, 2, \ldots, n\}$ e X, possiamo quindi elencare gli elementi di X e scrivere $X = \{x_1, x_2, \ldots, x_n\}$.

È possibile definire la cardinalità in maniera più raffinata, distinguendo tra varie cardinalità per gli insiemi infiniti. Ciò esula però dagli scopi di questo volume; qui ci accontenteremo di distinguere tra insiemi finiti e non.

Una prima osservazione sugli insiemi finiti è la seguente

Osservazione 2.1 *Un'applicazione $X \longrightarrow Y$ tra insiemi finiti della stessa cardinalità è iniettiva se e solo se è suriettiva se e solo se è biiettiva.*

Se $X = \{x_1, x_2, \ldots, x_n\}$ e $Y = \{y_1, y_2, \ldots, y_m\}$ sono due insiemi di cardinalità finita, gli elementi del prodotto cartesiano $X \times Y$ sono (x_i, y_j) con $i = 1, 2, \ldots, n$ e $j = 1, 2, \ldots, m$. Abbiamo cioè

Osservazione 2.2 *Se X e Y sono insiemi finiti allora si ha*

$$|X \times Y| = |X| \cdot |Y|.$$

Se invece uno dei due insiemi è infinito e l'altro è non vuoto, allora anche il prodotto cartesiano è infinito.

Una applicazione $f : X \longrightarrow Y$ con X di cardinalità n è completamente determinata da una n–upla di elementi di Y, esiste cioè una biiezione tra Y^X e Y^n; in particolare

Osservazione 2.3 *Se X e Y sono insiemi finiti non entrambi vuoti allora la cardinalità dell'insieme Y^X di tutte le applicazioni da X in Y è data da*

$$|Y^X| = |Y|^{|X|}.$$

Se invece uno dei due insiemi è infinito e l'altro è non vuoto, allora anche Y^X è infinito.

Ad un sottoinsieme A di X possiamo associare la sua *funzione caratteristica* $\chi_A : X \longrightarrow \{0, 1\}$ definita da $\chi_A(x) = 1$ se $x \in A$ e $\chi_A(x) = 0$ se $x \notin A$. I sottoinsiemi di X sono in biiezione con le loro funzioni caratteristiche e quindi

Osservazione 2.4 *Se X è un insieme finito allora la cardinalità dell'insieme delle parti $\mathcal{P}(X)$ è*

$$|\mathcal{P}(X)| = 2^{|X|},$$

se invece X è infinito allora anche $\mathcal{P}(X)$ è infinito.

Il numero delle applicazioni iniettive da un insieme X di n elementi in un insieme Y di m elementi può essere facilmente contato; basta osservare che un'applicazione iniettiva corrisponde ad una scelta ordinata di n elementi distinti di Y.

Osservazione 2.5 *Sia $|X| = n$ e $|Y| = m$. Se $n > m$ allora non ci sono applicazioni iniettive da X in Y, se invece $n \leq m$ allora il numero delle applicazioni iniettive da X in Y è $m(m-1)(m-2)\cdots(m-n+1)$.*

La conclusione di questa osservazione, per $n > m$, è a volta enunciata come segue

Osservazione 2.6 (Principio dei cassetti) *Se n oggetti sono disposti in m cassetti e $n > m$ allora esiste un cassetto che contiene almeno due oggetti.*

Il *fattoriale* $n!$ di un naturale n è definito per ricorrenza come $0! = 1$ e, per ogni $n \geq 0$, $(n+1)! = (n+1) \cdot n!$ Ovviamente, ciò è equivalente a porre $n! = n \cdot (n-1)\cdots 2 \cdot 1$. Grazie all'Osservazione 2.1, un caso particolare della formula appena vista per le funzioni iniettive è

Osservazione 2.7 *Il numero di permutazioni di un insieme con n elementi è n!*

Come vedremo in seguito, le permutazioni di un insieme di n elementi sono un oggetto fondamentale della teoria dei gruppi; se $X = \{1, 2, \ldots, n\}$ allora l'insieme $\mathsf{S}(X)$ delle permutazioni di X viene indicato semplicemente con S_n. Per quanto abbiamo appena visto $|\mathsf{S}_n| = n!$

L'insieme delle parti $\mathcal{P}(X)$ di un insieme X con n elementi può essere suddiviso in base alla cardinalità dei sottoinsiemi, cioè

$$\mathcal{P}(X) = \bigsqcup_{k=0}^{n} \{A \subseteq X \mid |A| = k\}.$$

Inoltre, da quanto richiamato sopra, possiamo subito ricavare che

Osservazione 2.8 *Se $|X| = n$ e $0 \leq k \leq n$, allora il numero di sottoinsiemi di X di cardinalità k è*

$$\frac{n \cdot (n-1) \cdots (n-k+1)}{k!}.$$

Questa conclusione ha un'importanza fondamentale per la combinatoria; se $n \geq 0$ e $0 \leq k \leq n$ definiamo il *coefficiente binomiale* di posto n, k come

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdots (n-k+1)}{k!} = \frac{n!}{k!(n-k)!}.$$

Si noti che, in particolare, $\binom{n}{0} = 1$, e infatti vi è un solo sottoinsieme con 0 elementi in X, cioè l'insieme vuoto, e $\binom{n}{n} = 1$ e infatti vi è un solo sottoinsieme con n elementi in X, cioè X stesso. È a volte utile estendere il significato del simbolo $\binom{n}{k}$ definendolo come 0 per ogni $k < 0$ e $k > n$.

I coefficienti binomiali soddisfano moltissime relazioni tra loro; due delle principali sono le seguenti

Osservazione 2.9 *Per ogni $n \geq 0$ si ha*

$$\binom{n}{n-k} = \binom{n}{k}$$

e vale anche

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

La seconda di queste relazioni può essere usata come definizione ricorsiva dei coefficienti binomiali dopo aver posto $\binom{0}{0} = 1$ e $\binom{0}{k} = 0$ per ogni $k \neq 0$.

Dalla decomposizione di $\mathcal{P}(X)$ in sottoinsiemi per cardinalità abbiamo l'altra relazione

Osservazione 2.10 *Se n è un naturale allora*

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

È usuale disporre i coefficienti binomiali in un triangolo che ha per righe i vari $\binom{n}{k}$ con n fissato. Le prime sei righe di tale triangolo, detto triangolo di Tartaglia o di Pascal, sono

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}$$

I coefficienti binomiali possono essere usati per sviluppare le potenze di un binomio.

Teorema 2.11 (del Binomio di Newton) *Se a e b sono due numeri e n è un intero non negativo, allora si ha*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

In realtà lo stesso risultato è valido per a e b in un qualsiasi anello commutativo; si veda in seguito nel capitolo sugli anelli.

Dati due sottoinsiemi X_1 e X_2 di un insieme X con $X = X_1 \cup X_2$ allora

$$|X| = |X_1| + |X_2| - |X_1 \cap X_2|,$$

infatti gli elementi di $X_1 \cap X_2$ appartengono ad entrambi i sottoinsiemi e sono quindi contati due volte in $|X_1| + |X_2|$. La formula appena vista è un caso particolare del seguente

Proposizione 2.12 (Principio di inclusione esclusione) *Se X è un insieme finito e $X_1, X_2, \ldots, X_k$ sono suoi sottoinsiemi con $X_1 \cup X_2 \cup \cdots \cup X_k = X$ allora si ha*

$$|X| = \sum (-1)^{h+1} |X_{i_1} \cap X_{i_2} \cap \cdots \cap X_{i_h}|$$

dove la somma è per $h = 1, \ldots, k$ e per tutte le h–uple $(i_1, i_2, \ldots, i_h)$ con $1 \leq i_1 < i_2 < \cdots < i_h \leq n$.

Ad esempio, il caso con $k = 3$ della formula di inclusione esclusione è

$$|X| = |X_1| + |X_2| + |X_3| - |X_1 \cap X_2| - |X_1 \cap X_3| - |X_2 \cap X_3| + |X_1 \cap X_2 \cap X_3|.$$

Se invece assumiamo che $\{X_1, X_2, \ldots, X_k\}$ sia una partizione dell'insieme X allora chiaramente

$$|X| = |X_1| + |X_2| + \cdots + |X_k|.$$

1.3 I numeri interi

1.3.1 La divisibilità tra interi

L'aritmetica degli interi è fondata sulla *Divisione Euclidea*, richiamata nella seguente

Proposizione 3.1 (Divisione Euclidea) *Dati un intero a e un intero positivo m, esistono e sono unici un intero q, detto* quoziente, *e un intero non negativo r, detto* resto, *tali che $a = q \cdot m + r$ e $0 \leq r < m$.*

Se nella Divisione Euclidea succede che $r = 0$ allora $a = q \cdot m$ e scriviamo $m \mid a$: diciamo che a è un *multiplo* di m o che m *divide* a e chiamiamo m un *divisore* di a. Se m invece non divide a scriviamo $m \nmid a$. Solo ± 1 dividono 1 mentre ogni intero non nullo è un divisore di 0.

Se a e b sono due interi non entrambi nulli chiamiamo *massimo comun divisore* di a e b un intero positivo m tale che: m è un divisore di a e di b e, se n è un altro divisore comune di a e b, allora n divide m. È grazie alla Divisione Euclidea che possiamo dimostrare

Proposizione 3.2 *Il massimo comun divisore m di due interi non entrambi nulli esiste ed è unico. Inoltre esistono due interi x e y per cui $m = xa + yb$; tale identità è detta Identità di Bezout.*

Nel seguito scriveremo (a, b) per indicare il massimo comun divisore di a e b. Osserviamo che $(a, b) = (|a|, |b|)$, possiamo cioè sempre ricondurci a due interi non negativi. Per il calcolo del massimo comun divisore si può utilizzare

Proposizione 3.3 (Algoritmo di Euclide) *Supponiamo che a e b siano interi non negativi con $a \geq b$ e poniamo $r_0 = a$, $r_1 = b$. Se, per $k \geq 1$, $r_k > 0$ allora definiamo ricorsivamente r_{k+1} come il resto della divisione di r_{k-1} per r_k. Visto che $r_0 > r_1 > r_2 > \cdots \geq 0$, in un numero finito di passi, diciamo n, avremo $r_n = 0$. Risulterà allora $(a, b) = r_{n-1}$.*

Questo algoritmo può essere usato per calcolare esplicitamente una soluzione (x, y) dell'Identità di Bezout; basta infatti sostituire le espressioni che definiscono i resti r_k in termini dei resti precedenti fino a giungere alla prima equazione $a = qb + r_1$ per ottenere un'identità contenente solo a, b e l'ultimo resto non nullo $r_{n-1} = (a, b)$.

Due numeri interi si dicono *primi tra loro* se succede che $(a, b) = 1$; ciò vale se e solo se esistono due interi x, y per cui $xa + yb = 1$.

Osservazione 3.4 (Lemma di Euclide) *Se m divide il prodotto di interi $a \cdot b$ e m è primo con a allora m divide b.*

Con il Lemma di Euclide possiamo facilmente trovare tutte le soluzioni dell'Identità di Bezout

Proposizione 3.5 *Siano a, b due interi non entrambi nulli, sia m il loro massimo comun divisore e sia (x_0, y_0) una soluzione dell'Identità di Bezout per a, b. Allora tutte le coppie di interi per cui vale l'Identità di Bezout sono date da*

$$\left(x_0 + k\frac{b}{m}, y_0 - k\frac{a}{m}\right), \quad k \in \mathbb{Z}.$$

Chiamiamo *equazione diofantea lineare* nelle due variabili intere x e y un'equazione del tipo $ax + by = c$ con a, b e c coefficienti interi. In generale ogni equazione con coefficienti interi di cui si cercano le soluzioni intere si chiama equazione diofantea. La soluzione di questo tipo di equazioni è ben diversa dalla soluzione in numeri reali ed è, di solito, molto difficile. Non è lontana dal vero l'affermazione che la matematica attuale è in grado di risolvere solo le equazioni diofantee lineari e quadratiche; già le equazioni cubiche fanno parte dell'intrigato e affascinante mondo in cui vivono anche le curve ellittiche.

Nell'Esercizio Preliminare 7, per il caso di equazioni lineari si utilizza l'Identità di Bezout per provare

Proposizione 3.6 *L'equazione diofantea $ax + by = c$ ha soluzione se e solo se il massimo comun divisore $m = (a, b)$ divide il termine noto c. In tal caso, detta (x_0, y_0) una soluzione, tutte le soluzioni sono date da*

$$\left(x_0 + k\frac{b}{m}, y_0 - k\frac{a}{m}\right), \quad k \in \mathbb{Z}.$$

Vediamo ora la definizione fondamentale dell'aritmetica degli interi. Un numero intero positivo p è detto *primo* se ha solo i due distinti divisori positivi 1 e p. Si noti che 1 non è quindi un numero primo. Se n è un intero allora il massimo comun divisore (p, n) può essere solo p, nel caso p divida n, o 1, nel caso p non divida n. Da ciò segue subito

Osservazione 3.7 *Se un primo p divide il prodotto $a \cdot b$ e p non divide a allora p divide b.*

È un classico risultato dell'aritmetica greca che ogni intero si fattorizzi in primi in modo essenzialmente unico, vale cioè

Teorema 3.8 (Fondamentale dell'Aritmetica) *Se n è un intero positivo allora esistono, unici a meno dell'ordine, numeri primi $p_1, p_2, \ldots, p_r$ tali che $n = p_1 p_2 \cdots p_r$.*

Se p è un primo e n è un intero, diciamo che una potenza p^e *divide esattamente* n se p^e divide n e p^{e+1} non divide n. In altre parole, p^e divide esattamente n se e solo se il primo p appare nella fattorizzazione di n con esponente e.

Dati due interi non entrambi nulli a e b definiamo il loro *minimo comune multiplo*, indicato con $[a, b]$, come un multiplo comune positivo che è diviso da ogni altro multiplo comune. Analogamente al massimo comun divisore, il minimo comune multiplo esiste ed è unico; vale inoltre $(a, b)[a, b] = ab$. La definizione di minimo comune multiplo è duale a quella di massimo comune divisore; così, spesso, le loro proprietà sono simili.

1.3.2 Le congruenze

Nel suo libro "Disquisitiones Arithmeticae" del 1801, Carl Friedrich Gauss introdusse quella che si è dimostrata essere una della più importanti relazioni tra numeri interi per l'aritmetica elementare: diciamo che l'intero a è *congruo* all'intero b modulo n, e scriviamo $a \equiv b \pmod{n}$, se $a - b$ è un multiplo di n. È facile provare che la relazione di congruenza è una relazione di equivalenza.

La classe di equivalenza dell'intero a, cioè l'insieme di tutti gli interi congrui ad a, è indicata con $[a]_n$ ed è chiaramente l'insieme $\{a + kn \mid k \in \mathbb{Z}\}$. In altri termini, $[a]_n$ è l'insieme degli interi che hanno lo stesso resto di a quando divisi per n. Se il modulo n è chiaro dal contesto, indicheremo la classe $[a]_n$ anche con $\overline{a}$.

Come per tutte le relazioni di equivalenza, le classi di congruenza modulo n formano una partizione di $\mathbb{Z}$. Come insieme di rappresentanti possiamo prendere $\{0, 1, 2, \ldots, n-1\}$, essi saranno detti *residui modulo* n; in particolare le classi di equivalenza sono in numero di n. Ovviamente, qualsiasi insieme di n interi che hanno resti distinti quando divisi per n, è un sistema di rappresentanti per le classi di congruenza modulo n. Si noti che n interi consecutivi formano sempre un sistema di rappresentanti.

L'insieme quoziente di $\mathbb{Z}$ per la relazione di congruenza modulo n è indicato con $\mathbb{Z}/n\mathbb{Z}$. Vedremo in seguito, quando studieremo i gruppi, il perché di questa particolare notazione, per ora essa ci ricorda che nel quoziente "identifichiamo" tra di loro gli interi che differiscono per un multiplo di n, cioè per un elemento di $n\mathbb{Z}$.

Vediamo alcune proprietà della congruenza modulo n.

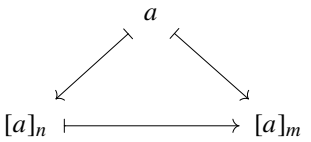
Proposizione 3.9 *Siano a e b due interi con $a \equiv b \pmod{n}$. Allora valgono*
(i) $(a, n) = (b, n)$,
(ii) *se $m \mid n$ allora $a \equiv b \pmod{m}$,*
(iii) *se si ha anche $a \equiv b \pmod{m}$ allora $a \equiv b \pmod{[n, m]}$,*

Un modo equivalente di enunciare la seconda proprietà è: se n è un multiplo di m allora le classi di congruenza modulo n sono una partizione più fine delle classi

di congruenza modulo m. Infatti

$$[a]_m = \bigsqcup_{h=0,1,\ldots,\frac{n}{m}-1} [a+mh]_n.$$

Osserviamo quindi che se n è un multiplo di m è definita una mappa $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ che manda la classe $[a]_n$ in $[a]_m$, essa rende commutativo il diagramma



come già osservato nella sezione sulle relazioni.

La relazione di congruenza modulo n è compatibile con l'addizione e la moltiplicazione di interi.

Proposizione 3.10 *Se a, b, a' e b' sono quattro interi e vale $a \equiv b \pmod{n}$, $a' \equiv b' \pmod{n}$ allora $a + a' \equiv b + b' \pmod{n}$ e $a \cdot a' \equiv b \cdot b' \pmod{n}$.*

In particolare, se $a \equiv b \pmod{n}$ e k è un intero, allora $ka \equiv kb \pmod{n}$. Osserviamo esplicitamente che l'inverso di quanto appena notato è in generale falso: $2 \cdot 2 \equiv 2 \cdot 0 \pmod{4}$ mentre $2 \not\equiv 0 \pmod{4}$. Un parziale inverso è

Proposizione 3.11 *Se a, b e k sono interi e $k \neq 0$ allora*

$$ka \equiv kb \pmod{n} \quad \textit{implica} \quad a \equiv b \quad \left(\textit{mod } \frac{n}{(n,k)}\right).$$

In particolare, se il fattore k è primo con il modulo n, allora

$$ka \equiv kb \pmod{n} \quad \textit{se e solo se} \quad a \equiv b \pmod{n}.$$

Quindi, continuando l'esempio di prima, da $2 \cdot 2 \equiv 2 \cdot 0 \pmod{4}$ ricaviamo correttamente $2 \equiv 0 \pmod{2}$ visto che $4/(4,2) = 2$.

Quanto richiamato finora, benché elementare, ha delle applicazioni già non del tutto ovvie all'aritmetica. Per esempio, usando la rappresentazione in base 10 di un intero e come modulo 3 è possibile ricavare il ben noto criterio di divisibilità per 3, basta infatti osservare che $10 \equiv 1 \pmod{3}$. Allo stesso modo si ricavano i criteri per 2, 4, 5, 9, 11 e 25; è anche possibile ottenere criteri, sempre più complicati, per 7 e per 13.

Un primo risultato non banale sulle classi di resto modulo un primo è il seguente

Teorema 3.12 (del Binomio Ingenuo) *Se p è un numero primo allora, per ogni coppia di interi a e b vale*

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

La dimostrazione di questo teorema segue facilmente una volta osservato che i coefficienti binomiali $\binom{p}{h}$ con p primo e $1 \leq h \leq p-1$ sono tutti divisibili per p.

Usando il Teorema del Binomio Ingenuo è possibile provare per induzione

Teorema 3.13 (di Fermat) *Se p è un numero primo allora*

$$a^p \equiv a \pmod{p}$$

per ogni intero a.

Abbiamo, come facile corollario di questo teorema, uno dei primi risultati non banali sui numeri primi della storia della matematica dopo Euclide

Corollario 3.14 (Piccolo Teorema di Fermat) *Se p è un primo e a è un intero primo con p, allora $a^{p-1} \equiv 1 \pmod{p}$.*

La soluzione di una congruenza lineare, cioè di un'equazione in x del tipo $ax \equiv b \pmod{n}$ con a e b interi, si riconduce immediatamente all'equazione diofantea lineare $ax + ny = b$ in x e y. Da ciò si ricava subito

Proposizione 3.15 *La congruenza lineare $ax \equiv b \pmod{n}$ ha soluzione se e solo se $m = (a, n)$ divide b. In tal caso, detta x_0 una soluzione, tutte le soluzioni sono date da*

$$\left[x_0 + k\frac{n}{m}\right]_n \quad per \quad k = 0, 1, \ldots, m-1;$$

in particolare vi sono m soluzioni modulo n.

Per la soluzioni dei sistemi di equazioni lineari è fondamentale il seguente teorema

Teorema 3.16 (Cinese dei Resti) *Se $n_1, n_2, \ldots, n_r$ sono r interi non nulli a due a due primi tra loro e $a_1, a_2, \ldots, a_r$ sono interi, allora il sistema di congruenze*

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \quad \vdots \\ x \equiv a_r \pmod{n_r} \end{cases}$$

ha una e una sola soluzione modulo $n_1 n_2 \cdots n_r$.

Alla fine della prossima sezione vedremo come calcolare una soluzione di un sistema lineare di congruenze come nel teorema appena visto.

1.3.3 L'aritmetica modulare

Le proprietà di compatibilità della relazione di congruenza modulo un intero non nullo n viste nella sezione precedente ci permettono di definire due operazioni sull'insieme quoziente $\mathbb{Z}/n\mathbb{Z}$ delle classi di resto modulo n.

Definiamo l'addizione $+$ e la moltiplicazione $\cdot$ delle due classi di resto $[a]_n$ e $[b]_n$ come

$$[a]_n + [b]_n = [a+b]_n \qquad [a]_n \cdot [b]_n = [ab]_n.$$

Queste definizioni sono ben poste: esse non dipendono dai rappresentanti a e b in $\mathbb{Z}$ scelti per le classi $[a]_n$ e $[b]_n$ ma solo dalle classi; ciò è una diretta conseguenza della Proposizione 3.10.

Dalle corrispondenti proprietà degli interi seguono le conclusioni del seguente

Teorema 3.17 (*i*) *Le operazioni* $+$ *e* $\cdot$ *sono associative, vale cioè*

$$([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n), \quad ([a]_n \cdot [b]_n) \cdot [c]_n = [a]_n \cdot ([b]_n \cdot [c]_n)$$

per ogni $[a]_n, [b]_n, [c]_n \in \mathbb{Z}/n\mathbb{Z}$.

(*ii*) *Le operazioni* $+$ *e* $\cdot$ *sono commutative, vale cioè*

$$[a]_n + [b]_n = [b]_n + [a]_n, \quad [a]_n \cdot [b]_n = [b]_n \cdot [a]_n$$

per ogni $[a]_n, [b]_n \in \mathbb{Z}/n\mathbb{Z}$.

(*iii*) *La classe* $[0]_n$ *è l'elemento neutro per l'addizione e la classe* $[1]_n$ *è l'elemento neutro per la moltiplicazione. Inoltre l'elemento* $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ *ha per inverso rispetto* a *+ l'elemento* $[-a]_n$.

(*iv*) *L'operazione* $\cdot$ *è distributiva rispetto all'operazione* $+$, *vale cioè*

$$[a]_n \cdot ([b]_n + [c]_n) = [a]_n \cdot [b]_n + [a]_n \cdot [c]_n$$

per ogni $[a]_n, [b]_n, [c]_n \in \mathbb{Z}/n\mathbb{Z}$.

A differenza dell'addizione non tutte le classi di resto hanno un inverso rispetto alla moltiplicazione: ad esempio $[2]_4$ non ha un inverso in $\mathbb{Z}/4\mathbb{Z}$. Le classi $[a]_n$ per cui un inverso moltiplicativo esiste sono dette *invertibili*: $[a]_n$ è quindi invertibile se esiste una classe $[b]_n$ per cui $[a]_n[b]_n = [1]_n$. L'insieme delle classi invertibili modulo n si indica con $(\mathbb{Z}/n\mathbb{Z})^*$.

Dal criterio di risolubilità per le congruenze lineari troviamo che la classe $[a]_n$ è invertibile se e solo se $(a, n) = 1$. È quindi chiaro che il prodotto di due classi invertibili è ancora una classe invertibile; in altri termini, la moltiplicazione induce per restrizione un'operazione, indicata ancora con $\cdot$, su $(\mathbb{Z}/n\mathbb{Z})^*$. Nel caso particolare di modulo p un numero primo si ha $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} \setminus \{[0]_p\}$, cioè ogni classe non nulla è invertibile modulo un primo.

Per calcolare l'inverso della classe $[a]_n$ si può usare l'Identità di Bezout. Infatti da $(a, n) = 1$ segue che esistono interi b e c, calcolabili con l'Algoritmo di Euclide,

per cui $ab + nc = 1$; ma allora, passando alle classi modulo n, otteniamo $ab \equiv 1 \pmod{n}$, cioè $[b]_n$ è l'inverso di $[a]_n$.

Possiamo enunciare il Teorema Cinese dei Resti sui sistemi di congruenze lineari, in modo equivalente, come una proprietà delle classi di resto

Teorema 3.18 *Se n e m sono due interi non nulli primi tra loro allora l'applicazione*

$$\mathbb{Z}/mn\mathbb{Z} \ni [a]_{nm} \longmapsto ([a]_n, [a]_m) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

è biiettiva.

Un immediato corollario è il seguente

Corollario 3.19 *Siano m e n due interi non nulli primi tra loro, la classe $[a]_{nm}$ è invertibile se e solo se $[a]_n$ e $[a]_m$ sono invertibili, inoltre l'applicazione $[a]_{nm} \longmapsto ([a]_n, [a]_m)$ è una biiezione tra $(\mathbb{Z}/nm\mathbb{Z})^*$ e $(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$.*

La *funzione di Eulero* $n \longmapsto \phi(n)$ associa ad un intero positivo n il numero $\phi(n)$ di interi tra 1 e n primi con n; questa funzione ha un ruolo importante nell'aritmetica modulare. Per quanto visto $\phi(n)$ è anche uguale al numero di elementi invertibili modulo n, cioè $\phi(n)$ è la cardinalità di $(\mathbb{Z}/n\mathbb{Z})^*$. Abbiamo ad esempio $\phi(p) = p - 1$.

Una funzione f su $\mathbb{N}$ è detta *moltiplicativa* se, per ogni coppia di naturali n e m primi tra loro, si ha $f(nm) = f(n)f(m)$. Il corollario precedente permette di concludere allora che la funzione di Eulero è moltiplicativa. Contando i numeri da 1 a p^e non divisibili per p è chiaro che $\phi(p^e) = (p-1)p^{e-1}$, per ogni intero $e \geq 1$. Abbiamo così provato la seguente formula

Osservazione 3.20 *Se $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ è la fattorizzazione di n in primi con $p_i \neq p_j$ per $i \neq j$ e $e_i \geq 1$ per ogni i, allora*

$$\phi(n) = \prod_{i=1}^{r} (p_i - 1) p_i^{e_i - 1}.$$

Il Corollario 3.14 può essere anche espresso come $a^{\phi(p)} \equiv 1 \pmod{p}$ se p è primo e a non è divisibile per p. In questo forma esso può essere generalizzato in

Teorema 3.21 (di Eulero) *Se a è un intero primo con il modulo n allora $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Terminiamo questa parte sulle congruenze illustrando in dettaglio alcuni metodi per risolvere i sistemi di congruenze lineari con moduli coprimi, come nel Teorema Cinese dei Resti. Consideriamo il sistema di due congruenze

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \end{cases}$$

con n_1 e n_2 primi tra loro. Risolvere il sistema è equivalente a trovare due interi u e v per cui $x = a_1 + un_1$ e $x = a_2 + vn_2$. In altri termini, u e v sono soluzioni dell'equazione diofantea lineare

$$n_1 u - n_2 v = a_2 - a_1.$$

Questo tipo di equazioni è risolto in dettaglio nell'Esercizio Preliminare 7. Trovati u e v, abbiamo che la soluzione del sistema è la classe di resto di $x_0 = a_1 + un_1 = a_2 + vn_2$ modulo $n_1 n_2$. Come sappiamo essa è l'unica soluzione modulo $n_1 n_2$ o, equivalentemente, tutte le soluzioni intere sono date da $x_0 + hn_1 n_2$ al variare di h in $\mathbb{Z}$.

Passiamo ora a sistemi con un numero r qualsiasi di congruenze lineari

$$\begin{cases} x \equiv a_1 & (\text{mod } n_1) \\ x \equiv a_2 & (\text{mod } n_2) \\ x \equiv a_3 & (\text{mod } n_3) \\ \quad \vdots & \\ x \equiv a_r & (\text{mod } n_r) \end{cases}$$

con $n_1, n_2, \ldots, n_r$ a due a due primi tra loro. Possiamo usare il metodo sopra descritto per trovare l'unica soluzione x_0 modulo $n_1 n_2$ del sottosistema delle prime due congruenze e considerare il sistema equivalente

$$\begin{cases} x \equiv x_0 & (\text{mod } n_1 n_2) \\ x \equiv a_3 & (\text{mod } n_3) \\ \quad \vdots & \\ x \equiv a_r & (\text{mod } n_r) \end{cases}$$

che ha ora $r - 1$ congruenze. Continuando a risolvere le prime due congruenze, troviamo via via sistemi equivalenti con meno congruenze fino alla soluzione del sistema dato.

Vediamo ora un altro metodo per risolvere l'iniziale sistema di r congruenze lineari. Sappiamo che esso ammette una sola soluzione modulo $n_1 n_2 \cdots n_r$. Per calcolarla cerchiamo prima dei numeri interi $x_1, x_2, \ldots, x_r$ per cui, per ogni $i = 1, 2, \ldots, r$, si ha $x_i \equiv 0 \pmod{n_j}$ per ogni $j \neq i$ e $x_i \equiv 1 \pmod{n_i}$. In altri termini, $x_1, x_2, \ldots, x_r$ sono soluzioni dei sistemi

$$\begin{cases} x_1 \equiv 1 & (\text{mod } n_1) \\ x_1 \equiv 0 & (\text{mod } n_2) \\ \quad \vdots & \\ x_1 \equiv 0 & (\text{mod } n_r) \end{cases} \quad \begin{cases} x_2 \equiv 0 & (\text{mod } n_1) \\ x_2 \equiv 1 & (\text{mod } n_2) \\ \quad \vdots & \\ x_2 \equiv 0 & (\text{mod } n_r) \end{cases} \quad \cdots \quad \begin{cases} x_r \equiv 0 & (\text{mod } n_1) \\ x_r \equiv 0 & (\text{mod } n_2) \\ \quad \vdots & \\ x_r \equiv 1 & (\text{mod } n_r). \end{cases}$$

Una volta risolti questi sistemi è chiaro che la soluzione del sistema originario è

$$x_0 \equiv a_1 x_1 + a_2 x_2 + \ldots + a_r x_r \pmod{n_1 n_2 \cdots n_r}.$$

Per trovare l'intero x_1, e analogamente $x_2, \ldots, x_r$, basta osservare che necessariamente $x_1 = y_1 n_2 \cdots n_r$ per qualche intero y_1. Inoltre, $n_2 \cdots n_r$ è una classe invertibile modulo n_1, date le ipotesi sui moduli $n_1, n_2, \ldots, n_r$; y_1 si ottiene quindi risolvendo $y_1(n_2 \cdots n_r) \equiv 1 \pmod{n_1}$ o, equivalentemente, $y_1 \equiv (n_2 \cdots n_r)^{-1} \pmod{n_1}$. Questa congruenza è, come sopra, equivalente ad un'equazione diofantea lineare e può quindi essere esplicitamente risolta.

Questo secondo metodo per il calcolo delle soluzioni del sistema attraverso le soluzioni ausiliarie $x_1, x_2, \ldots, x_r$, può essere utile quando si debbano risolvere più sistemi di congruenze con moduli $n_1, n_2, \ldots, n_r$ fissati ma termini noti $a_1, a_2, \ldots, a_r$ che cambiamo di sistema in sistema; ciò capita spesso negli esercizi.

Le osservazioni qui viste sul calcolo esplicito delle soluzioni di un sistema di congruenze lineari verranno ripetutamente usate, solitamente senza menzione esplicita, nelle soluzioni degli esercizi presentati.

1.4 I gruppi

1.4.1 Definizione e prime proprietà

Una delle strutture fondamentali dell'algebra è quella di gruppo; essa è abbastanza semplice da essere definita in poche righe ma, nello stesso tempo, ha un'importanza cruciale. Le strutture più complesse che vedremo in seguito saranno tutte basate sui gruppi.

Un insieme non vuoto G con un'operazione $\cdot$ si dice *gruppo* se

(i) l'operazione $\cdot$ è associativa,

(ii) in G esiste un elemento e, detto *elemento neutro*, per cui $g \cdot e = g = e \cdot g$ per ogni g in G,

(iii) per ogni elemento g di G esiste un elemento h, detto *inverso* di g, tale che $g \cdot h = e = h \cdot g$.

Nel seguito diremo che $(G, \cdot)$ è un gruppo per indicare che $\cdot$ è un'operazione su G che rende tale insieme un gruppo; se l'operazione è chiara dal contesto diremo semplicemente che G è un gruppo. A volte il simbolo $\cdot$ dell'operazione di un gruppo verrà omesso anche nelle composizioni e scriveremo gh per indicare la composizione $g \cdot h$ di g e h in G.

Gli esempi di gruppo sono innumerevoli: l'insieme $\mathbb{Z}$ dei numeri interi con l'operazione di addizione; l'insieme $\mathbb{Q}^*$ dei numeri razionali non nulli con l'operazione di moltiplicazione; l'insieme $\mathbb{R}^*$ dei numeri reali non nulli, come anche l'insieme $\mathbb{C}^*$ dei numeri complessi non nulli, con l'operazione di prodotto; l'insieme S_n delle permutazioni di n elementi con l'operazione di composizione.

È molto facile provare che in un gruppo esiste un solo elemento neutro. Altrettanto ovvio è che dato un elemento g in un gruppo, esiste un unico inverso di g; esso è indicato con g^{-1}.

In generale se n è un intero positivo e g un elemento di un gruppo, definiamo g^n come la composizione di g con se stesso n volte e poniamo, inoltre, $g^{-n} = (g^n)^{-1}$.

In questo modo valgono le usuali regole per le potenze: $g^n \cdot g^m = g^{n+m}$ e $(g^n)^m = g^{nm}$ per ogni coppia di naturali n e m.

Se g e h sono due elementi di un gruppo, diciamo che essi *commutano* se $gh = hg$. Inoltre, se succede che l'operazione di un gruppo G è commutativa, se cioè vale $gh = hg$ per ogni g e h in G, o in altri termini se ogni coppia di elementi commuta, diciamo che il gruppo è *commutativo* o *abeliano*. È usuale indicare l'operazione di un gruppo abeliano con $+$, si dice allora che il gruppo è *denotato additivamente*. In un gruppo denotato additivamente scriviamo $-g$ per l'inverso di un elemento g e ng per g^n. Abbiamo ovviamente $(n+m)g = ng + mg$ e $(nm)g = n(mg)$ per ogni coppia di naturali n e m.

L'*ordine* di un gruppo G è la cardinalità dell'insieme G, esso si indica con $|G|$; l'ordine è quindi il numero di elementi di G se G è finito altrimenti l'ordine è infinito. Invece, l'*ordine* di un elemento g è il minimo intero positivo n, se esiste, per cui $g^n = e$; se invece $g^n \neq e$ per ogni n positivo allora diciamo che g ha ordine *infinito*. Indichiamo l'ordine di g con $\mathrm{ord}(g)$.

Si osservi che l'insieme $\mathbb{Z}/n\mathbb{Z}$ delle classi di congruenza modulo un naturale non nullo n è un gruppo con l'operazione $+$ di addizione tra classi, come segue subito dal Teorema 3.17. È chiaro che si tratta di un gruppo abeliano di ordine n. Anche l'insieme $(\mathbb{Z}/n\mathbb{Z})^*$ delle classi invertibili modulo n è un gruppo abeliano con l'operazione $\cdot$ di moltiplicazione tra classi; il suo ordine è $\phi(n)$.

La nostra prima osservazione teorica sui gruppi è la seguente. Dalla definizione di gruppo segue subito che valgono le seguenti leggi

Osservazione 4.1 (Leggi di Cancellazione) *Se in un gruppo G si ha $gh = gk$ allora $h = k$; allo stesso modo se vale $hg = kg$ allora $h = k$.*

1.4.2 Sottogruppi

Un sottoinsieme H di un gruppo G si dice *sottogruppo* se l'operazione $\cdot$ di G può essere ristretta ad un'operazione di H e, con questa operazione, H è un gruppo. Scriviamo $H \leq G$ per indicare che H è un sottogruppo di G. Per verificare che un sottoinsieme non vuoto H è un sottogruppo basta controllare che dati comunque due elementi h e k in H si ha $h \cdot k \in H$ e che, per ogni elemento h di H, vale $h^{-1} \in H$.

Ad esempio, il sottoinsieme $2\mathbb{Z}$ dei numeri pari è un sottogruppo di $\mathbb{Z}$, come lo è il sottoinsieme $n\mathbb{Z}$ dei multipli di un fissato naturale n. Il sottoinsieme $\{\pm 1\}$ è un sottogruppo di $\mathbb{Q}^*$ che, a sua volta, è un sottogruppo di $\mathbb{R}^*$. Il sottoinsieme delle permutazioni che fissano 1 è un sottogruppo di S_n.

Il sottoinsieme $\{e\}$ è sempre un sottogruppo di un gruppo G, come anche G è un sottogruppo di G; questi due sottogruppi sono detti *banali* e i sottogruppi non banali sono anche detti *propri*.

Dato un gruppo G il sottoinsieme $Z(G)$ di tutti gli elementi z di G per cui $zg = gz$ per ogni g di G, si chiama *centro* di G; un elemento z è nel centro se commuta con tutti gli elementi del gruppo.

Osservazione 4.2 *Il centro $Z(G)$ è un sottogruppo di G.*

Ritroveremo spesso in seguito il centro in varie questioni, esso misura quanto un gruppo è non abeliano: infatti G è abeliano se e solo se $Z(G) = G$.

Osserviamo che l'intersezione di sottogruppi è ancora un sottogruppo; ciò non è invece vero in generale per l'unione. Dato un sottoinsieme X di un gruppo G, indichiamo con $\langle X \rangle$ il sottogruppo *generato* da X in G: esso è definito come l'intersezione di tutti i sottogruppi di G che contengono X. Si osservi che esiste sempre almeno un tale sottogruppo, infatti G contiene X. Diciamo che X è un *insieme di generatori* per il gruppo $\langle X \rangle$. Il sottogruppo $\langle X \rangle$ generato da X in G può essere caratterizzato come il più piccolo sottogruppo di G che contiene X.

In particolare un gruppo G si dice *ciclico* se esiste un elemento g in G per cui $G = \langle g \rangle$; l'elemento g è un generatore per G. Se G è ciclico allora è chiaramente abeliano. Inoltre se g ha ordine finito n allora $G = \{e, g, g^2, \ldots, g^{n-1}\}$ e quindi il gruppo ciclico generato da g ha ordine n. Lo stesso vale se g ha ordine infinito, in tal caso si avrà $G = \{\ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots\}$.

Ad esempio, $\mathbb{Z}$ è un gruppo ciclico infinito, infatti $\mathbb{Z} = \langle 1 \rangle$. Anche $n\mathbb{Z} = \langle n \rangle$ è un gruppo ciclico infinito e $\mathbb{Z}/n\mathbb{Z} = \langle [1]_n \rangle$ è un gruppo ciclico di ordine n.

Usando la Divisione Euclidea possiamo subito dimostrare che

Osservazione 4.3 *Un sottogruppo di un gruppo ciclico è ancora ciclico.*

Da questa osservazione abbiamo la descrizione dei sottogruppi di $\mathbb{Z}$

Corollario 4.4 *Se H è un sottogruppo di $\mathbb{Z}$ allora $H = n\mathbb{Z}$ per qualche intero non negativo n.*

Non solo, come richiamato sopra $\mathbb{Z}/n\mathbb{Z}$ è un gruppo ciclico, esso è anche il prototipo di ogni gruppo ciclico finito, come vedremo in seguito. Studiamo quindi i suoi sottogruppi cominciando con l'osservare che dalle proprietà delle congruenze segue

Osservazione 4.5 *Per ogni intero a l'ordine di $[a]_n$ in $\mathbb{Z}/n\mathbb{Z}$ è*

$$\mathrm{ord}([a]_n) = \frac{n}{(a, n)}.$$

Come possiamo vedere subito dalla formula, abbiamo sempre che $\mathrm{ord}([a]_n)$ divide $n = |\mathbb{Z}/n\mathbb{Z}|$; questo non è un caso come avremo modo di vedere nella successiva sezione. Altre importanti conseguenze sono

Osservazione 4.6 *Per ogni divisore d dell'ordine n ci sono $\phi(d)$ elementi di ordine d in $\mathbb{Z}/n\mathbb{Z}$ e, inoltre, vi è un solo sottogruppo di $\mathbb{Z}/n\mathbb{Z}$ di ordine d; esso è generato dalla classe $[n/d]_n$. Infine, questi sottogruppi esauriscono la classe dei sottogruppi di $\mathbb{Z}/n\mathbb{Z}$.*

Abbiamo un'ulteriore interessante conseguenza suddividendo gli elementi di $\mathbb{Z}/n\mathbb{Z}$ per ordine. Risulta infatti

Osservazione 4.7 *Se n è un naturale non nullo allora $\sum_{d \mid n} \phi(d) = n$.*

1.4.3 Prodotto di sottogruppi

Se H e K sono sottoinsiemi di un gruppo G definiamo HK come l'insieme di tutti i prodotti hk al variare di h in H e k in K. Anche se H e K sono sottogruppi non è detto che HK sia un sottogruppo di G. Sicuramente se G è abeliano allora HK è un sottogruppo; in generale si ha

Proposizione 4.8 *Il prodotto HK di due sottogruppi H e K è un sottogruppo se e solo se $HK = KH$.*

In generale però, anche se HK non è un sottogruppo, possiamo dire qualcosa sulla sua cardinalità. Si trova subito infatti che ogni elemento di HK può essere espresso come hk per $|H \cap K|$ coppie (h, k) in $H \times K$. Abbiamo quindi

Osservazione 4.9 *Siano H e K due sottogruppi finiti di un gruppo G, allora $|HK| = |H||K|/|H \cap K|$.*

1.4.4 Classi laterali di un sottogruppo

Se H è un sottogruppo di G definiamo una relazione $\sim_H$ in G nel seguente modo: $g \sim_H k$ se e solo se $g^{-1}k \in H$; diciamo che g è *congruo* a k modulo H o, anche, che g e k sono *congruenti* modulo H. È facile provare che $\sim_H$ è una relazione di equivalenza. Si noti che, in particolare, se n è un naturale non nullo, per il sottogruppo $n\mathbb{Z}$ del gruppo $\mathbb{Z}$ ritroviamo la relazione di congruenza per gli interi definita in precedenza.

Le classi di equivalenza di $\sim_H$ si chiamano *laterali sinistri* di H in G; questo nome è giustificato dall'essere la classe di equivalenza di g il sottoinsieme $gH = \{gh \,|\, h \in H\}$. Possiamo chiaramente definire una versione destra ponendo $g \ {}_H\!\sim k$ se e solo se $gk^{-1} \in H$; per questa nuova relazione le classi di equivalenza saranno i *laterali destri* $Hg = \{hg \,|\, h \in H\}$. È chiaro che in un gruppo abeliano non vi è alcuna differenza tra le due relazioni, un sottoinsieme è un laterale destro se e solo se è un laterale sinistro.

L'insieme quoziente rispetto alla relazione $\sim_H$ si indica con G/H, se invece usiamo ${}_H\!\sim$ allora scriviamo $H\backslash G$ per il quoziente. Si noti che $gH \longmapsto Hg$ è una corrispondenza biunivoca tra G/H e $H\backslash G$.

Definiamo l'*indice* $[G : H]$ del sottogruppo H di G come la cardinalità dell'insieme quoziente G/H. Per quanto osservato questa è anche la cardinalità di $H\backslash G$. Useremo l'indice di un sottogruppo quasi esclusivamente quando esso è finito.

Vogliamo ora ricavare un'importante proprietà dei sottogruppi di un gruppo finito. La mappa $h \longmapsto gh$ definisce una biiezione tra H e il laterale sinistro gH; in particolare ogni laterale ha la stessa cardinalità di H. Visto che $\sim_H$ induce una partizione di G ricaviamo subito

Teorema 4.10 (di Lagrange) *L'ordine di un sottogruppo di un gruppo finito divide l'ordine del gruppo.*

E come corollario abbiamo

Corollario 4.11 *L'ordine di un elemento di un gruppo finito divide l'ordine del gruppo. In particolare se il gruppo finito G ha ordine n e g è un suo elemento allora $g^n = e$.*

Da questo risultato possiamo ricavare il Teorema di Eulero 3.21: basta infatti osservare che $(\mathbb{Z}/n\mathbb{Z})^*$ ha ordine $\phi(n)$.

Un'altra immediata conseguenza riguarda i gruppi di ordine un primo. Se g è un elemento diverso dall'elemento neutro di un gruppo G di ordine primo p, allora l'ordine di g, dovendo dividere p, non può che essere p. Abbiamo così

Corollario 4.12 *Un gruppo di ordine primo è ciclico.*

Infine, per un gruppo finito G e un suo sottogruppo H, troviamo che $[G : H] = |G|/|H|$; in particolare anche l'indice di un sottogruppo è un divisore dell'ordine del gruppo.

1.4.5 Sottogruppi normali

Abbiamo osservato sopra che in un gruppo abeliano i laterali destri di un sottogruppo coincidono con i laterali sinistri. Questa è una proprietà fondamentale e i sottogruppi per cui questo vale hanno un'estrema importanza; è stato Évariste Galois a capirlo per primo.

Sia G un gruppo e h un suo elemento, ogni elemento del tipo ghg^{-1} si dice *coniugato* di h. Se H è un sottoinsieme di G allora gHg^{-1} è l'insieme di tutti gli elementi ghg^{-1} al variare di h in H. Un sottogruppo H si dice *normale* se $gHg^{-1} = H$ per ogni g in G. È chiaro che in un gruppo abeliano ogni sottogruppo è normale visto che $ghg^{-1} = h$ per ogni h e g. Notiamo che possiamo riscrivere la condizione di normalità come $gH = Hg$; troviamo quindi che un sottogruppo è normale se e solo se ogni laterale destro è un laterale sinistro.

Chiaramente i sottogruppo banali $\{e\}$ e G sono normali. Come altro esempio di sottogruppo normale possiamo considerare il centro: infatti $gZ(G) = Z(G)g$ visto che gli elementi di $Z(G)$ commutano con tutti gli elementi di G e, quindi, in particolare con l'elemento g.

Osserviamo inoltre che se H è un sottogruppo normale allora, per ogni coppia g_1, g_2 di elementi di G abbiamo $g_1Hg_2H = g_1g_2HH = g_1g_2H$, cioè il prodotto di due laterali sinistri, come sottoinsiemi di G, è ancora un laterale sinistro.

Ciò suggerisce la possibilità di definire un'operazione sul quoziente G/H ponendo $(g_1H) \cdot (g_2H) = (g_1g_2)H$. L'operazione tra le classi g_1H, g_2H dipende solo

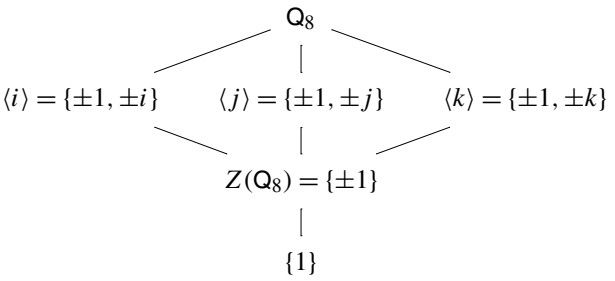
dalle classi e non dai rispettivi rappresentanti g_1 e g_2 scelti; infatti richiedere che questa definizione sia ben posta è esattamente equivalente ad avere H normale in G. Molto di più è vero

Teorema 4.13 *Se H è un sottogruppo normale di G allora l'operazione $g_1H \cdot g_2H = (g_1g_2)H$ definisce una struttura di gruppo sull'insieme quoziente G/H. L'ordine di questo gruppo è $[G : H]$.*

Diciamo che la struttura di gruppo del quoziente G/H è *indotta* dalla struttura di G. Se ritorniamo a considerare il gruppo abeliano $\mathbb{Z}$ e il suo sottogruppo, chiaramente normale, $n\mathbb{Z}$, vediamo che l'operazione di addizione definita sulle classi di congruenza è la struttura indotta sull'insieme quoziente $\mathbb{Z}/n\mathbb{Z}$ dall'addizione di $\mathbb{Z}$. Questo motiva la scelta della notazione $\mathbb{Z}/n\mathbb{Z}$ per le classi di resto.

Poter costruire un gruppo sull'insieme quoziente è una procedura estremamente importante. In G/H ci dimentichiamo di alcune informazioni, per così dire, visto che identifichiamo gli elementi di G che differiscono per elementi di H; ma d'altra parte G/H può essere più "semplice" di G. Inoltre, ed è questo il punto, potremmo essere in grado di ricavare alcune informazioni su G dalla conoscenza di G/H.

Abbiamo visto che tutti i sottogruppi di un gruppo abeliano sono normali; non è però vero il viceversa. Infatti, come esempio di sottogruppo non abeliano con tutti i sottogruppi normali, possiamo considerare il gruppo Q_8 delle *unità dei quaternioni*; esso è definito come segue. Gli elementi di Q_8 sono ± 1, $\pm i$, $\pm j$ e $\pm k$ in cui 1 è l'elemento neutro, la moltiplicazione per -1 cambia segno agli elementi, $i^2 = j^2 = k^2 = -1$ e $ij = k = -ji$, $jk = i = -kj$ e $ki = j = -ik$. È facile provare che i sottogruppi di Q_8 sono i seguenti



dove due sottogruppi sono collegati se quello più in basso è un sottogruppo di quello più in alto.

La normalità dei sottogruppi di Q_8 segue da principi generali; notiamo infatti che in questo caso un sottogruppo proprio H o ha indice 2 o è il centro. Ma, come già osservato, il centro è normale ed è, inoltre, sempre vero che

Osservazione 4.14 *Un sottogruppo di indice 2 è normale.*

1.4.6 Il gruppo simmetrico

Fissato un naturale n, l'insieme S_n di tutte le permutazioni di $\{1, 2, \ldots, n\}$ è un gruppo con la composizione di applicazioni, esso è detto *gruppo simmetrico* su n elementi. Sappiamo infatti che la composizione di applicazioni biiettive è ancora un'applicazione biiettiva, che l'applicazione identità è l'elemento neutro per la composizione e che ogni applicazione biiettiva è invertibile. Abbiamo anche visto che S_n ha $n!$ elementi.

Se $\sigma \in \mathsf{S}_n$ è una permutazione e $i_1, i_2, \ldots, i_n$ sono tali che $\sigma(k) = i_k$ per ogni $k = 1, 2, \ldots, n$, allora indichiamo la permutazione σ nel seguente modo

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}.$$

Dati $k_1, k_2, \ldots, k_\ell$ interi distinti nell'insieme $\{1, 2, \ldots, n\}$ la permutazione σ per cui

$\sigma(k_t) = k_{t+1}$, per ogni $t = 1, 2, \ldots, \ell - 1$,
$\sigma(k_\ell) = k_1$,
$\sigma(j) = j$ per ogni $j \in \{1, 2, \ldots, n\} \setminus \{k_1, k_2, \ldots, k_\ell\}$

è detta *ciclo* di *lunghezza* ℓ o anche ℓ–ciclo. Indicheremo il ciclo σ appena definito come $(k_1, k_2, \ldots, k_\ell)$.

Osserviamo che l'ordine di un ciclo è dato dalla sua lunghezza. Ad esempio, se $n \geq 3$, allora il ciclo $(1, 2, 3)$ in S_n ha ordine 3. Un ciclo (i, j) di lunghezza 2 è detto *trasposizione*: esso scambia i e j e non permuta nessun altro numero in $\{1, 2, \ldots, n\}$.

Il gruppo simmetrico S_n è *non* abeliano per ogni $n \geq 3$. Infatti si ha, ad esempio,

$$(123)(12) = (13) \neq (23) = (12)(123).$$

Come si vedrà nel seguito dello studio dell'algebra, non solo i gruppi simmetrici sono non abeliani, ma, anzi, essi sono sufficientemente complicati da contenere ogni gruppo finito come sottogruppo.

1.4.7 Omomorfismi di gruppi

Introduciamo ora gli omomorfismi, applicazioni che rispettano la struttura di gruppo; con gli omomorfismi possiamo confrontare i gruppi mettendoli in relazione tra loro. Come vedremo, questo modo di procedere sarà particolarmente fecondo.

Siano G, H due gruppi con rispettive operazioni $\cdot$ e $\circ$. Un'applicazione $f : G \longrightarrow H$ tra due gruppi si dice *omomorfismo* se $f(g_1 \cdot g_2) = f(g_1) \circ f(g_2)$ per ogni coppia di elementi g_1, g_2 di G.

È immediato dalla definizione che un omomorfismo manda l'elemento neutro di G nell'elemento neutro di H, cioè $f(e_G) = e_H$; inoltre $f(g^{-1}) = f(g)^{-1}$ e

$\text{ord}(f(g)) \mid \text{ord}(g)$. I sottogruppi vengono mandati in sottogruppi come chiarito dalla seguente proposizione

Proposizione 4.15 *Sia $G \xrightarrow{f} H$ un omomorfismo di gruppi. Se G' è un sottogruppo di G, allora $f(G')$ è un sottogruppo di H e se H' è un sottogruppo di H, $f^{-1}(H')$ è un sottogruppo di G.*

In particolare, l'immagine $f(G)$ di f è un sottogruppo di H; essa viene detta *immagine omomorfa* di G. L'immagine inversa del sottogruppo banale $\{e_H\}$ di H ha un'importanza fondamentale, essa è il *nucleo* di f, indicato con $\text{Ker}(f)$; in altri termini

$$\text{Ker}(f) = \{g \in G \mid f(g) = e_H\}.$$

Il nucleo misura quanto un omomorfismo non è iniettivo, abbiamo infatti

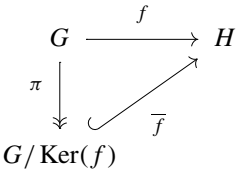
Proposizione 4.16 *Il nucleo di un omomorfismo è un sottogruppo normale di G. Inoltre, per ogni h in $\text{Im}(f)$ si ha $f^{-1}(h) = g\,\text{Ker}(f)$ con g un qualsiasi elemento di $f^{-1}(h)$. In particolare, f è iniettivo se e solo se $\text{Ker}(f)$ è banale.*

Non solo il nucleo di un omomorfismo è un sottogruppo normale, ma ogni sottogruppo normale è il nucleo di un omomorfismo: infatti, se H è normale in G, allora H è il nucleo dell'omomorfismo di proiezione al quoziente $G \longrightarrow G/H$. Riportiamo questa osservazione nella seguente

Proposizione 4.17 *Un sottogruppo di un gruppo è normale se e solo se è il nucleo di un omomorfismo.*

Il risultato fondamentale sugli omomorfismi di gruppi è il seguente

Teorema 4.18 (di Omomorfismo) *Se $G \xrightarrow{f} H$ è un omomorfismo e $G \xrightarrow{\pi} G/\text{Ker}(f)$ è l'omomorfismo quoziente, allora esiste un omomorfismo, necessariamente iniettivo, $\overline{f}$ che rende commutativo il diagramma*



Un omomorfismo biiettivo si chiama *isomorfismo*; se esiste un isomorfismo tra G e H diciamo che i due gruppi sono *isomorfi* e scriviamo $G \simeq H$. In particolare, dal teorema precedente abbiamo

Corollario 4.19 *Se f è suriettivo, $\overline{f}$ è un isomorfismo tra $G/\text{Ker}(f)$ e H.*

Questo corollario ci permette di concludere che le immagini omomorfe del gruppo G sono tutte quozienti di G e possono quindi essere costruite usando solo G. Inoltre ogni omomorfismo $f : G \longrightarrow H$ può essere fattorizzato nel seguente modo: l'omomorfismo di proiezione $\pi : G \longrightarrow G/\mathrm{Ker}(f)$, seguito dall'isomorfismo $\overline{f} : G/\mathrm{Ker}(f) \longrightarrow \mathrm{Im}(f)$ e infine dall'inclusione $\mathrm{Im}(f) \hookrightarrow H$; abbiamo cioè il diagramma commutativo

$$\begin{array}{ccc} G & \xrightarrow{\quad f \quad} & H \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ G/\mathrm{Ker}(f) & \xrightarrow[\sim]{\overline{f}} & \mathrm{Im}(f) \end{array}$$

Sia G un gruppo, chiamiamo *automorfismo* ogni isomorfismo di G con se stesso e indichiamo con $\mathrm{Aut}(G)$ l'insieme degli automorfismi di G. È chiaro che l'identità è un automorfismo, che la composizione di due automorfismi è ancora un automorfismo e che l'inverso di un automorfismo è un automorfismo, quindi $\mathrm{Aut}(G)$ è un gruppo con la composizione di applicazioni.

L'omomorfismo di passaggio al quoziente π associato ad un sottogruppo normale H di G ci permette di precisare il contenuto della Proposizione 4.15.

Proposizione 4.20 *L'insieme dei sottogruppi di G/H è in corrispondenza biunivoca con l'insieme dei sottogruppi di G che contengono H. In particolare le applicazioni $K' \longmapsto \pi^{-1}(K')$ e $G' \longmapsto \pi(G')$ realizzano questa corrispondenza. Inoltre a sottogruppi normali di G/H corrispondono sottogruppi normali di G.*

Possiamo ora dedurre facilmente la struttura dei gruppi ciclici. Basta infatti osservare che se $G = \langle g \rangle$ è un gruppo ciclico allora $\mathbb{Z} \ni k \longmapsto g^k \in G$ è un omomorfismo suriettivo. Applicando quanto visto a questo omomorfismo abbiamo

Teorema 4.21 (di Struttura dei Gruppi Ciclici) *Sia G un gruppo ciclico, se G è infinito allora $G \simeq \mathbb{Z}$ mentre, se $|G|$ ha ordine finito n allora $G \simeq \mathbb{Z}/n\mathbb{Z}$. Inoltre se $G = \langle g \rangle$ è infinito, i suoi sottogruppi sono $\langle g^k \rangle$ al variare di k tra gli interi positivi. Mentre se $|G| = n < \infty$, allora G ha un solo sottogruppo di ordine d per ogni divisore d di n.*

Si noti che la seconda parte sui sottogruppi nel caso di ordine finito è una conseguenza della corrispondenza tra sottogruppi di $\mathbb{Z}/n\mathbb{Z}$ e sottogruppi di $\mathbb{Z}$ che contengono $n\mathbb{Z}$; abbiamo cioè un'altra dimostrazione dell'Osservazione 4.6.

Sappiamo che, per gruppi finiti, l'ordine di un elemento divide l'ordine di un gruppo. Non è però vero che, in generale, per ogni divisore d dell'ordine di G esista un elemento di ordine d in G. Nel caso particolare di un divisore primo, ciò è vero e, per i gruppi abeliani, può essere dimostrato, ad esempio, usando il Teorema di Omomorfismo e una facile induzione.

Teorema 4.22 (di Cauchy) *Sia G è un gruppo finito e p un primo che divide l'ordine di G, allora in G esiste un elemento di ordine p.*

Anche l'ordine di un sottogruppo divide l'ordine di un gruppo; ma, come per gli elementi, non è vero che per ogni divisore dell'ordine di un gruppo esiste un sottogruppo di ordine il divisore. Sappiamo, invece, che un gruppo ciclico ha esattamente un sottogruppo per ogni divisore dell'ordine; questa situazione è molto speciale e anzi

Osservazione 4.23 *Se G è un gruppo finito con esattamente un sottogruppo di ordine d per ogni divisore d di $|G|$, allora G è ciclico.*

1.4.8 Prodotto diretto di gruppi

Dati due gruppi G e H con rispettive operazioni $\cdot$ e $\circ$, possiamo definire un'operazione sul prodotto cartesiano $G \times H$ ponendo $(g_1, h_1)(g_2, h_2) = (g_1 \cdot g_2, h_1 \circ h_2)$ per ogni $g_1, g_2 \in G$ e $h_1, h_2 \in H$. È molto facile provare che con questa operazione $G \times H$ è un gruppo, detto il *prodotto diretto* dei gruppi G e H.

Come vedremo le proprietà del prodotto diretto $G \times H$ sono in semplice relazione con le proprietà dei gruppi G e H. Troveremo spesso che un gruppo, definito in un qualche modo, risulta essere isomorfo al prodotto diretto di altri gruppi, ricaveremo così dai fattori le proprietà del gruppo a cui siamo interessati.

L'insieme $G \times H$ ha cardinalità il prodotto delle cardinalità di G e di H: se G e H hanno ordine finito allora $G \times H$ ha ordine $|G| \cdot |H|$ mentre, se anche uno solo dei due gruppi è infinito allora anche $G \times H$ è infinito. Per gli ordine degli elementi abbiamo la seguente

Osservazione 4.24 *Se gli elementi $g \in G$ e $h \in H$ hanno ordini finiti rispettivamente m e n, allora l'ordine dell'elemento (g, h) in $G \times H$ è il minimo comune multiplo di m e n.*

Anche il centro di $G \times H$ è semplicemente descritto, si verifica subito infatti che $Z(G \times H) = Z(G) \times Z(H)$. In particolare

Osservazione 4.25 *Il gruppo $G \times H$ è abeliano se e solo se G e H sono entrambi abeliani.*

Se G' è un sottogruppo di G e H' un sottogruppo di H, il gruppo $G' \times H'$ è in modo naturale un sottogruppo di $G \times H$; ma si noti che *non* tutti i sottogruppi di $G \times H$ sono prodotti diretti di sottogruppi. Ad esempio il sottogruppo diagonale $\{(g, g) \mid g \in G\}$ non è prodotto diretto di sottogruppi non appena G ha più di un elemento.

Vediamo ora un'applicazione dell'osservazione precedente sull'ordine degli elementi di un prodotto. Troviamo subito

Osservazione 4.26 *Un prodotto diretto di gruppi ciclici finiti, di ordini m e n rispettivamente, è ciclico se e solo se m e n sono primi tra loro.*

In particolare per i gruppi ciclici delle classi di resto $\mathbb{Z}/m\mathbb{Z}$ e $\mathbb{Z}/n\mathbb{Z}$ abbiamo che l'omomorfismo

$$\mathbb{Z}/mn\mathbb{Z} \ni [a]_{mn} \longmapsto ([a]_m, [a]_n) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

è un isomorfismo se e solo se m e n sono primi tra loro. Inoltre possiamo restringere questo omomorfismo a $(\mathbb{Z}/mn\mathbb{Z})^*$ e ottenere un omomorfismo tra le strutture moltiplicative

$$(\mathbb{Z}/mn\mathbb{Z})^* \ni [a]_{mn} \longmapsto ([a]_m, [a]_n) \in (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*;$$

anche in questo caso abbiamo un isomorfismo se e solo se m e n sono primi tra loro. Si noti che, in questo modo, abbiamo precisato il contenuto del Teorema 3.18 e del relativo Corollario 3.19.

1.5 Gli anelli

1.5.1 Definizione e prime proprietà

Gli anelli sono insiemi con due operazioni le cui proprietà sono modellate su quelle dell'addizione e della moltiplicazione tra interi: un insieme A con due operazioni $+$ e $\cdot$ si dice *anello* se

(i) A è un gruppo abeliano con l'operazione $+$,
(ii) l'operazione $\cdot$ è associativa,
(iii) l'operazione $\cdot$ è distributiva rispetto a $+$.

Chiamiamo l'operazione $+$ *addizione* e l'operazione $\cdot$ *moltiplicazione*. L'elemento neutro per l'addizione è indicato con 0, chiamato *zero* dell'anello A. Si noti, invece, che non è detto che esista un elemento neutro per $\cdot$, se ciò accade allora diciamo che l'anello è *con unità* o *unitario*, l'unità è allora unica e verrà indicata con 1, detta *uno* dell'anello. Si noti che può ben succedere che $0 = 1$, ma allora è facile provare che $A = \{0\}$, tale anello si chiama l'anello *nullo*. Se la moltiplicazione è un'operazione commutativa per A allora l'anello si dice *commutativo*.

Le elementari regole di calcolo degli interi continuano a valere in un anello qualsiasi, abbiamo infatti

Osservazione 5.1 *Sia A un anello, allora per ogni a e b in A si ha*: $a0 = 0a = 0$, $a(-b) = (-a)b = -(ab)$, $(-a)(-b) = ab$. *Se inoltre, A è unitario allora* $(-1)a = -a$ *e* $(-1)(-1) = 1$.

Il primo esempio di anello è ovviamente $\mathbb{Z}$, un anello commutativo unitario. Grazie al Teorema 3.17 anche le classi di resto $\mathbb{Z}/n\mathbb{Z}$ modulo un intero positivo n sono un anello commutativo unitario, $0 + n\mathbb{Z}$ è lo zero e $1 + n\mathbb{Z}$ è l'uno.

Un elemento a di un anello A è detto *divisore dello zero* se esiste un elemento $b \neq 0$ in A per cui $ab = 0$. Indichiamo l'insieme dei divisori dello zero dell'anello A con $D(A)$. Ovviamente zero è un divisore dello zero in ogni anello non nullo. Un anello che non ha divisori dello zero oltre a 0 è detto *dominio d'integrità*. Gli interi sono un dominio di integrità mentre $\mathbb{Z}/n\mathbb{Z}$ è un dominio di integrità se e solo se n è un primo. Infatti, grazie alla Proposizione 3.11 i divisori di zero sono le classi $a + n\mathbb{Z}$ con $(a, n) \neq 1$.

Un elemento a di un anello è *nilpotente* se esiste un intero positivo k per cui $a^k = 0$. Ad esempio, se $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ è la fattorizzazione di n in primi distinti, allora una classe $\overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$ è nilpotente se e solo se $p_1 p_2 \cdots p_r$ divide a in $\mathbb{Z}$; si veda l'Esercizio Preliminare 14.

Useremo spesso in seguito il contenuto della seguente osservazione, di fatto equivalente alla definizione di dominio di integrità.

Osservazione 5.2 (Legge dell'Annullamento del Prodotto) *Siano a, b due elementi di un dominio di integrità, se $ab = 0$ allora $a = 0$ o $b = 0$.*

Un elemento a di un anello unitario A è *invertibile* se esiste un elemento $b \in A$ per cui $ab = ba = 1$; indichiamo con A^* l'insieme degli elementi invertibili di A. Per l'anello $\mathbb{Z}$ abbiamo $\mathbb{Z}^* = \{1, -1\}$; anche $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ sono anelli commutativi unitari e si ha $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ e $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. È una conseguenza immediata della Proposizione 3.15 che la classe $a + n\mathbb{Z}$ è invertibile in $\mathbb{Z}/n\mathbb{Z}$ se solo se $(a, n) = 1$.

Osservazione 5.3 *Se A è unitario allora l'insieme A^* degli elementi invertibili è un gruppo con la moltiplicazione, abeliano se A è commutativo. Inoltre, in ogni caso, $A^* \cap D(A) = \varnothing$.*

Per un anello finito vale di più

Osservazione 5.4 *Se A è un anello unitario finito allora $A = A^* \sqcup D(A)$; cioè ogni elemento è o invertibile o un divisore di zero.*

Se $\mathbb{K}$ è un anello commutativo non nullo con unità per cui tutti gli elementi non nulli sono invertibili, diciamo che $\mathbb{K}$ è un *campo*. In altre parole, $\mathbb{K} \neq \{0\}$ è un campo se e solo se $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$; inoltre, in tal caso, questo insieme è un gruppo abeliano con l'operazione di moltiplicazione. Osserviamo che ogni campo è un dominio di integrità e quindi nei campi vale la Legge dell'Annullamento del Prodotto. Esempi di campi sono $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$. Possiamo però anche costruire campi con un numero finito di elementi, infatti, se p è un numero primo allora $\mathbb{Z}/p\mathbb{Z}$ è un campo in quanto, come osservato in precedenza, ogni classe non nulla è invertibile modulo p.

In un anello commutativo il calcolo delle potenze di un binomio è simile a quello per i binomi di numeri.

Osservazione 5.5 (Binomio di Newton) *Se a e b sono due elementi di un anello commutativo A, allora per ogni intero positivo n vale*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

1.5.2 Sottoanelli, ideali e quozienti

Un sottoinsieme B di un anello A è detto *sottoanello* se le operazioni $+$ e $\cdot$ possono essere ristrette a B e se con queste operazioni ristrette B è un anello. È chiaro che per controllare che un sottoinsieme non vuoto B è un sottoanello basta controllare che $b_1 + b_2$ e $b_1 \cdot b_2$ siano elementi di B per ogni b_1 e b_2 di B e che $-b \in B$ per ogni $b \in B$. Equivalentemente un sottoinsieme B è un sottoanello se è un sottogruppo per l'addizione e se è chiuso per la moltiplicazione.

Sia ora A' un anello contenente l'anello A e sia X un sottoinsieme di A'. È chiaro che l'intersezione di un numero qualunque di sottoanelli di A' è ancora un sottoanello. Possiamo quindi definire l'anello *generato* da X su A come l'intersezione di tutti i sottoanelli di A' che contengono $A \cup X$; indichiamo tale anello con $A[X]$, esso è il più piccolo sottoanello di A' che contiene $A \cup X$. Per un anello commutativo A è facile provare che $A[X]$ è l'insieme di tutte le somme

$$a_1 y_1 + a_2 y_2 + \cdots + a_k y_k$$

al variare di k nei naturali, $a_1, a_2, \ldots, a_k$ in A e $y_1, y_2, \ldots, y_r$ tra i possibili prodotti di elementi di X. Se l'insieme X è finito, diciamo $X = \{x_1, x_2, \ldots, x_r\}$, scriviamo $A[x_1, x_2, \ldots, x_r]$ per $A[X]$. In particolare se $X = \{x\}$ e A è commutativo, allora $A[x]$ è l'insieme di tutte le somme

$$\sum_{h=0}^{k} a_k x^k$$

al variare di k nei naturali e $a_0, a_1, \ldots, a_k$ in A.

Un *omomorfismo* di anelli è un'applicazione $A \xrightarrow{f} B$ tra due anelli A e B con la proprietà: $f(a_1 + a_2) = f(a_1) + f(a_2)$ e $f(a_1 a_2) = f(a_1) f(a_2)$ per ogni $a_1, a_2 \in A$. Inoltre, se A e B sono unitari allora richiediamo che un omomorfismo f mandi l'unità 1_A di A nell'unità 1_B di B, cioè $f(1_A) = 1_B$. Un *isomorfismo* di anelli è un omomorfismo biiettivo di anelli; come per i gruppi scriviamo $A \simeq B$ se esiste un isomorfismo da A in B e diciamo che A e B sono *isomorfi*.

Se A è un anello commutativo unitario allora vi è un solo modo di estendere l'assegnazione $\mathbb{Z} \ni 1 \longmapsto 1_A \in A$ ad un omomorfismo di anelli. In particolare possiamo pensare ai numeri interi come ad elementi di A; si noti però che questo omomorfismo non è iniettivo in generale.

Un omomorfismo di anelli è anche un omomorfismo tra i gruppi additivi $(A, +)$ e $(B, +)$. Possiamo quindi definire il *nucleo* $\mathrm{Ker}(f)$ di un omomorfismo di anelli f come il nucleo dell'omomorfismo tra i gruppi additivi, cioè $\mathrm{Ker}(f)$ è l'insieme degli elementi di A che vengono mandati in 0_B da f

$$\mathrm{Ker}(f) = \{a \in A \mid f(a) = 0_B\}.$$

Non solo $\mathrm{Ker}(f)$ è un sottoanello di A, ma vale anche $a_1 \cdot a_2 \in \mathrm{Ker}(f)$ se a_1 o a_2 sono in $\mathrm{Ker}(f)$, diciamo che $\mathrm{Ker}(f)$ *assorbe* rispetto alla moltiplicazione. In generale, un qualsiasi sottogruppo additivo I di A che assorba rispetto alla moltiplicazione è detto *ideale*.

Un ideale è per un anello quello che un sottogruppo normale è per un gruppo. Infatti, essendo $(A, +)$ un gruppo abeliano, un ideale I è un sottogruppo normale rispetto a $+$. Inoltre se consideriamo l'insieme quoziente A/I delle classi laterali $a + I$ dell'ideale I rispetto all'addizione, al variare di a in A,

$$A/I = \{a + I \mid a \in A\},$$

esso non solo è un gruppo abeliano con l'addizione delle classi indotta da $+$ in A, ma, ponendo $(a_1 + I) \cdot (a_2 + I) = a_1 a_2 + I$ definiamo una moltiplicazione che rende A/I un anello. In altre parole, se I è un ideale di A allora le operazioni $+$ e $\cdot$ di A passano all'insieme quoziente A/I e rendono tale insieme un anello. Abbiamo che l'applicazione di passaggio al quoziente

$$A \ni a \longmapsto a + I \in A/I$$

è un omomorfismo suriettivo. Quindi, analogamente ai gruppi, gli ideali sono esattamente i nuclei degli omomorfismi.

Vediamo ora un'altra definizione che, nel seguito, si dimostrerà estremamente importante: un ideale $M \neq A$ è detto *massimale* se non è contenuto propriamente in nessun ideale diverso da A.

Sia A un anello e X un suo sottoinsieme. Definiamo l'ideale *generato* da X come l'intersezione di tutti gli ideali di A che contengono X, indichiamo tale ideale con (X), esso è il più piccolo ideale di A che contiene X. Per un anello commutativo A, l'ideale X è l'insieme di tutte le somme

$$a_1 x_1 + a_2 x_2 + \cdots + a_k x_k$$

al variare di k nei naturali, $a_1, a_2, \ldots, a_k$ in A e $x_1, x_2, \ldots, x_k$ in X. Se l'insieme X è finito, diciamo $X = \{x_1, x_2, \ldots, x_r\}$, scriviamo $(x_1, x_2, \ldots, x_r)$ per (X). In particolare, se $X = \{x\}$ e A è commutativo, allora l'ideale (x) generato da x è il sottoinsieme $A \cdot x$ di A di tutti i multipli ax con $a \in A$.

1.5.3 Anelli di polinomi

Vediamo ora la definizione di polinomio a coefficienti in un anello commutativo A. Per non appesantire la trattazione, introducendo ad esempio il linguaggio delle

successioni definitivamente nulle, scegliamo di non essere completamente formali; ci accontentiamo di un minore livello di rigore confidando che il lettore abbia già un'idea intuitiva di cosa siano i polinomi.

Sia x un simbolo, che chiamiamo *indeterminata*; consideriamo inoltre i simboli $1 = x^0, x = x^1, x^2, x^3, \dots$ che chiamiamo *potenze* dell'indeterminata. Se n è un naturale e $a_0, a_1, a_2, \dots, a_n$ sono elementi dell'anello A, la somma formale

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

è detta *polinomio* nell'indeterminata x con *coefficienti* $a_0, a_1, \dots, a_n$ nell'anello A. Per comodità di linguaggio, pensiamo che $f(x)$ abbia i coefficienti $a_{n+1}, a_{n+2}, \dots$ tutti nulli. Il coefficiente a_0 è detto il *termine noto* del polinomio. Il polinomio *nullo*, indicato con 0 si ottiene scegliendo $n = 0$ e $a_0 = 0$; esso ha quindi tutti i coefficienti nulli. Due polinomi $a_0 + a_1 x + \cdots + a_n x^n$ sono *uguali* se hanno i coefficienti corrispondentemente uguali, cioè se $a_0 = b_0$, $a_1 = b_1$ e così via.

Dato un polinomio $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ non nullo, chiamiamo *grado* di $f(x)$, indicato con $\deg(f)$, il più piccolo intero r per cui i coefficienti $a_{r+1}, a_{r+2}, \dots$ sono tutti nulli. Sottolineiamo che non assegniamo alcun grado al polinomio nullo. Per un polinomio di grado r, il coefficiente a_r si chiama *coefficiente direttore* di $f(x)$. Se A è unitario, un polinomio *monico* è un polinomio con coefficiente direttore 1. Un polinomio *costante* è un polinomio nullo o di grado 1, quindi $f(x)$ è costante se e solo se $f(x) = a_0$, con $a_0 \in A$.

L'insieme dei polinomi a coefficienti in A e nell'indeterminata x è indicato con $A[x]$. Vediamo ora come usare le operazioni dell'anello A per definire un'addizione e una moltiplicazione che rendano $A[x]$ un anello. Se $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$ e $g(x) = b_0 + b_1 x + b_2 x^2 + \cdots$ sono polinomi allora definiamo l'addizione di $f(x)$ e $g(x)$ come

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots .$$

È facile verificare che con questa operazione $A[x]$ è un gruppo abeliano, l'elemento neutro è il polinomio nullo e l'opposto di $a_0 + a_2 x + a_2 x^2 + \cdots$ è il polinomio $-a_0 - a_1 x - a_2 x^2 - \cdots$.

Per la moltiplicazione cominciamo definendo il prodotto tra potenze della indeterminata: $x^n \cdot x^m = x^{n+m}$ per ogni n e m naturali. Estendiamo poi questa operazione ai polinomi *per bilinearità*: se $f(x)$ e $g(x)$ sono i polinomi introdotti sopra poniamo

$$\begin{aligned} f(x) \cdot g(x) &= (a_0 + a_1 x + a_2 x^2 + \cdots) \cdot (b_0 + b_1 x + b_2 x^2 + \cdots) \\ &= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \cdots \\ &= \sum_k \left(\sum_{h=0}^{k} a_h b_{k-h} \right) x^k . \end{aligned}$$

È molto facile provare che l'operazione così definita è commutativa e associativa e, se A è unitario, allora il polinomio 1 è l'elemento neutro per il prodotto. Inoltre,

come è chiaro dalla stessa definizione di prodotto, la moltiplicazione è distributiva rispetto alla somma. Abbiamo quindi

Proposizione 5.6 *Dato un anello commutativo A, l'insieme $A[x]$ dei polinomi a coefficienti in A è un anello commutativo. Se inoltre A è unitario allora anche $A[x]$ lo è.*

Il grado dei polinomi ha due importanti proprietà rispetto all'addizione e alla moltiplicazione

Osservazione 5.7 *Siano $f(x)$ e $g(x)$ due polinomi non nulli in $A[x]$, valgono*
(i) *se $f(x)+g(x)$ non è il polinomio nullo allora*

$$\deg(f+g) \leq \max\{\deg(f), \deg(g)\},$$

(ii) *se A è un dominio di integrità allora* $\deg(f \cdot g) = \deg(f)\deg(g)$; *in particolare $A[x]$ è un dominio di integrità.*

Possiamo subito ricavare da ciò gli elementi invertibili

Corollario 5.8 *Se A è un dominio di integrità allora $A[x]^* = A^*$.*

Nel seguito useremo spesso la valutazione di un polinomio in un elemento, precisiamo ora cosa intendiamo con questo. Sia a un fissato elemento di A. Esiste allora un unico omomorfismo di anelli

$$A[x] \ni f(x) \overset{v_a}{\longmapsto} f(a) \in A$$

detto, *valutazione* in a, ottenuto sostituendo ogni occorrenza di x in $f(x)$ con a. Una *radice* di $f(x)$ è un elemento a di A per cui $f(a) = 0$. È chiaro che se A è un sottoanello di B allora $A[x]$ è un sottoanello di $B[x]$, possiamo quindi valutare i polinomi di $A[x]$ anche negli elementi di B. In particolare possiamo cercare le radici di un polinomio in un anello più grande dell'anello dei coefficienti. È inoltre chiaro che l'immagine di $A[x]$ in B attraverso la mappa di valutazione in a è il sottoanello $A[a]$ di B generato da a su A.

Se abbiamo un omomorfismo tra anelli $A \overset{f}{\longrightarrow} B$ possiamo indurre una mappa tra i rispettivi anelli di polinomi ponendo

$$A[x] \ni a_0 + a_1 x + \cdots + a_n x^n \longmapsto f(a_0) + f(a_1)x + \cdots + f(a_n)x^n \in B[x].$$

Segue subito dalla definizione delle operazioni sui polinomi che questa mappa è un omomorfismo di anelli. Osserviamo che questo omomorfismo non aumenta il grado dei polinomi e, in particolare, se il coefficiente direttore a_n di $f(x)$ non è nel nucleo di f, allora l'omomorfismo mantiene il grado di $f(x)$.

1.5.4 Divisibilità tra polinomi

In questa e nelle prossime sezioni studieremo in particolare l'anello dei polinomi $\mathbb{K}[x]$ a coefficienti in un campo $\mathbb{K}$. Esiste una stretta analogia tra questo anello e l'anello degli interi; un primo esempio è la divisione euclidea tra polinomi in cui il grado gioca il ruolo del valore assoluto.

Proposizione 5.9 (Divisione Euclidea tra Polinomi) *Siano $f(x)$, $g(x)$ due polinomi in $\mathbb{K}[x]$ con $f(x)$ non nullo. Allora esistono e sono unici due polinomi $q(x), r(x) \in \mathbb{K}[x]$ per cui $g(x) = q(x)f(x) + r(x)$ con $r(x) = 0$ o $\deg(r) < \deg(f)$.*

Come per gli interi, $q(x)$ è detto *quoziente* della divisione di $g(x)$ per $f(x)$ e $r(x)$ è detto *resto*. Se accade che $r(x) = 0$, e quindi $g(x) = q(x)f(x)$, allora diciamo che $f(x)$ *divide* $g(x)$ o che $g(x)$ è un *multiplo* di $f(X)$, in simboli $f(x) \mid g(x)$.

Teorema 5.10 (di Ruffini) *L'elemento $a \in \mathbb{K}$ è una radice per $f(x) \in \mathbb{K}[x]$ se e solo se $x - a$ divide $f(x)$.*

Usando il Teorema di Ruffini possiamo definire la *molteplicità* di una radice a del polinomio $f(x)$, come il naturale k per cui $(x-a)^k$ divide $f(x)$ ma $(x-a)^{k+1}$ non divide $f(x)$. Una radice di molteplicità 1 si dice *semplice*, invece una radice di molteplicità maggiore di 1 si dice *multipla* o *non semplice*.

Se $a_1, a_2, \ldots, a_r$ sono le radici di $f(x)$ con rispettive molteplicità $k_1, k_2, \ldots, k_r$ allora il numero delle radici, contate con la loro molteplicità, è $k_1 + k_2 + \cdots + k_r$. Confrontando il grado di un polinomio con i fattori $x - a$ al variare di a nelle radici otteniamo

Corollario 5.11 *Un polinomio non nullo $f(x) \in \mathbb{K}[x]$ ha in $\mathbb{K}$ al più $\deg(f)$ radici contate con la loro molteplicità.*

Siano $f(x)$ e $g(x)$ sono polinomi non entrambi nulli di $\mathbb{K}[x]$, chiamiamo *massimo comun divisore* di $f(x)$ e $g(x)$ un polinomio $p(x)$ che verifichi le seguenti proprietà

(i) $p(x)$ divide sia $f(x)$ che $g(x)$,

(ii) se $q(x)$ è un polinomio che divide $f(x)$ e $g(x)$ allora $q(x)$ divide $p(x)$.

Indichiamo un massimo comun divisore di $f(x)$ e $g(x)$ con $(f(x), g(x))$. Con una dimostrazione esattamente analoga a quella degli interi possiamo dimostrare l'esistenza del massimo comun divisore e l'Identità di Bezout

Proposizione 5.12 *Se $f(x), g(x)$ non sono entrambi nulli allora esiste un massimo comune divisore $(f(x), g(x)) \in \mathbb{K}[x]$. Inoltre esistono $h(x), k(x) \in \mathbb{K}[x]$ per cui $(f(x), g(x)) = h(x)f(x) + k(x)g(x)$.*

Osserviamo subito che l'Algoritmo di Euclide per gli interi funziona anche per i polinomi sostituendo la divisione tra interi con la divisione tra polinomi. In que-

sto modo possiamo calcolare esplicitamente un massimo comun divisore e scrivere l'Identità di Bezout tra polinomi.

Si noti, però, che il massimo comun divisore tra polinomi *non* è unico. Comunque, se $h(x)$ e $k(x)$ sono due massimi comun divisori di $f(x)$ e $g(x)$, allora esiste $\lambda \in \mathbb{K}^*$ per cui $h(x) = \lambda \cdot k(x)$. Se, come in questo caso, due polinomi $h(x)$ e $k(x)$ differiscono per una costante moltiplicativa non nulla, allora diciamo che $h(x)$ e $h(x)$ sono *associati*. Possiamo quindi dire che il massimo comun divisore tra polinomi è unico a meno di associati. In particolare esiste un unico massimo comun divisore monico, detto spesso *il* massimo comun divisore.

Come tra i numeri interi, due polinomi sono *primi tra loro* se il loro massimo comun divisore è 1.

1.5.5 Fattorizzazione di polinomi

Continuiamo a studiare l'analogia tra gli interi e l'anello dei polinomi $\mathbb{K}[x]$ a coefficienti in un campo $\mathbb{K}$. Un polinomio non costante $f(x)$ si dice *irriducibile* se in ogni fattorizzazione $f(x) = g(x)h(x)$ si ha che $g(x)$ o $h(x)$ è una costante. Nel seguito sarà chiaro come i polinomi irriducibili hanno per $\mathbb{K}[x]$ le stesse proprietà che hanno in numeri primi per $\mathbb{Z}$. Ad esempio, ragionando come per gli interi, usando il grado al posto del valore assoluto, troviamo

Teorema 5.13 *Ogni polinomio non costante si fattorizza in polinomi irriducibili*; *tale fattorizzazione è unica a meno dell'ordine dei fattori una volta identificati i fattori associati*.

Vediamo ora come si fattorizzano i polinomi su alcuni campi particolari. Cominciamo dai numeri complessi per cui usiamo il seguente

Teorema 5.14 (Fondamentale dell'Algebra) *Ogni polinomio non costante a coefficienti complessi ha una radice complessa*.

A dispetto del nome, non esiste una dimostrazione puramente algebrica di questo teorema; infatti la completezza dei numeri reali o qualche altra proprietà analitica o topologica è essenziale.

Vediamo ora varie immediate conseguenze che descrivono i polinomi irriducibili a coefficienti complessi o reali.

Corollario 5.15

(i) *Un polinomio in* $\mathbb{C}[x]$ *è irriducibile se e solo se è di primo grado*,

(ii) *ogni polinomio in* $\mathbb{C}[x]$ *si fattorizza in polinomi di primo grado*,

(iii) *un polinomio non nullo* $f(x) \in \mathbb{C}[x]$ *ha* $\deg(f)$ *radici contate con la loro molteplicità*,

(iv) *un polinomio è irriducibile in* $\mathbb{R}[x]$ *se e solo se ha grado* 1 *o grado* 2 *ed è del tipo* $x^2 + ax + b$ *con* $a^2 - 4b < 0$.

Studiamo ora la fattorizzazione e l'irriducibilità dei polinomi a coefficienti razionali; decidere l'irriducibilità di un polinomio su $\mathbb{Q}$ è estremamente più difficile che per $\mathbb{R}$ o $\mathbb{C}$. Per prima cosa vediamo come possiamo ricondurci a polinomi a coefficienti interi.

Dato un polinomio a coefficienti interi $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, il *contenuto* $c(f)$ di $f(x)$ è il massimo comun divisore dei coefficienti $a_0, a_1, \ldots, a_n$. Un polinomio di contenuto 1 è detto *primitivo*; ovviamente ogni polinomio si scrive come $f(x) = c(f) \cdot f_1(x)$ con $f_1(x)$ primitivo. Il risultato chiave per passare da $\mathbb{Q}$ a $\mathbb{Z}$ è il seguente

Lemma 5.16 (di Gauss) *Il prodotto di due polinomi primitivi è ancora primitivo.*

Dal Lemma di Gauss ricaviamo alcuni corollari

Corollario 5.17 *Se* $f(x), g(x) \in \mathbb{Z}[x]$ *allora* $c(f \cdot g) = c(f)c(g)$.

Corollario 5.18 *Siano* $f(x), g(x) \in \mathbb{Z}[x]$ *e supponiamo che* $f(x)$ *sia primitivo e che divida* $g(x)$ *in* $\mathbb{Q}[x]$, *allora* $f(x)$ *divide* $g(x)$ *in* $\mathbb{Z}[x]$.

Osserviamo ora che, dato il polinomio $f(x) \in \mathbb{Q}[x]$, possiamo sempre scrivere $f(x) = cf_1(x)$ con c razionale e $f_1(x) \in \mathbb{Z}[x]$ primitivo. Quindi, se dobbiamo fattorizzare $f(x)$ possiamo sempre ricondurci alla fattorizzazione in $\mathbb{Q}[x]$ del polinomio $f_1(x)$ primitivo e a coefficienti interi. Il seguente risultato ci dice che basta studiare la fattorizzazione di $f_1(x)$ in $\mathbb{Z}[x]$ e non in $\mathbb{Q}[x]$.

Corollario 5.19 *Un polinomio primitivo in* $\mathbb{Z}[x]$ *è irriducibile in* $\mathbb{Q}[x]$ *se e solo se è irriducibile in* $\mathbb{Z}[x]$.

Vediamo ora alcuni criteri per la fattorizzazione in $\mathbb{Z}[x]$. Il primo ci permette di controllare se esistono radici; ovviamente un polinomio con una radice è irriducibile se e solo se è di primo grado, grazie al Teorema di Ruffini.

Osservazione 5.20 *Sia* $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ *un polinomio a coefficienti interi di grado* n, *allora una radice in* $\mathbb{Q}$ *si può scrivere come* a/b *con* a *un divisore intero di* a_0 *e* b *un divisore intero di* a_n.

Questo criterio ci permette di decidere in un numero finito di passi se $f(x)$ ha una radice, basta infatti controllare i razionali a/b come nell'osservazione e questi sono in numero finito.

Il successivo criterio usa la riduzione dei coefficienti modulo un primo. Sia $f(x)$ come sopra un polinomio in $\mathbb{Z}[x]$ e sia p un primo che non divide il coefficiente direttore di $f(x)$. L'omomorfismo quoziente $\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$ induce un omomorfismo $\pi : \mathbb{Z}[x] \longrightarrow (\mathbb{Z}/p\mathbb{Z})[x]$ ed $f(x)$ non è nel nucleo di tale omomorfismo.

Osservazione 5.21 *Se $\pi(f)$ è irriducibile in $(\mathbb{Z}/p\mathbb{Z})[x]$ allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$.*

L'interesse di questa osservazione è che il campo $\mathbb{Z}/p\mathbb{Z}$ ha p elementi, è cioè finito, e quindi è anche finito il numero di polinomi di un certo grado. Può risultare così agevole provare che un polinomio è irriducibile. Si noti però che esistono polinomi irriducibili in $\mathbb{Z}[x]$ ma riducibili modulo p per ogni primo p; la conclusione dell'osservazione non è quindi invertibile.

Un utile criterio per l'irriducibilità di un polinomio a coefficienti interi è

Proposizione 5.22 (Criterio di Eisenstein) *Sia $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ un polinomio a coefficienti interi, se esiste un primo p per cui: p non divide a_n, p divide $a_0, a_1, \ldots, a_{n-1}$ e p^2 non divide a_0; allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$, e quindi anche in $\mathbb{Q}[x]$.*

Il Criterio di Eisenstein si applica ai polinomio del tipo $x^n - p$ con n naturale e p primo. In particolare abbiamo

Osservazione 5.23 *Per ogni naturale n esistono infiniti polinomi irriducibili in $\mathbb{Q}[x]$ di grado n.*

Per illustrare un'ulteriore applicazione del criterio di Eisenstein, fissiamo un primo p e consideriamo il polinomio

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1},$$

detto polinomio *ciclotomico* p–esimo. Osserviamo che il polinomio $g(x) = f(x+1) = \sum_{k=0}^{p-1} \binom{p}{k+1} x^k$ ha per termine noto p e tutti i coefficienti divisibili per p tranne quello direttore che è 1. Possiamo allora applicare il Criterio di Eisenstein per concludere che $g(x)$ è irriducibile. Ma allora anche $f(x)$ lo è visto che l'applicazione

$$\mathbb{Z}[x] \ni h(x) \longmapsto h(x+1) \in \mathbb{Z}[x]$$

è un isomorfismo di anelli. Abbiamo così provato

Osservazione 5.24 *Per ogni primo p il polinomio $x^{p-1} + x^{p-2} + \cdots + x + 1$ è irriducibile in $\mathbb{Q}[x]$.*

1.5.6 Quozienti di anelli di polinomi

Sia $f(x)$ un polinomio in $\mathbb{K}[x]$ con $\mathbb{K}$ un campo e sia $(f(x)) = \mathbb{K}[x] \cdot f(x)$ l'ideale generato da $f(x)$ in $\mathbb{K}[x]$. Vogliamo studiare l'anello quoziente $\mathbb{K}[x]/(f(x))$.

A questo scopo, per completezza, è necessario ricordare alcune definizioni e un risultato sugli spazi vettoriali.

Un gruppo abeliano $(V, +)$ è detto *spazio vettoriale* sul campo $\mathbb{K}$ se esiste un'applicazione

$$\mathbb{K} \times V \ni (\lambda, v) \longmapsto \lambda \cdot v \in V$$

detta *prodotto per scalare*, con le seguenti proprietà

(i) $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$ per ogni $\lambda, \mu \in \mathbb{K}$ e $v \in V$,
(ii) $\lambda \cdot (u + v) = \lambda \cdot u + \lambda \cdot v$ per ogni $\lambda \in \mathbb{K}$ e $u, v \in V$,
(iii) $(\lambda\mu) \cdot v = \lambda \cdot (\mu \cdot v)$ per ogni $\lambda, \mu \in \mathbb{K}$ e $v \in V$,
(iv) $1 \cdot v = v$ per ogni $v \in V$.

Nel contesto degli spazi vettoriali gli elementi del campo $\mathbb{K}$ sono detti *scalari* e gli elementi di V *vettori*. In particolare l'elemento neutro di V rispetto a $+$ è detto *vettore nullo* e indicato, come al solito per i gruppi abeliani, con 0.

Un naturale esempio di spazio vettoriale è dato dall'insieme dei *vettori colonna*, cioè degli elementi di $\mathbb{K}^n$, dove n è un fissato intero positivo, con operazione di addizione e prodotto per scalare definiti da

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix}, \qquad \lambda \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \lambda x_2 \\ \vdots \\ \lambda x_n \end{pmatrix}.$$

Dati k vettori $v_1, v_2, \ldots, v_k$ di un spazio vettoriale V, una loro *combinazione lineare* è un qualunque vettore del tipo

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k$$

dove $\lambda_1, \lambda_2, \ldots, \lambda_k$ sono scalari qualsiasi. Se succede che l'unica combinazione lineare dei vettori $v_1, v_2, \ldots, v_k$ ad essere il vettore nullo è quella con $\lambda_1 = \lambda_2 = \cdots = \lambda_k = 0$, allora i vettori sono detti *linearmente indipendenti* altrimenti *linearmente dipendenti*.

I vettori di un insieme $\mathcal{V} \subseteq V$ sono dei *generatori* per lo spazio vettoriale V, se ogni vettore di V è combinazione lineare dei vettori di $\mathcal{V}$.

Una *base* per lo spazio vettoriale V è un insieme di generatori che sono anche linearmente indipendenti. Dalle definizioni segue che un insieme $v_1, v_2, \ldots, v_k$ è una base per V se e solo se ogni vettore di v si scrive in modo unico come combinazione lineare di $v_1, v_2, \ldots, v_k$. È possibile provare

Teorema 5.25 *Ogni spazio vettoriale ammette una base. Inoltre, due basi per lo stesso spazio vettoriale hanno la medesima cardinalità.*

La cardinalità comune a tutte le basi di uno spazio vettoriale V è detta la sua *dimensione*, indicata con $\dim V$. Ad esempio, è facile provare che $\mathbb{K}^n$ ha dimensione n.

Vediamo ora un'osservazione di carattere generale. Se A è un anello che contiene un campo $\mathbb{K}$ come sottoanello allora, con le operazioni di addizione di A come anello e l'operazione di moltiplicazione di A ristretta a $\mathbb{K} \times A \longrightarrow A$, l'anello A è uno spazio vettoriale su $\mathbb{K}$. In particolare, prendendo come A l'anello quoziente $\mathbb{K}[x]/(f(x))$, abbiamo

Proposizione 5.26 *L'insieme quoziente $\mathbb{K}[x]/(f(x))$ è un anello commutativo unitario. Un insieme di rappresentanti per le classi modulo $(f(x))$ è dato da 0 unito ai polinomi di grado minore di $\deg(f)$. Inoltre $\mathbb{K}[x]/(f(x))$ è uno spazio vettoriale su $\mathbb{K}$ di dimensione $n = \deg(f)$; una sua base è $1 + (f(x)), x + (f(x)), \ldots, x^{n-1} + (f(x))$.*

È possibile descrivere in maniera esplicita i divisori di zero, gli elementi invertibili e gli elementi nilpotenti di $\mathbb{K}[x]/(f(x))$ in modo perfettamente analogo agli anelli $\mathbb{Z}/n\mathbb{Z}$; infatti

Osservazione 5.27 *La classe $g(x) + (f(x))$ è un divisore di zero nell'anello $\mathbb{K}[x]/(f(x))$ se e solo se $g(x)$ e $f(x)$ non sono primi tra loro. Essa è invertibile se e solo se $g(x)$ e $f(x)$ sono primi tra loro ed è nilpotente se e solo se $g(x)$ è divisibile per ogni fattore irriducibile di $f(x)$ in $\mathbb{K}[x]$.*

Concludiamo questa sezione con un ulteriore analogia tra gli anelli del tipo $\mathbb{K}[x]/(f(x))$ e i quozienti $\mathbb{Z}/n\mathbb{Z}$.

Corollario 5.28 *L'anello $\mathbb{K}[x]/(f(x))$ è un campo se e solo se $f(x)$ è irriducibile in $\mathbb{K}[x]$.*

1.6 I campi

1.6.1 Caratteristica di un campo

Sia $\mathbb{K}$ un campo e consideriamo l'unico omomorfismo di anelli $\mathbb{Z} \xrightarrow{\varphi} \mathbb{K}$ per cui $\mathbb{Z} \ni 1 \longmapsto 1 \in \mathbb{K}$. È facile provare che per il nucleo di questo omomorfismo abbiamo due possibilità: o φ è iniettivo o esiste un intero primo p per cui $\mathrm{Ker}(\varphi) = p\mathbb{Z}$.

Nel primo caso $\mathbb{Z}$ è isomorfo ad un sottoanello di $\mathbb{K}$ e quindi, essendo $\mathbb{K}$ un campo, $\mathbb{K}$ contiene una copia isomorfa di $\mathbb{Q}$; in questo caso diciamo che $\mathbb{K}$ ha *caratteristica zero*.

Se invece $\mathrm{Ker}(\varphi) = p\mathbb{Z}$ allora $\mathbb{K}$ contiene una copia isomorfa del campo $\mathbb{Z}/p\mathbb{Z}$ e diciamo che $\mathbb{K}$ ha *caratteristica* p o *positiva*. Osserviamo che in questo caso

$$p \cdot a = \underbrace{a + a + \cdots + a}_{p \text{ volte}} = 0$$

per ogni a in $\mathbb{K}$. Ovviamente un campo con un numero finito di elementi ha caratteristica p per qualche primo p, esso infatti non può avere caratteristica 0 in quanto non contiene l'insieme infinito $\mathbb{Q}$.

Per un campo di caratteristica p il Teorema del Binomio di Newton con esponente p assume una forma particolarmente semplice.

Teorema 6.1 (del Binomio Ingenuo) *Se $\mathbb{K}$ è un campo di caratteristica positiva p allora*

$$(a+b)^p = a^p + b^p$$

per ogni $a, b \in \mathbb{K}$.

Nel caso particolare del campo $\mathbb{Z}/p\mathbb{Z}$ il Teorema del Binomio Ingenuo si specializza al Teorema 3.12 sulle congruenze modulo p.

Un'altra immediata conseguenza è che, per un campo $\mathbb{K}$ di caratteristica p, l'applicazione

$$\mathbb{K} \ni a \overset{F}{\longmapsto} a^p \in \mathbb{K}$$

è un *automorfismo* di $\mathbb{K}$, cioè un isomorfismo di $\mathbb{K}$ con se stesso; esso è detto l'automorfismo di Frobenius.

1.6.2 Gruppo moltiplicativo

Dato un campo $\mathbb{K}$, l'insieme $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ è un gruppo con l'operazione di moltiplicazione e la struttura di questo gruppo è molto particolare. Osserviamo, infatti, che se $a \in \mathbb{K}^*$ è un elemento di ordine che divide un intero positivo n, allora a è una radice del polinomio $x^n - 1$. Quindi in $\mathbb{K}^*$ non ci potranno essere più di n elementi di ordine un divisore di n. Segue allora subito dall'Osservazione 4.23 che

Proposizione 6.2 *Se G è un sottogruppo finito del gruppo moltiplicativo $\mathbb{K}^*$ di un campo $\mathbb{K}$ allora G è ciclico.*

Ciò si applica in particolare ai campi finiti

Corollario 6.3 *Il gruppo moltiplicativo $\mathbb{K}^*$ di un campo finito $\mathbb{K}$ è un gruppo ciclico di ordine $|\mathbb{K}| - 1$.*

1.6.3 Estensioni di campi

Dati due campi $\mathbb{K}$ e $\mathbb{F}$, diciamo che $\mathbb{F}$ è un'*estensione* di $\mathbb{K}$ se $\mathbb{K} \subseteq \mathbb{F}$, cioè se $\mathbb{K}$ è un sottocampo di $\mathbb{F}$. A volte scriveremo $\mathbb{F}/\mathbb{K}$ per indicare che $\mathbb{F}$ è un'estensione

di $\mathbb{K}$. Come già richiamato, se abbiamo un'estensione $\mathbb{F}/\mathbb{K}$ allora $\mathbb{F}$ è uno spazio vettoriale sul campo $\mathbb{K}$; definiamo *grado* dell'estensione $\mathbb{F}/\mathbb{K}$, indicato con $[\mathbb{F} : \mathbb{K}]$, la dimensione $\dim_{\mathbb{K}} \mathbb{F}$ di $\mathbb{F}$ come spazio vettoriale su $\mathbb{K}$. L'estensione $\mathbb{F}/\mathbb{K}$ è detta *finita* se ha grado finito.

Una *torre di estensioni* è una successione di estensioni di campi. Il grado è moltiplicativo in una torre di estensioni, vale cioè

Proposizione 6.4 *Se $\mathbb{L}/\mathbb{F}$ e $\mathbb{F}/\mathbb{K}$ sono estensioni di campi allora*

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{F}] \cdot [\mathbb{F} : \mathbb{K}].$$

Sia $\mathbb{F}/\mathbb{K}$ un'estensione di campi e sia X un sottoinsieme di $\mathbb{F}$. Visto che, come per gli anelli, l'intersezione di sottocampi di $\mathbb{F}$ è ancora un sottocampo, possiamo definire $\mathbb{K}(X)$ come l'intersezione di tutti i sottocampi di $\mathbb{F}$ che contengono $\mathbb{K} \cup X$. Esso è il più piccolo sottocampo di $\mathbb{F}$ che contiene $\mathbb{K} \cup X$ ed è chiaramente l'insieme di tutti i quozienti degli elementi del sottoanello $\mathbb{K}[X]$ di $\mathbb{F}$ generato da X su $\mathbb{K}$. Se l'insieme X è finito, diciamo $X = \{a_1, a_2, \ldots, a_k\}$, scriviamo $\mathbb{K}(a_1, a_2, \ldots, a_k)$ per $\mathbb{K}(X)$.

In particolare, se $a \in \mathbb{F}$, il sottocampo $\mathbb{K}(a)$ generato da a su $\mathbb{K}$ è l'insieme di tutti i possibili quozienti

$$\frac{f(a)}{g(a)}$$

al variare di $f(x)$ e $g(x)$ in $\mathbb{K}[x]$ con la condizione $g(a) \neq 0$.

Un elemento a di un'estensione $\mathbb{F}$ di $\mathbb{K}$ si dice *algebrico* su $\mathbb{K}$ se esiste un polinomio $f(x)$ non nullo a coefficienti in $\mathbb{K}$ per cui $f(a) = 0$. Un elemento non algebrico è detto *trascendente*. Ad esempio, il numero $\sqrt{2}$ è un elemento di $\mathbb{R}$ algebrico su $\mathbb{Q}$ visto che soddisfa $x^2 - 2 \in \mathbb{Q}[x]$. Nel 1882 il matematico tedesco Ferdinand von Lindemann ha fornito la prima dimostrazione che π è trascendente su $\mathbb{Q}$.

Dato un campo $\mathbb{L}$, un sottocampo $\mathbb{K}$ e due estensioni $\mathbb{E}$, $\mathbb{F}$ di $\mathbb{K}$ in $\mathbb{L}$, definiamo il *composto* di $\mathbb{E}$ e $\mathbb{F}$ come $\mathbb{E} \cdot \mathbb{F} = \mathbb{E}(\mathbb{F}) = \mathbb{F}(\mathbb{E})$; in altri termini $\mathbb{E} \cdot \mathbb{F}$ è la più piccola estensione di $\mathbb{K}$ in $\mathbb{L}$ che contiene $\mathbb{E}$ e $\mathbb{F}$.

Un'estensione $\mathbb{F}/\mathbb{K}$ è *algebrica* se ogni elemento di $\mathbb{F}$ è algebrico su $\mathbb{K}$. È facile dimostrare che $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ è un'estensione algebrica; invece $\mathbb{R}/\mathbb{Q}$ non è ovviamente un'estensione algebrica visto che $\pi \in \mathbb{R}$ non è algebrico su $\mathbb{Q}$.

Possiamo decidere se un elemento è algebrico o trascendente studiando l'omomorfismo di valutazione. Infatti

Osservazione 6.5 *Sia $\mathbb{F}/\mathbb{K}$ un'estensione di campi e sia $a \in \mathbb{F}$. L'elemento a è algebrico su $\mathbb{K}$ se e solo se l'omomorfismo di valutazione*

$$\mathbb{K}[x] \ni f(x) \overset{v_a}{\longmapsto} f(a) \in \mathbb{F}$$

ha nucleo non banale. In modo equivalente, a è trascendente se e solo se questo omomorfismo è iniettivo.

Dato $a \in \mathbb{F}$ algebrico su $\mathbb{K}$, sia $\mu(x)$ un polinomio monico di grado minimo nel nucleo $\mathrm{Ker}(v_a)$ della valutazione in a.

Proposizione 6.6 *Se $a \in \mathbb{F}$ è algebrico su $\mathbb{K}$ allora: μ è irriducibile in $\mathbb{K}[x]$, genera il nucleo $\mathrm{Ker}(v_a)$ della valutazione in a ed è l'unico polinomio monico irriducibile che si annulla in a.*

Alla luce di questa proposizione possiamo chiamare $\mu(x)$ il *polinomio minimo* di a su $\mathbb{K}$. Dalla definizione sappiamo che $\mathrm{Ker}(v_a) = (\mu(x)) = \mu(x) \cdot \mathbb{K}[x]$ e quindi abbiamo

Osservazione 6.7 *Se $a \in \mathbb{F}$ è algebrico su $\mathbb{K}$ allora $\mathbb{K}[a]$ è isomorfo a $\mathbb{K}[x]/(\mu(x))$.*

Ma allora, essendo $\mu(x)$ irriducibile, possiamo usare l'Identità di Bezout per ricaviamo gli inversi degli elementi non nulli in $\mathbb{K}[a]$ e concludere che $\mathbb{K}[a]$ è un campo. E quindi

Corollario 6.8 *Se $a \in \mathbb{F}$ è algebrico su $\mathbb{K}$ allora $\mathbb{K}(a) = \mathbb{K}[a]$.*

Un'ulteriore conseguenza dell'Osservazione 6.5 è il legame tra grado e carattere algebrico o trascendente di un elemento

Corollario 6.9 *L'elemento $a \in \mathbb{F}$ è algebrico su $\mathbb{K}$ se e solo se $\mathbb{K}(a)/\mathbb{K}$ è un'estensione finita. Inoltre, se questo è il caso, il grado $[\mathbb{K}(a) : \mathbb{K}]$ è uguale al grado del polinomio minimo di a su $\mathbb{K}$.*

È allora chiaro che in un'estensione finita non ci sono elementi trascendenti

Corollario 6.10 *Se $\mathbb{F}/\mathbb{K}$ è un'estensione finita allora è algebrica.*

Un'altra importante proprietà delle estensioni algebriche, essenzialmente una conseguenza del corollario precedente e della moltiplicatività del grado nelle torri, è la seguente

Proposizione 6.11 *Se $\mathbb{L}/\mathbb{F}$ e $\mathbb{F}/\mathbb{K}$ sono estensioni algebriche allora anche $\mathbb{L}/\mathbb{K}$ è un'estensione algebrica.*

In particolare

Osservazione 6.12 *Se $a_1, a_2, \ldots, a_k$ sono elementi di $\mathbb{F}$ algebrici su $\mathbb{K}$ allora l'anello $\mathbb{K}[a_1, a_2, \ldots, a_k]$ è un campo e il suo grado è finito su $\mathbb{K}$.*

Vediamo ora come si comporta il massimo comun divisore tra polinomi nelle estensioni di campi. Sia $\mathbb{F}/\mathbb{K}$ un'estensione di campi e siano $f(x)$ e $g(x)$ due polinomi in $\mathbb{K}[x]$. Possiamo allora calcolare il massimo comun divisore di $f(x)$ e $g(x)$ sia in $\mathbb{K}[x]$ e che in $\mathbb{F}[x]$. Ebbene

Osservazione 6.13 *Il massimo comun divisore tra $f(x)$ e $g(x)$ calcolato in $\mathbb{K}[x]$ è uguale al massimo comun divisore calcolato in $\mathbb{F}[x]$.*

Possiamo allora concludere che due polinomi di $\mathbb{K}[x]$ primi tra loro in $\mathbb{K}[x]$ continuano ad essere primi tra loro anche in $\mathbb{F}[x]$.

1.6.4 Campo di spezzamento

Un campo Ω si dice *algebricamente chiuso* se ogni polinomio in $\mathbb{K}[x]$ ha una radice in $\mathbb{K}$. Ad esempio, $\mathbb{C}$ è algebricamente chiuso ma $\mathbb{R}$ non lo è visto che il polinomio x^2+1 non ha radici in $\mathbb{R}$. Osserviamo che, grazie al Teorema di Ruffini, se Ω è algebricamente chiuso allora, dall'esistenza di una radice per $f(x)$, segue subito che $f(x)$ si fattorizza in polinomi di primo grado in $\mathbb{F}[x]$.

Un'estensione Ω di $\mathbb{K}$ è una *chiusura algebrica* di $\mathbb{K}$ se $\Omega/\mathbb{K}$ è un'estensione algebrica e Ω è algebricamente chiuso. Ad esempio $\mathbb{C}$ è la chiusura algebrica di $\mathbb{R}$ ma non è la chiusura algebrica di $\mathbb{Q}$ in quanto $\mathbb{C}/\mathbb{Q}$ non è un'estensione algebrica, infatti non lo è già $\mathbb{R}/\mathbb{Q}$.

La dimostrazione del seguente risultato usa in modo essenziale delle nozioni non elementari di logica matematica.

Teorema 6.14 *Ogni campo ammette una chiusura algebrica. Due chiusure algebriche dello stesso campo $\mathbb{K}$ sono isomorfe in un isomorfismo che fissa punto a punto $\mathbb{K}$.*

Per enunciare un criterio sull'esistenza di radici multiple per un polinomio abbiamo bisogno della derivata. Vediamo come sia possibile definire tale operatore senza il ricorso alla nozione di limite dell'analisi, cosa che, d'altra parte, richiederebbe una topologia sul campo $\mathbb{K}$ dei coefficienti. Sia $f(x)=a_0+a_1x+\cdots+a_nx^n$ un polinomio in $\mathbb{K}[x]$, definiamo la sua *derivata* come $f'(x)=a_1+2a_2x+\cdots+na_nx^{n-1}$. Questa definizione coincide con quella dell'analisi per i polinomi a coefficienti reali; non è quindi sorprendente che valgano le seguenti proprietà

(i) $(f(x)+g(x))'=f'(x)+g'(x)$, per ogni $f(x), g(x)\in\mathbb{K}[x]$,
(ii) $(\lambda f(x))'=\lambda f'(x)$, per ogni $\lambda\in\mathbb{K}$ e $f(x)\in\mathbb{K}[x]$,
(iii) $(f(x)g(x))'=f'(x)g(x)+f(x)g'(x)$, per ogni $f(x), g(x)\in\mathbb{K}[x]$.

In particolare, l'ultimo punto ci dice che continua a valere la Regola di Leibniz per la derivazione del prodotto. Da ciò abbiamo che se un elemento a della chiusura algebrica Ω di $\mathbb{K}$ è una radice multipla, allora $(x-a)$ è un fattore comune a $f(x)$ e $f'(x)$ in $\Omega[x]$. Però, visto che il massimo comun divisore non cambia nelle estensioni di campi, $f(x)$ e $f'(x)$ hanno un fattore comune in $\mathbb{K}[x]$.

Osservazione 6.15 (Criterio della Derivata) *Il polinomio $f(x)$ in $\mathbb{K}[x]$ ha una radice multipla nella chiusura algebrica di $\mathbb{K}$ se e solo se $f(x)$ e la sua derivata non sono primi tra loro in $\mathbb{K}[x]$.*

Sia ora $f(x) \in \mathbb{K}[x]$ un polinomio e sia Ω una chiusura algebrica di $\mathbb{K}$. In particolare Ω contiene tutte le radici $a_1, a_2, \ldots, a_k$ di $f(x)$. Chiamiamo *campo di spezzamento* di $f(x)$ in Ω il campo $\mathbb{K}(a_1, a_2, \ldots, a_k)$; esso avrà grado al più $\deg(f)$!

Il campo di spezzamento è il più piccolo sottocampo di Ω in cui il polinomio $f(x)$ si spezza in fattori lineari ed è *univocamente* determinato da $f(x)$ una volta fissata la chiusura algebrica Ω. Inoltre, il campo Ω è solo strumentale in quanto due campi di spezzamento costruiti in chiusure algebriche distinte sono tra loro isomorfi.

Come esempio vogliamo descrivere il campo di spezzamento del polinomio $x^n - 1$ su $\mathbb{Q}$. Le radici complesse di questo polinomio sono chiaramente le radici n–esime dell'unita: fissando $\zeta_n = e^{2\pi i/n} = \cos(2\pi/n) + i \sin(2\pi/n)$, esse si scrivono come $1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$. Notiamo che l'insieme di queste radici è un sottogruppo ciclico di ordine n di $\mathbb{C}^*$; una radice che sia un generatore di questo gruppo, come ad esempio ζ_n, è detta radice n–esima *primitiva* dell'unità. Vi sono, ovviamente, $\phi(n)$ radici primitive e si ottengono come ζ_n^h con $(h, n) = 1$.

Concludiamo che il campo di spezzamento di $x^n - 1$ su $\mathbb{Q}$ è $\mathbb{Q}(\zeta_n)$, questo campo è detto l'*estensione ciclotomica* n–esima di $\mathbb{Q}$. Ad esempio, per $n = 4$, otteniamo $\mathbb{Q}(i)$ e, essendo $x^2 + 1$ il polinomio minimo di i su $\mathbb{Q}$, il grado di $\mathbb{Q}(i)$ su $\mathbb{Q}$ è 2.

1.6.5 Campi finiti

Ricordiamo che un campo si dice *finito* se ha un numero finito di elementi. Come già osservato un campo finito non può avere caratteristica zero; esso è sempre di caratteristica positiva, che nel seguito indicheremo con p.

Sia $\mathbb{F}$ un campo finito e osserviamo che il campo $\mathbb{Z}/p\mathbb{Z}$ è un sottocampo di $\mathbb{F}$, in particolare $[\mathbb{F} : \mathbb{Z}/p\mathbb{Z}] = r < \infty$ e $\mathbb{F}$ ha p^r elementi. Troviamo così che $\mathbb{F}^*$ è un gruppo, necessariamente ciclico, con $p^r - 1$ elementi e quindi $a^{p^r-1} = 1$ per ogni $a \neq 0$, da cui ricaviamo che $a^{p^r} - a = 0$ per ogni elemento di $\mathbb{F}$.

Altra utile osservazione è che la chiusura algebrica di $\mathbb{F}$ e di $\mathbb{Z}/p\mathbb{Z}$ coincidono visto che $\mathbb{F}$ è un'estensione finita di $\mathbb{Z}/p\mathbb{Z}$.

Consideriamo ora il polinomio $x^{p^r} - x$, se fissiamo una chiusura algebrica Ω di $\mathbb{Z}/p\mathbb{Z}$, ricaviamo che il campo $\mathbb{F}$ è l'insieme delle radici in Ω di questo polinomio. Osservando anche che $x^{p^r} - x$ non ha radici multiple per il Criterio della Derivata e usando in modo cruciale l'Osservazione 4.23, possiamo facilmente dimostrare

Teorema 6.16 *Per ogni numero primo p e naturale r esiste un campo con p^r elementi. Tale campo è il campo di spezzamento del polinomio $x^{p^r} - x$ in una fissata chiusura algebrica Ω di $\mathbb{Z}/p\mathbb{Z}$. Esso è l'unico sottocampo con p^r elementi in Ω.*

Una volta fissata la chiusura algebrica Ω possiamo allora indicare con $\mathbb{F}_{p^r}$ l'unico suo sottocampo con p^r elementi. È usuale porre $q = p^r$ e, nel seguito, ci atterremo a questa convenzione anche senza richiamarla esplicitamente.

Osserviamo, per chiarire ogni eventuale dubbio, che $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$ ma in generale $\mathbb{F}_q$ *non* è isomorfo a $\mathbb{Z}/q\mathbb{Z}$ se r è maggiore di uno; infatti, $\mathbb{Z}/q\mathbb{Z}$ non è neanche un campo avendo $p + q\mathbb{Z}$ come divisore di zero.

Dall'unicità del campo di spezzamento troviamo che

Corollario 6.17 *Due campi finiti con lo stesso numero di elementi sono isomorfi.*

In Ω abbiamo quindi tutti i campi $\mathbb{F}_{p^r}$ al variare di r nei naturali. Il successivo risultato ci dice che la relazione di inclusioni tra questi sottocampi mima la relazione di divisibilità tra interi.

Proposizione 6.18 *Si ha l'inclusione $\mathbb{F}_{p^r} \subseteq \mathbb{F}_{p^s}$ se e solo se r divide s.*

Studiamo ora i campi di spezzamento per polinomi su campi finiti. Sia $f(x)$ un polinomio irriducibile in $\mathbb{F}_q[x]$ di grado r e sia a una sua qualunque radice in una chiusura algebrica Ω di $\mathbb{F}_p$. Visto che $f(x)$ è irriducibile, $\mathbb{F}_q(a)$ ha grado r su $\mathbb{F}_q$. Ma esiste un solo campo con q^r elementi in Ω, così $\mathbb{F}_q(a)$ contiene tutte le radici di $f(x)$; abbiamo cioè

Proposizione 6.19 *Sia $f(x) \in \mathbb{F}_q[x]$ un polinomio irriducibile di grado r e sia a una sua radice in una chiusura algebrica, allora $\mathbb{F}_q(a) = \mathbb{F}_{q^r}$ è il campo di spezzamento di $f(x)$.*

Come corollario otteniamo la descrizione del campo di spezzamento di un polinomio generico

Corollario 6.20 *Se $f(x)$ è un polinomio a coefficienti in $\mathbb{F}_q$ e*

$$f(x) = f_1(x) f_2(x) \cdots f_k(x)$$

è la sua decomposizione in polinomi irriducibili, allora il campo di spezzamento di $f(x)$ è $\mathbb{F}_{q^m}$ con m il minimo comune multiplo dei gradi dei fattori irriducibili $f_1(x), f_2(x), \ldots, f_k(x)$.

Vediamo ora un'applicazione di quanto appena visto, dato un naturale n e un primo p, studiamo il campo di spezzamento del polinomio $x^n - 1$ su $\mathbb{F}_p$. Se $n = p^e \cdot n'$ con p che non divide n' allora $x^n - 1 = (x^{n'} - 1)^{p^e}$ per il Teorema del Binomio Ingenuo e i polinomi $x^{n'} - 1$ e $(x^{n'} - 1)^{p^e}$ hanno ovviamente lo stesso campo di spezzamento. Possiamo quindi assumere, senza perdita di generalità, che p non divida n. Fondamentale è la seguente semplice osservazione

Osservazione 6.21 *Sia n un intero non divisibile per p e Ω una fissata chiusura algebrica di $\mathbb{F}_p$. Allora l'insieme delle radici di $x^n - 1$ forma un sottogruppo ciclico di ordine n in Ω^*.*

Il polinomio $x^n - 1$ si spezza così in $\mathbb{F}_{p^r}$ se e solo se $\mathbb{F}_{p^r}^*$ contiene un elemento di ordine n, come dire se e solo se n divide $p^r - 1$. Abbiamo quindi

Teorema 6.22 (Estensioni Ciclotomiche in caratteristica positiva) *Sia n un intero non divisibile per il primo p; il campo di spezzamento di $x^n - 1$ è $\mathbb{F}_{p^r}$ dove r è l'ordine di p nel gruppo moltiplicativo $(\mathbb{Z}/n\mathbb{Z})^*$.*

Passiamo ora ad un altro esempio. Lo studio della risolubilità delle equazioni di secondo grado in $\mathbb{F}_p$ è già particolarmente interessante. È stato il primo caso ad essere studiato ed ha quindi una qualche importanza storica.

Se $p = 2$ allora i polinomi di secondo grado sono solo: x^2, $x^2 + 1 = (x + 1)^2$, $x^2 + x = x(x + 1)$ e $x^2 + x + 1$ con quest'ultimo l'unico irriducibile visto che non ha radici. Nel seguito supponiamo $p \neq 2$.

La ben nota formula risolutiva delle equazioni di secondo grado, continua a valere in $\mathbb{F}_p$ se $p \neq 2$: l'equazione $ax^2 + bx + c = 0$ ha soluzioni

$$\frac{-b \pm \sqrt{\Delta}}{2a}$$

se $\Delta = b^2 - 4ac$ è un quadrato in $\mathbb{F}_p$, altrimenti non ha alcuna radice. Il problema si riduce quindi a capire quali elementi $a \in \mathbb{F}_p$ sono quadrati, detti *residui quadratici*, e quali non lo sono, detti *non residui quadratici*. Si introduce il *simbolo di Legendre*

$$\mathbb{F}_p^* \ni a \longmapsto \left(\frac{a}{p}\right) = \begin{cases} +1 & a \text{ è un residuo quadratico,} \\ -1 & a \text{ è un non residuo quadratico.} \end{cases}$$

Ad esempio, è facile provare quando -1 è un residuo quadratico; si ha infatti

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

per ogni primo p dispari, mentre chiaramente $-1 = 1$ è un residuo quadratico in $\mathbb{F}_2$. La dimostrazione di questo risultato è contenuta nell'Esercizio Preliminare 18. Esiste una formula simile, solo lievemente più complicata, per $\left(\frac{2}{p}\right)$. Infine, la Legge di Reciprocità Quadratica, congetturata da Eulero e Lagrange e dimostrata da Gauss nel 1796, permette il calcolo dei simboli di Legendre usando una notevole simmetria di $\left(\frac{q}{p}\right)$ quando p e q sono entrambi primi.

1.7 Esercizi preliminari

In questa sezione vediamo alcuni esercizi preliminari; essi dovrebbero essere studiati prima degli esercizi dei testi d'esame. Spesso infatti, le loro conclusioni e le tecniche impiegate sono usate come strumenti per risolvere gli esercizi dei capitoli successivi.

Esercizio 1 Sia X un insieme non vuoto. Dimostrare che il numero dei sottoinsiemi di X che hanno cardinalità pari è uguale al numero dei sottoinsiemi di X che hanno cardinalità dispari.

Soluzione 1 Usiamo l'induzione sulla cardinalità n di X. Il caso iniziale è $n = 1$, e in questo caso c'è un solo sottoinsieme di cardinalità pari, l'insieme vuoto, e un solo sottoinsieme di cardinalità dispari, X stesso. Pertanto l'enunciato è vero per $n = 1$.

Supponiamo ora che l'enunciato sia vero per $|X| = n$, e dimostriamolo per $|X| = n + 1$. Un insieme X con $n + 1$ elementi si può scrivere nella forma $X = Y \cup \{z\}$, dove Y è un insieme di n elementi e $z \notin Y$. Distinguiamo i sottoinsiemi A di X in due categorie: quella in cui $z \in A$ e quella in cui $z \notin A$. In altre parole, un sottoinsieme A di X è della forma $A = B \cup Z$ dove B è un sottoinsieme di Y e $Z = \varnothing$ oppure $Z = \{z\}$.

È chiaro che A ha cardinalità pari nei seguenti due casi: B ha cardinalità pari e $Z = \varnothing$ oppure B ha cardinalità dispari e $Z = \{z\}$. Per ipotesi induttiva, i sottoinsiemi relativi a ciascuno dei due casi sono 2^{n-1}, quindi in totale sono $2 \cdot 2^{n-1} = 2^n$. Poiché $2^n = \frac{1}{2} \cdot 2^{n+1}$ è la metà del numero totale dei sottoinsiemi di X, il numero di sottoinsiemi di cardinalità pari coincide con il numero di sottoinsiemi di cardinalità dispari.

Soluzione 2 Contiamo i sottoinsiemi di X dividendoli secondo la loro cardinalità, ed usiamo la formula del binomio,

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Ponendo $a = 1$ e $b = -1$ otteniamo

$$0 = 0^n = (1 - 1)^n = \sum_{k=0}^{n} (-1)^n \binom{n}{k},$$

ossia la somma dei termini con k pari, corrispondente al numero di sottoinsiemi di cardinalità pari, è uguale alla somma dei termini con k dispari, corrispondente al numero dei sottoinsiemi di cardinalità dispari.

Esercizio 2 Contare il numero di permutazioni σ di $\{1, \ldots, n\}$ tali che $\sigma(x) \neq x$ per ogni $x \in \{1, \ldots, n\}$.

Soluzione Il modo migliore per risolvere l'esercizio è l'uso del Principio di Inclusione Esclusione. Il numero totale di permutazioni di $\{1, \ldots, n\}$ è uguale a $n!$ Dunque è sufficiente contare le permutazioni σ che *non* soddisfano la proprietà richiesta, cioè quelle per cui esiste almeno un elemento x tale $\sigma(x) = x$. Per differenza si otterrà poi il risultato voluto.

Per $i = 1, 2, \ldots, n$ sia P_i l'insieme delle permutazioni σ di $\{1, \ldots, n\}$ tali che $\sigma(i) = i$. Quello che abbiamo deciso di contare è esattamente il numero degli elementi dell'insieme $P_1 \cup \cdots \cup P_n$, infatti per tali permutazioni almeno un elemento x è tale che $\sigma(x) = x$.

Calcoliamo ora la cardinalità $|P_1 \cup \cdots \cup P_n|$ usando il Principio di Inclusione Esclusione.

Per ogni $i = 1, \ldots, n$, in tutto n casi, la cardinalità di P_i è uguale a $(n-1)!$, in quanto le permutazioni σ ammesse sono quelle per cui $\sigma(i) = i$ e σ può permutare liberamente tutti gli elementi $j \neq i$.

Per ogni coppia $\{i, j\} \subseteq \{1, \ldots, n\}$, in tutto $\binom{n}{2}$ casi, la cardinalità di $P_i \cap P_j$ è uguale a $(n-2)!$, in quanto ogni $\sigma \in P_i \cap P_j$ deve soddisfare $\sigma(i) = i$ e $\sigma(j) = j$, ma può permutare liberamente gli altri $n-2$ elementi.

Proseguendo questo ragionamento per tutte le intersezioni possibili dei P_i, si ottiene la formula

$$\begin{aligned} |P_1 \cup \cdots \cup P_n| &= n(n-1)! - \binom{n}{2}(n-2)! + \binom{n}{3}(n-3)! + \cdots \\ &\quad \cdots + (-1)^{n-2}\binom{n}{n-1}1! + (-1)^{n-1}\binom{n}{n}0! \\ &= n!\left(\frac{1}{1!} - \frac{1}{2!} + \frac{1}{3!} + \cdots + (-1)^{n-1}\frac{1}{n!}\right). \end{aligned}$$

Per differenza, la cardinalità cercata è dunque

$$n!\left(\frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n\frac{1}{n!}\right) = n!\left(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n\frac{1}{n!}\right).$$

⟦Questo esercizio ha una suggestiva formulazione alternativa, nota come *il problema delle buste e delle lettere*. Immaginiamo che una persona affidi alla sua segretaria il compito di imbustare n lettere ad n indirizzi diversi, ma senza darle indicazioni su quale lettera corrisponda a quale indirizzo. Qual è la probabilità che nessuna delle lettere sia imbustata con l'indirizzo corretto?

È noto che la serie

$$\sum_{k=0}^{\infty}(-1)^k\frac{1}{k!}$$

converge al valore $1/e$, dove e è la costante di Nepero. Quindi la probabilità cercata tende al limite $1/e$ per n che diventa grande.⟧

Esercizio 3 Siano X un insieme di m elementi e Y un insieme di n elementi. Contare il numero di funzioni suriettive $X \longrightarrow Y$.

Soluzione Anche qui è essenziale il Principio di Inclusione Esclusione. Il numero totale di funzioni è n^m. Se contiamo il numero di funzioni *non* suriettive otteniamo, per differenza, il numero di funzioni suriettive.

Sia $Y = \{y_1, \ldots, y_n\}$. Una funzione $f\colon X \to Y$ non è suriettiva se almeno un elemento $y_i \in Y$ non fa parte dell'immagine. Altrimenti detto, le funzioni non suriettive $f\colon X \to Y$ sono l'unione degli insiemi $F_1, \ldots, F_n$, dove F_i è l'insieme delle funzioni la cui immagine non contiene l'elemento y_i.

La cardinalità degli insiemi F_i, in tutto n casi al variare di i, è uguale alla cardinalità dell'insieme delle funzioni definite su X e a valori in $Y \setminus \{y_i\}$, e quindi è

uguale a $(n-1)^m$. La cardinalità degli insiemi $F_i \cap F_j$, in tutto $\binom{n}{2}$ casi al variare di i e j, è uguale alla cardinalità dell'insieme delle funzioni definite su X e a valori in $Y \setminus \{y_i, y_j\}$, e quindi è uguale a $(n-2)^m$, e così via. In definitiva abbiamo

$$|F_1 \cup \cdots \cup F_n| = n(n-1)^m - \binom{n}{2}(n-2)^m + \cdots + (-1)^{n-1}\binom{n}{n-1}1^m$$

e, per differenza, il numero di funzioni suriettive è uguale a

$$n^m - n(n-1)^m + \binom{n}{2}(n-2)^m + \cdots + (-1)^n\binom{n}{n-1}1^m .$$

⟦È interessante, ma non ovvio, che quando $m < n$ la formula data nella soluzione produca il risultato uguale a zero, ossia confermi che non ci sono funzioni suriettive $f : X \to Y$.⟧

Esercizio 4 Siano n e k interi positivi. Determinare il numero di soluzioni dell'equazione

$$x_1 + \cdots + x_k = n ,$$

dove tutti gli x_i sono interi maggiori di zero.

Soluzione Esiste una corrispondenza biunivoca fra le soluzioni $(x_1, \ldots, x_k)$ dell'equazione data e le k–uple $(y_1, y_2, \ldots, y_k)$

$$\begin{aligned} y_1 &= x_1 \\ y_2 &= x_1 + x_2 \\ &\vdots \\ y_{k-1} &= x_1 + x_2 + \cdots + x_{k-1} \\ y_k &= x_1 + x_2 + \cdots + x_k = n. \end{aligned}$$

Poiché $y_1 < y_2 < \cdots < y_k = n$ e y_k è fissato, contare le k–uple in questione equivale a contare tutti i possibili sottoinsiemi $\{y_1, \ldots, y_{k-1}\}$ dell'insieme $\{1, \ldots, n-1\}$, che sono $\binom{n-1}{k-1}$. Pertanto la risposta cercata è $\binom{n-1}{k-1}$.

⟦Ci sono alcune varianti dell'esercizio, che si affrontano allo stesso modo. Una prima variante consiste nel considerare l'equazione

$$x_1 + \cdots + x_k \le n .$$

In questo caso, le k–uple $\{y_1, \ldots, y_k\}$ non hanno più la limitazione per cui $y_k = n$, dunque corrispondono a tutti i sottoinsiemi di k elementi di un insieme di n elementi, cioè il loro numero è $\binom{n}{k}$. Si possono anche considerare le soluzioni dell'equazione

$$x_1 + \cdots + x_k = n ,$$

dove gli x_i sono maggiori *o uguali* a zero. Ponendo $y_i = x_i + 1$ si ottiene però che $y_i > 0$, con la differenza che, essendo tutte le variabili aumentate di 1, la loro somma è aumentata

di k, ossia

$$y_1 + \cdots + y_k = n + k\,,$$

pertanto in questo caso la risposta è $\binom{n+k-1}{k-1}$.⟧

Esercizio 5 Determinare, in termini della fattorizzazione del numero intero positivo n, il numero dei divisori positivi di n.

Soluzione Sia $n = p_1^{a_1} \cdots p_k^{a_k}$ la fattorizzazione di n in primi $p_1, \ldots, p_k$ distinti. Un divisore d di n ha una fattorizzazione del tipo $d = p_1^{b_1} \cdots p_k^{b_k}$ dove gli esponenti b_i soddisfano la disuguaglianza $0 \le b_i \le a_i$. Dunque ogni esponente b_i ha $a_i + 1$ possibilità, ed il numero cercato è

$$\prod_{i=1}^{k} (a_1 + 1)\,.$$

Esercizio 6 Sia n un intero positivo, sia p un numero primo e, per un numero reale x sia $\lfloor x \rfloor$ la parte intera di x, ossia il massimo intero m tale che $m \le x$. Dimostrare che

$$\sum_{h=0}^{\infty} \left\lfloor \frac{n}{p^h} \right\rfloor$$

è l'esatta potenza di p che divide $n!$

Soluzione Osserviamo innanzitutto che la somma descritta è una somma finita, perché ovviamente, per h abbastanza grande, $\frac{n}{p^h} < 1$, e quindi $\lfloor \frac{n}{p^h} \rfloor = 0$.

Invece di contare quante volte una potenza di p divide un intero k con $1 \le k \le n$, contiamo quanti sono gli interi divisibili per p^h. Questo modo di contare permetterà di contare l'intero k per tutti gli indici h tali che $p^h \mid k$, ossia di contare esattamente l'intero k tante volte quante sono le potenze di p che lo dividono.

Con questo stratagemma abbiamo evidentemente che, per ogni h, il numero degli elementi k con $1 \le k \le n$ tali che $p^h \mid k$ è uguale a

$$\left\lfloor \frac{n}{p^h} \right\rfloor$$

e quindi la formula cercata segue.

Esercizio 7 Siano a, b, c numeri interi con a, b non entrambi nulli. Determinare l'insieme delle soluzioni $(x, y) \in \mathbb{Z}^2$ dell'equazione $ax + by = c$.

Soluzione Guardiamo innanzitutto per quali interi c l'equazione data ammette almeno una soluzione. Dall'Identità di Bezout, esiste una coppia di interi (x_0, y_0) tale che $ax_0 + by_0 = m$, dove $m = (a, b)$ è il massimo comune divisore fra a e b. Se c è un multiplo di m, diciamo $c = km$, allora moltiplicando l'equazione precedente per k si ottiene $a(kx_0) + b(ky_0) = km = c$, quindi di nuovo esiste una soluzione.

Viceversa, supponiamo che l'equazione data abbia una soluzione (x_1, y_1). Allora $ax_1 + by_1 = c$ e, poiché $m \mid a$ e $m \mid b$, allora necessariamente m deve dividere anche c. In conclusione, l'equazione data ha almeno una soluzione se e solo se $(a, b) \mid c$.

Supponiamo ora che $(a, b) \mid c$ e scriviamo $a = ma_1$, $b = mb_1$, $c = mc_1$, cosicché $(a_1, b_1) = 1$. Semplificando, l'equazione diventa $a_1x + b_1x = c_1$. Per l'Algoritmo di Euclide, sappiamo determinare una soluzione (x_0, y_0) dell'equazione $a_1x + b_1y = 1$, e quindi possiamo trovare una soluzione particolare dell'equazione $ax_1 + by_1 = c_1$: per esempio, $(x, y) = (c_1x_0, c_1y_0)$. Ora sia (x', y') una qualsiasi altra soluzione. Sottraendo termine a termine le due equazioni

$$a_1x' + b_1y' = c_1$$
$$a_1x_0 + b_1y_0 = c_1$$

otteniamo

$$a_1(x' - x_0) = b_1(y_0 - y').$$

Poiché $(a_1, b_1) = 1$, questo significa che $a_1 \mid y_0 - y'$ e $b_1 \mid x' - x_0$. Ponendo $x' - x_0 = kb_1$ per qualche intero k si ottiene che necessariamente $y' - y_0 = -ka_1$. D'altra parte, sostituendo nell'equazione originaria

$$x' = x_0 + kb_1, \quad y' = y_0 - ka_1,$$

si vede facilmente che l'equazione è verificata.

Quindi la soluzione generale dell'equazione data è

$$\begin{cases} x = x_0 + kb_1 \\ y = y_0 - ka_1. \end{cases}$$

Esercizio 8 Sia m/n un numero razionale, con $(m, n) = 1$, e sia $n = 2^e5^f n'$ con $(10, n') = 1$. Dimostrare che la scrittura decimale di m/n, dopo la virgola, è periodica, con un antiperiodo di lunghezza $\max\{e, f\}$.

Soluzione Poiché $(n', 2^e5^f) = 1$, l'equazione diofantea di primo grado

$$2^e5^f x + n'y = m$$

è risolubile; sia (a, b) una soluzione. Visto che $(m, n) = 1$, abbiamo necessariamente $(a, n') = (b, 2^e5^f) = 1$. Dividendo per n si ottiene

$$\frac{a}{n'} + \frac{b}{2^e5^f} = \frac{m}{n}.$$

Eseguiamo la Divisione Euclidea di a per n': $a = sn' + r$. Notiamo che anche $(r, n') = 1$. Le cifre dopo la virgola di a/n' sono esattamente le cifre dell'espressione decimale di r/n'. Ricordando l'usuale processo di divisione, si

ha che la $(i+1)$–esima cifra decimale di r/n' è completamente determinata dal resto della divisione di $10^i r$ per n'.

Poiché $(10, n') = 1$, la successione $(10^i)_i$ è periodica modulo n', ed anzi puramente periodica, ossia non c'è un antiperiodo, di periodo uguale all'ordine moltiplicativo h di 10 modulo n'. Moltiplicando per r, si ottiene che anche la successione $(10^i r)_i$ è puramente periodica modulo n', con un periodo h' che divide h. Posto però r' uguale all'inverso di r modulo n', si ha che la successione $(10^i r r')_i$ è puramente periodica modulo n', e quindi il suo periodo h divide h'. Ne segue che $h' = h$.

Sia ora $k = \max\{e, f\}$ e osserviamo che il numero $\beta = b/2^e 5^f$ si può scrivere anche come $b'/10^k$, con $b' \in \mathbb{Z}$, ed ha precisamente k cifre dopo la virgola, in quanto $10^k \beta \in \mathbb{Z}$, mentre $10^{k-1}\beta \notin \mathbb{Z}$.

Sommiamo a/n' e β: il primo ha una scrittura decimale puramente periodica e il secondo ha un'espressione decimale con esattamente k cifre dopo la virgola. La somma ha un'espressione decimale le cui prime k cifre formano un antiperiodo e le successive sono periodiche.

Esercizio 9 Sia g un elemento di ordine n di un gruppo G. Dimostrare che, per ogni intero k, l'ordine di g^k è uguale a $n/(k, n)$.

Soluzione Per ogni intero positivo m, si ha $(g^k)^m = e$ se e solo se $km \equiv 0 \pmod{n}$, ossia se e solo se $m \equiv 0 \pmod{n/(k,n)}$. Quindi il più piccolo intero positivo m per cui $(g^k)^m = e$ è uguale a $n/(k, n)$.

Esercizio 10 Provare che se in un gruppo abeliano esistono elementi di ordine m e n allora esistono elementi di ordine $[m, n]$.

Soluzione Sia $g \in G$ di ordine m e $h \in G$ di ordine n. Supponiamo dapprima che $(m, n) = 1$, e quindi $[m, n] = mn$; dimostriamo che $z = gh$ ha ordine mn. Infatti si ha $z^{mn} = g^{mn} h^{mn} = e \cdot e = e$, quindi $\mathrm{ord}(z) \mid mn$. Inoltre i sottogruppi di G generati rispettivamente da g e da h hanno ordini primi tra loro, quindi la loro intersezione è uguale al solo elemento neutro. Se $z^k = e$, cioè $g^k h^k = e$, allora $g^k = h^{-k}$, e dunque necessariamente $g^k = h^{-k} = e$. Ne segue che $m \mid k$ ed $n \mid k$, da cui $mn \mid k$, cioè $mn \mid \mathrm{ord}(z)$.

Vediamo ora il caso generale. Fattorizziamo m ed n

$$m = \prod_p p^{\mu_p}, \qquad n = \prod_p p^{\nu_p},$$

da cui $[m, n] = \prod_p p^{\gamma_p}$, dove $\gamma_p = \max\{\mu_p, \nu_p\}$. Per ogni primo p, p^{γ_p} divide o l'ordine di g, se $\mu_p \geq \nu_p$, o l'ordine di h, se $\mu_p < \nu_p$, quindi o nel sottogruppo generato da g o nel sottogruppo generato da h esiste un elemento z_p di ordine p^{γ_p}. Prendendo $z = \prod_p z_p$ si ottiene l'elemento cercato.

Esercizio 11 Siano p un numero primo e k un intero positivo. Per ogni a con $0 \leq a \leq k$, determinare il numero di sottogruppi di ordine p^a del gruppo additivo $(\mathbb{Z}/p\mathbb{Z})^k$.

Soluzione Il gruppo $G = (\mathbb{Z}/p\mathbb{Z})^k$ ha una naturale struttura di spazio vettoriale sul campo $\mathbb{F}_p$, in quanto la moltiplicazione per uno scalare si può definire in termini della somma: $\lambda \cdot x = x + \cdots + x$, λ volte. Analogamente, ogni sottogruppo di G ha una naturale struttura di spazio vettoriale. Per determinare i sottogruppi di G di ordine p^a basta dunque determinare i sottospazi vettoriali di $(\mathbb{Z}/p\mathbb{Z})^k$ di dimensione a.

Ogni a–upla $(v_1, \ldots, v_a)$ di vettori linearmente indipendenti genera un sottospazio di dimensione a. Il numero di a–uple ordinate di vettori linearmente indipendenti è uguale a $(p^k - 1)(p^k - p) \cdots (p^k - p^{a-1})$. Infatti v_1 può essere scelto in $p^k - 1$ modi, cioè tutti i vettori diversi da zero, v_2 in $p^k - p$ modi, cioè tutti i vettori meno i p multipli di v_1, v_3 in $p^k - p^2$ modi, cioè tutti i vettori meno le p^2 combinazioni lineari di v_1 e v_2, e così via.

D'altra parte, ogni sottospazio vettoriale di dimensione a può essere generato da un insieme ordinato di a vettori linearmente indipendenti $(v_1, \ldots, v_a)$ in $(p^a - 1)(p^a - p) \cdots (p^a - p^{a-1})$ modi. Infatti v_1 può essere scelto in $p^a - 1$ modi, tutti i vettori diversi da zero, v_2 in $p^a - p$ modi, tutti i vettori meno i p multipli di v_1, e così via.

Ne segue che il numero di sottospazi vettoriali di dimensione a di $(\mathbb{Z}/p\mathbb{Z})^k$, e quindi il numero di sottogruppi di ordine p^a, è uguale a

$$\frac{(p^k - 1)(p^k - p) \cdots (p^k - p^{a-1})}{(p^a - 1)(p^a - p) \cdots (p^a - p^{a-1})}.$$

⟦Il ragionamento della soluzione dell'esercizio implica, tra l'altro, che la frazione scritta sopra sia sempre un numero intero. Se inoltre si sostituisce a con $k - a$, non è difficile verificare che la formula dà lo stesso risultato. Un'interpretazione di questo fatto si può ottenere considerando che c'è una corrispondenza biunivoca fra i sottospazi e i loro sottospazi ortogonali, ed osservando che l'ortogonale di un sottospazio di dimensione a è un sottospazio di dimensione $k - a$.⟧

Esercizio 12 Determinare gli ordini degli elementi del gruppo simmetrico S_3 e descrivere tutti i suoi sottogruppi.

Soluzione Il gruppo S_3 ha 6 elementi, i possibili ordini sono quindi i divisori di 6. Sappiamo che S_3 non è abeliano, non ci sono quindi elementi di ordine 6 perché altrimenti S_3 sarebbe addirittura ciclico.

Ovviamente l'elemento neutro, cioè la permutazione identica, ha ordine 1. Le tre trasposizioni (12), (13) e (23) hanno ordine 2 e i due tre cicli (123) e (132) hanno ordine 3. Le permutazioni considerate finora sono già 6, esse esauriscono quindi S_3. Abbiamo cioè calcolato gli ordini di tutti gli elementi di S_3.

Sia ora G un sottogruppo di S_3. Se G ha ordine 1 o 6 allora è, rispettivamente, il gruppo banale con solo la permutazione identica o tutto S_3. Visto che per il Teorema di Lagrange l'ordine di G deve dividere 6 abbiamo solo altre due possibilità: G ha ordine 2 o G ha ordine 3.

Se G ha ordine 2 allora contiene l'elemento neutro e una trasposizione. Abbiamo quindi tre sottogruppi di ordine 2: $\{e, (12)\}$, $\{e, (13)\}$ e $\{e, (23)\}$.

Se invece G ha ordine 3 allora contiene l'elemento neutro e due elementi di ordine tre, l'unica possibilità è $G = \{e, (123), (132)\}$. Questo termina la descrizione dei sottogruppi di S_3.

Esercizio 13 Sia G un gruppo ciclico, descrivere gli omomorfismi di G in sé e determinare il gruppo degli automorfismi di G.

Soluzione Denotiamo G additivamente e sia g un suo fissato generatore. Mostriamo, per prima cosa, che la scelta del generatore g induce una corrispondenza biunivoca tra gli elementi di G e l'insieme degli omomorfismi di G.

Sia infatti h un qualsiasi elemento di G e sia φ_h la mappa definita da $\varphi_h(ng) = nh$. Osserviamo subito che, essendo g un generatore allora si deve avere $h = kg$ per qualche $k \in \mathbb{Z}$; quindi se $ng = 0$ allora si ha anche $nh = nkg = kng = k \cdot 0 = 0$. Questo prova che φ_h è ben definita. Inoltre si ha $\varphi_h(ng + mg) = \varphi_h((n + m)g) = (n + m)h = nh + mh = \varphi_h(ng) + \varphi_h(mg)$ e quindi φ_h è un omomorfismo di G.

D'altra parte, se φ è un qualsiasi omomorfismo è chiaro che $\varphi = \varphi_h$ per $h = \varphi(g)$. Questo finisce la dimostrazione che gli omomorfismi sono in corrispondenza con gli elementi di G.

Descriviamo ora gli automorfismi. Visto che $\mathrm{Im}(\varphi_h) = \langle h \rangle$, l'omomorfismo φ_h è suriettivo se e solo se h è un generatore di G.

Se G è infinito allora, usando il Teorema di Struttura dei Gruppi Ciclici $G \simeq \mathbb{Z}$, gli unici generatori di G sono allora g e $-g$. In particolare, per $h = g$ e $h = -g$, abbiamo $\varphi_h^2 = \mathrm{Id}_G$; cioè prova che φ_g e φ_{-g} sono automorfismi e che la mappa $\mathbb{Z}/2\mathbb{Z} \simeq \{\pm 1\} \ni k \longmapsto \varphi_{kg} \in \mathrm{Aut}(G)$ è un isomorfismo di gruppi.

Supponiamo infine che G sia finito, allora un omomorfismo suriettivo è anche iniettivo. In particolare, visto che i generatori di $\mathbb{Z}/n\mathbb{Z}$ sono dati dalle classi k con $(k, n) = 1$, troviamo che la mappa $(\mathbb{Z}/n\mathbb{Z})^* \ni k \longmapsto \varphi_{kg} \in \mathrm{Aut}(G)$ è un isomorfismo.

Esercizio 14 Descrivere, in termini della fattorizzazione di n, gli elementi nilpotenti di $\mathbb{Z}/n\mathbb{Z}$.

Soluzione Sia $n = p_1^{e_1} \cdots p_k^{e_k}$ la fattorizzazione di n, dove i primi $p_1, \ldots, p_k$ sono distinti e $e_i > 0$ per $i = 1, \ldots, k$. Un elemento nilpotente $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ è la classe di resto di un intero x per il quale esiste un esponente positivo m con la proprietà $x^m \equiv 0 \pmod{n}$ o, altrimenti detto, un esponente positivo m per cui $n \mid x^m$.

Poiché $p_i \mid n$ per ogni $i = 1, \ldots k$, si deve avere $p_i \mid x^m$ e, essendo p_i un numero primo, $p_i \mid x$. D'altra parte, se $p_1 \mid x, \ldots, p_k \mid x$, e quindi $p_1 \cdots p_k \mid x$, allora, scegliendo $m \geq \max\{a_1, \ldots, a_k\}$, si ha che $n \mid x^m$.

In definitiva, gli elementi nilpotenti di $\mathbb{Z}/n\mathbb{Z}$ sono tutte e sole le classi rappresentate dai multipli di $p_1 \cdots p_k$.

Esercizio 15 Sia $\mathbb{K}$ un campo di caratteristica diversa da 2. Dimostrare che

(i) ogni estensione di $\mathbb{K}$ di grado 2 è della forma $\mathbb{K}(\sqrt{a})$ per qualche $a \in \mathbb{K}$;

(ii) se $[\mathbb{K}(\sqrt{a}) : \mathbb{K}] = [\mathbb{K}(\sqrt{b}) : \mathbb{K}] = 2$, allora $\mathbb{K}(\sqrt{a}) = \mathbb{K}(\sqrt{b})$ se e solo se ab è il quadrato di un elemento di $\mathbb{K}$.

Soluzione (i) Un'estensione $\mathbb{F}$ di grado 2 di $\mathbb{K}$ è della forma $\mathbb{F} = \mathbb{K}(\alpha)$ dove α è un numero algebrico il cui polinomio mimino su $\mathbb{K}$ ha grado 2. Supponiamo che il polinomio minimo di α su $\mathbb{K}$ sia $\mu_\alpha(x) = x^2 + rx + s$. Poiché la caratteristica di $\mathbb{K}$ è diversa da 2, le soluzioni dell'equazione $\mu_\alpha(x) = 0$ possono essere calcolate con la formula risolutiva

$$x_1, x_2 = \frac{-r \pm \sqrt{r^2 - 4s}}{2},$$

visto che 2 è un elemento invertibile. A questo punto è ovvio che, ponendo $a = r^2 - 4s$, le soluzioni dell'equazione data sono contenute in $\mathbb{K}(\sqrt{a})$.

(ii) Dimostriamo innanzitutto che, se $\mathbb{K}(\sqrt{a}) = \mathbb{K}(\sqrt{b})$, allora ab è il quadrato di un elemento di $\mathbb{K}$. Poiché, in particolare, $\mathbb{K}(\sqrt{a}) \subseteq \mathbb{K}(\sqrt{b})$, esistono elementi $c, d \in \mathbb{K}$ tali che $\sqrt{a} = c + d\sqrt{b}$. Elevando al quadrato, si ottiene

$$a = c^2 + d^2 b + 2cd\sqrt{b}.$$

Per l'indipendenza lineare su $\mathbb{K}$ degli elementi 1 e $\sqrt{b}$, e poiché la caratteristica di K è diversa da 2, si deve avere $cd = 0$, e quindi $c = 0$ oppure $d = 0$. Se $c = 0$ si ha $a = d^2 b$ da cui $ab = d^2 b^2$, e quindi la tesi. Se $d = 0$ si ha $a = c^2$, contro l'ipotesi che il grado $[\mathbb{K}(\sqrt{a}) : \mathbb{K}]$ sia uguale a 2.

Viceversa, supponiamo che ab sia il quadrato di un elemento di $\mathbb{K}$, ossia $ab = c^2$ con $c \in \mathbb{K}$. Per le ipotesi fatte, a e b sono diversi da zero, quindi $\sqrt{a} = \pm\frac{c}{\sqrt{b}} \in \mathbb{K}(\sqrt{b})$ e $\sqrt{b} = \pm\frac{c}{\sqrt{a}} \in \mathbb{K}(\sqrt{a})$.

Esercizio 16 Per ogni intero positivo k sia $f_k(x) = x^k - 1 \in \mathbb{Q}[x]$. Dimostrare che per ogni $m, n > 0$ il massimo comune divisore tra $f_m(x)$ e $f_n(x)$ è uguale a $f_d(x)$ dove d è il massimo comune divisore tra m e n.

Soluzione Sia $d = (n, m)$; poniamo $m = da$ e $n = db$. Chiaramente

$$x^d \equiv 1 \pmod{x^d - 1}$$

e, elevando ambo i membri di questa congruenza sia alla a che alla b, otteniamo $x^m \equiv (x^d)^a \equiv 1 \pmod{x^d - 1}$ e $x^n \equiv (x^d)^b \equiv 1 \pmod{x^d - 1}$, quindi $x^d - 1 \mid (x^m - 1, x^n - 1)$.

Viceversa, sia $f(x) = (x^m - 1, x^n - 1)$. Per ogni $\alpha \in \mathbb{C}$ radice di $f(x)$ sia ha che α è radice sia di $x^m - 1$ che di $x^n - 1$, quindi $\alpha^m = \alpha^n = 1$. Da questo si deduce che l'ordine moltiplicativo di α divide sia m che n, e quindi divide il loro massimo comune divisore d, cioè ogni radice di $f(x)$ è anche radice di $x^d - 1$. Per il Criterio della Derivata $x^m - 1$ non ha radici multiple, e quindi neanche il polinomio $f(x)$ ha radici multiple; otteniamo allora che $f(x) \mid x^d - 1$. Quindi $f(x)$ e $x^d - 1$ si dividono reciprocamente, ed essendo entrambi monici, coincidono.

Esercizio 17 Sia $f(x) = x^2 + a$ un polinomio con coefficienti razionali e sia $\overline{f}(x)$ la sua classe nell'anello $\mathbb{Q}[x]/(x^3 - x^2)$. Determinare i valori di a per cui $\overline{f}(x)$ è invertibile e calcolarne l'inverso.

Soluzione Sappiamo che la classe di $f(x)$ è invertibile in $A = \mathbb{Q}[x]/(x^3 - x^2)$ se e solo se il massimo comune divisore tra $f(x)$ e $x^3 - x^2$ è 1. Poiché $x^3 - x^2 = x^2(x-1)$, questo polinomio è coprimo con $f(x)$ se e solo se 0 e 1 non sono radici di $f(x)$. Imponiamo quindi $f(0) = a \neq 0$ e $f(1) = a + 1 \neq 0$. Quindi $\overline{f}(x)$ è invertibile in A se e solo se $a \neq 0, -1$, mentre per $a = 0$ o $a = -1$ esso è un divisore di zero.

Sia quindi $a \neq 0, -1$ e, per calcolare l'inverso di $\overline{f}(x)$, usiamo l'Algoritmo di Euclide. Si ha

$$x^3 - x^2 = (x^2 + a)(x-1) - a(x-1)$$

$$x^2 + a = a(x-1)\left(\frac{1}{a}x + \frac{1}{a}\right) + a + 1$$

da cui si ricava

$$\begin{aligned} a + 1 &= (x^2 + a) - a(x-1)\left(\frac{1}{a}x + \frac{1}{a}\right) \\ &= (x^2 + a)\left(1 - \frac{1}{a}(x^2 - 1)\right) + \frac{1}{a}(x+1)(x^3 - x^2) \end{aligned}$$

e quindi

$$(x^2 + a)\left(-\frac{1}{a(a+1)}x^2 + \frac{1}{a}\right) \equiv 1 \pmod{x^3 - x^2}.$$

Concludiamo che l'inverso di $\overline{f}(x)$ in A è la classe di

$$-\frac{1}{a(a+1)}x^2 + \frac{1}{a}.$$

Esercizio 18 Sia p un numero primo diverso da 2. Dimostrare che

(i) gli elementi $a \in \mathbb{F}_p^*$ che sono quadrati di un elemento di $\mathbb{F}_p^*$ formano un sottogruppo di $\mathbb{F}_p^*$ di ordine $(p-1)/2$;

(ii) il simbolo di Legendre

$$\mathbb{F}_p^* \ni a \longmapsto \left(\frac{a}{p}\right) \in \{\pm 1\}$$

è un omomorfismo suriettivo di gruppi, in particolare il prodotto di due non quadrati è un quadrato;

(iii) -1 è il quadrato di un elemento di $\mathbb{F}_p^*$ se e solo se $p \equiv 1 \pmod 4$, cioè vale

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Soluzione (i) Consideriamo l'applicazione $\mathbb{F}_p^* \ni a \overset{f}{\longmapsto} a^2 \in \mathbb{F}_p^*$. Essa è evidentemente un omomorfismo, in quanto $f(ab) = (ab)^2 = a^2 b^2 = f(a) f(b)$. Il nucleo

di f è costituito dall'insieme $\{a \in \mathbb{F}_p^* \mid a^2 = 1\}$; poiché $\mathbb{F}_p$ è un campo, le uniche soluzioni di $x^2 = 1$ sono ± 1, troviamo quindi $\mathrm{Ker}(f) = \{\pm 1\}$. Per il Teorema di Omomorfismo, l'immagine è dunque un sottogruppo di $\mathbb{F}_p^*$ di ordine $(p-1)/2$. Questo risponde alla domanda posta in quanto $\mathrm{Im}(f)$ è formata dagli elementi che sono quadrati in $\mathbb{F}_p^*$.

(ii) Abbiamo visto nel punto precedente che il sottoinsieme Q dei quadrati in $\mathbb{F}_p^*$ è un sottogruppo di ordine $(p-1)/2$. Il quoziente $\mathbb{F}_p^*/Q$ ha quindi due elementi e la composizione $\mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*/Q \longrightarrow \{\pm 1\}$ è un omomorfismo di gruppi. Questa composizione è chiaramente

$$\mathbb{F}_p^* \ni a \longmapsto \left(\frac{a}{p}\right) \in \{\pm 1\}.$$

Troviamo quindi che il simbolo di Legendre è moltiplicativo e, in particolare, il prodotto di due non residui quadratici è un residuo quadratico.

(iii) Supponiamo che esista $a \in \mathbb{F}_p^*$ tale che $a^2 = -1$, allora $a^4 = (-1)^2 = 1$, quindi a ha ordine divisore di 4. Ma d'altra parte l'ordine di a non può essere minore di 4 visto che $a^2 = -1 \neq 1$. Ne segue che 4 deve dividere l'ordine del gruppo, ossia $4 \mid p-1$.

Viceversa, supponiamo che $4 \mid p-1$. Poiché $\mathbb{F}_p^*$ è un gruppo ciclico di ordine $p-1$, $\mathbb{F}_p^*$ possiede un sottogruppo ciclico di ordine d per ogni divisore d di $p-1$. In particolare, $\mathbb{F}_p^*$ possiede un sottogruppo ciclico di ordine 4 e quindi un elemento a di ordine 4. Se a ha ordine 4, allora $b = a^2 \neq 1$, ma d'altra parte $b^2 = a^4 = 1$, quindi necessariamente $b = -1$ perché -1 è l'unico elemento di ordine 2 di $\mathbb{F}_p^*$.

Esercizio 19 Fattorizzare il polinomio $x^8 - 1$ in $\mathbb{K}[x]$ per $\mathbb{K} = \mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{F}_{17}$ e $\mathbb{F}_{43}$.

Soluzione Osserviamo che, se $\mathbb{K} \subseteq \mathbb{F}$ sono due campi uno contenuto nell'altro, ogni decomposizione di un polinomio in $\mathbb{K}[x]$ vale anche in $\mathbb{F}[x]$. Dunque la fattorizzazione in $\mathbb{F}[x]$ è un raffinamento della fattorizzazione in $\mathbb{K}[x]$. Altrimenti detto, la fattorizzazione in $\mathbb{K}[x]$ si ottiene raggruppando alcuni fattori della fattorizzazione in $\mathbb{F}[x]$.

Osserviamo inoltre che ogni decomposizione di un polinomio in $\mathbb{Z}[x]$ vale anche in $(\mathbb{Z}/m\mathbb{Z})[x]$ per ogni intero positivo m.

Per il Teorema Fondamentale dell'Algebra, in $\mathbb{C}[x]$ il polinomio si spezza in fattori lineari, corrispondenti alle 8 radici ottave dell'unità. Detta ζ una radice ottava primitiva, cioè di ordine esattamente uguale a 8 come, ad esempio, $\zeta = (1+i)/\sqrt{2}$, la fattorizzazione in $\mathbb{C}[x]$ è

$$x^8 - 1 = \prod_{h=0}^{7} (x - \zeta^h).$$

Ogni polinomio a coefficienti reali che ha una radice complessa ha anche la radice complessa coniugata. Pertanto, a partire dalla fattorizzazione in $\mathbb{C}[x]$, i fattori $x-1$ e $x+1$, corrispondenti alle due radici reali, rimangono invariati in $\mathbb{R}[x]$, mentre,

per ottenere un polinomio a coefficienti reali, bisogna moltiplicare fra loro i fattori corrispondenti a radici complesse coniugate. Otteniamo

$$\begin{aligned}(x-\zeta)(x-\zeta^{-1}) &= x^2-\sqrt{2}x+1,\\ (x-\zeta^2)(x-\zeta^{-2}) &= x^2+1,\\ (x-\zeta^3)(x-\zeta^{-3}) &= x^2+\sqrt{2}x+1.\end{aligned}$$

Pertanto la fattorizzazione in $\mathbb{R}[x]$ è

$$x^8-1=(x-1)(x+1)(x^2-\sqrt{2}x+1)(x^2+1)(x^2+\sqrt{2}x+1).$$

I fattori $x-1, x+1$ e x^2+1 sono a coefficienti razionali e irriducibili in $\mathbb{R}[x]$; a maggior ragione, sono irriducibili anche in $\mathbb{Q}[x]$. Invece, poiché i fattori $x^2-\sqrt{2}x+1$ e $x^2+\sqrt{2}x+1$ non sono a coefficienti razionali, essi vanno raggruppati, ottenendo $(x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1)=x^4+1$. Pertanto la fattorizzazione in $\mathbb{Q}[x]$ è

$$x^8-1=(x-1)(x+1)(x^2+1)(x^4+1).$$

Per il Lemma di Gauss, un polinomio primitivo è irriducibile in $\mathbb{Z}[x]$ se e solo se lo è in $\mathbb{Q}[x]$, pertanto le fattorizzazioni di x^8-1 in $\mathbb{Z}[x]$ e in $\mathbb{Q}[x]$ coincidono.

Consideriamo ora il campo $\mathbb{K}=\mathbb{F}_{17}$. Il gruppo moltiplicativo di $\mathbb{K}$ è ciclico di ordine 16, quindi ha uno e un solo sottogruppo ciclico di ordine 8. Un elemento $\alpha\in\mathbb{K}^*$ appartiene a questo sottogruppo se e solo se $\alpha^8=1$; quindi il polinomio x^8-1 ha 8 radici in $\mathbb{F}_{17}$, che sono gli elementi di questo sottogruppo ciclico. Con facili conti, si vede che un generatore di questo gruppo ciclico è la classe di resto di 2 modulo 17. Si ottiene la fattorizzazione

$$x^8-1=(x-2)(x-4)(x-8)(x+1)(x+2)(x+4)(x+8)(x-1).$$

Infine, consideriamo il caso $\mathbb{K}=\mathbb{F}_{43}$. Sicuramente, data la fattorizzazione in $\mathbb{Z}[x]$, abbiamo la decomposizione $x^8-1=(x-1)(x+1)(x^2+1)(x^4+1)$. Il polinomio x^2+1 rimane irriducibile in $\mathbb{K}$; esso non ha infatti radici visto che una sua radice dovrebbe avere ordine 4 in $\mathbb{K}^*$, ma 4 non divide 42 che è l'ordine di $\mathbb{K}^*$.

A maggior ragione il polinomio x^4+1 non ha radici perché una sua radice dovrebbe avere ordine 8. Osserviamo invece che $\mathbb{F}^*_{43^2}$ ha ordine divisibile per 8 e contiene quindi tutte le radici di x^8-1. Il grado del campo di spezzamento di un polinomio a coefficienti in un campo finito è il minimo comune multiplo dei gradi dei suoi fattori irriducibili, quindi i fattori irriducibili di x^4+1 devono avere grado 2.

Per calcolare esplicitamente la fattorizzazione imponiamo che

$$x^4+1=(x^2+ax+b)(x^2+cx+d)$$

per certi $a, b, c, d \in \mathbb{K}$. Uguagliando i coefficienti dei polinomi di sinistra e di destra otteniamo

$$\begin{cases} a + c = 0 \\ b + ac + d = 0 \\ ad + bc = 0 \\ bd = 1 \end{cases}$$

e, sostituendo $c = -a$,

$$\begin{cases} b + d - a^2 = 0 \\ a(d - b) = 0 \\ bd = 1. \end{cases}$$

La seconda equazione di quest'ultimo sistema dà due possibilità: $a = 0$ oppure $d = b$. Se $a = 0$, allora $b + d = 0$ e $bd = 1$, e cioè $(x - b)(x - d) = x^2 + 1$; ma, come già visto, l'equazione $x^2 + 1$ non ha soluzioni in $\mathbb{K}$, e quindi questo caso va escluso. Se $d = b$, otteniamo $2b - a^2 = 0$ e $b^2 = 1$, cioè $b = \pm 1$ e $a^2 = \pm 2$.

Osserviamo ora che $2^7 = 128 \equiv -1 \pmod{43}$, da cui $(-2)^8 \equiv -2 \pmod{43}$ e quindi $a = \pm 16$ è soluzione del sistema e abbiamo $d = b = 1$ e $c = \mp 16$; questi valori corrispondono alla fattorizzazione $x^4 + 1 = (x^2 + 16x - 1)(x^2 - 16x - 1)$. È ora chiaro che il sistema per $b = -1$, cioè $a^2 = 2$, non ha soluzioni in quanto non possono esserci 4 fattori di secondo grado di $x^4 + 1$ visto che la fattorizzazione è unica.

Concludiamo che la fattorizzazione di $x^8 - 1$ in $\mathbb{F}_{43}$ è

$$x^8 - 1 = (x - 1)(x + 1)(x^2 + 1)(x^2 + 16x - 1)(x^2 - 16x - 1).$$

⟦Possiamo provare che $a^2 = 2$ non ha alcuna soluzione in $\mathbb{F}_{43}$ anche nel seguente modo. Da $2^7 \equiv -1 \pmod{43}$ troviamo che l'ordine di 2 in $\mathbb{F}_{43}^*$ è 14. Ma allora 2 non è un quadrato in $\mathbb{F}_{43}$ in quanto i quadrati non nulli sono l'immagine dell'omomorfismo $\mathbb{F}_{43}^* \ni x \longmapsto x^2 \in \mathbb{F}_{43}^*$ che ha ordine $(43 - 1)/2 = 21$, non divisibile per 14.⟧

Esercizio 20 Sia $\mathbb{K}$ un campo e sia $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{K}[x]$ un polinomio di grado n; chiamiamo *reciproco* di $f(x)$ il polinomio $\hat{f}(x) = a_0 x^n + \cdots + a_n$. Dimostrare che se $f(0) \neq 0$ allora vale: $f(x)$ è irriducibile in $\mathbb{K}[x]$ se e solo se $\hat{f}(x)$ è irriducibile in $\mathbb{K}[x]$.

Soluzione Supponiamo nel seguito che tutti i polinomi considerati abbiano termine noto non nullo.

Osserviamo per prima cosa che si ha $\hat{f}(x) = x^n f(1/x)$ con $n = \deg f$; da ciò segue subito che il reciproco di $f(x)g(x)$ è $\hat{f}(x)\hat{g}(x)$. Inoltre $\deg(\hat{f}(x)) = \deg(f)$ e $\hat{\hat{f}}(x) = f(x)$.

L'enunciato da dimostrare è equivalente al seguente: $f(x)$ è riducibile in $\mathbb{K}[x]$ se e solo se $\hat{f}(x)$ è riducibile in $\mathbb{K}[x]$. Supponiamo dunque che $f(x)$ sia riducibile, $f(x) = g(x)h(x)$; ma allora anche $\hat{f}(x) = \hat{g}(x)\hat{h}(x)$ è riducibile.

L'implicazione inversa è conseguenza di $\hat{\hat{f}}(x) = f(x)$.

Esercizio 21 Determinare tutti i polinomi irriducibili in $\mathbb{F}_2[x]$ di grado minore o uguale a 5.

Soluzione I polinomi di grado 1 sono chiaramente irriducibili e sono x e $x+1$.

Osserviamo che in $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ le possibili radici di un polinomio sono solo 0 e 1. Ora un polinomio ha 0 come radice se e solo se ha termine noto nullo e, in $\mathbb{F}_2$ ha 1 come radice se e solo se è somma di un numero pari di monomi. Poiché i polinomi di grado 2 e di grado 3 sono irriducibili se e solo se non hanno radici, da quanto osservato otteniamo che i polinomi irriducibili di grado 2 e di grado 3 sono quelli che hanno termine noto 1 e un numero dispari di monomi, quindi x^2+x+1, x^3+x+1 e x^3+x^2+1.

Un polinomio di grado 4 o 5 è irriducibile se non ha radici e non ha fattori irriducibili di secondo grado. Per quanto detto sopra, i polinomi di quarto grado che non hanno radici sono $x^4+x^3+x^2+x+1$, x^4+x^3+1, x^4+x+1 e x^4+x^2+1. Per ottenere quelli irriducibili occorre escludere quelli che sono prodotto di polinomi irriducibili di secondo grado: poiché ne esiste solo uno, l'unico polinomio da escludere dalla lista data è $(x^2+x+1)^2 = x^4+x^2+1$. I polinomi irriducibili di grado 4 sono quindi $x^4+x^3+x^2+x+1$, x^4+x^3+1 e x^4+x+1.

Analogamente per il grado 5, quelli che non hanno radici sono i polinomi di grado 5 con termine noto 1 e un numero dispari di monomi. Per ottenere gli irriducibili occorre togliere da questi quelli che sono il prodotto di x^2+x+1 e di un polinomio irriducibile di terzo grado, cioè $(x^2+x+1)(x^3+x+1) = x^5+x^4+1$ e $(x^2+x+1)(x^3+x^2+1) = x^5+x+1$. I polinomi irriducibili di grado 5 sono quindi $x^5+x^3+x^2+x+1$, $x^5+x^4+x^2+x+1$, $x^5+x^4+x^3+x+1$, $x^5+x^4+x^3+x^2+1$, x^5+x^3+1 e x^5+x^2+1.

Esercizio 22 Contare i polinomi irriducibili in $\mathbb{F}_2[x]$ di grado minore o uguale a 6.

Soluzione Indichiamo con $\overline{\mathbb{F}_2}$ una fissata chiusura algebrica di $\mathbb{F}_2$. Le radici dei polinomi irriducibili di grado d di $\mathbb{F}_2[x]$ in $\overline{\mathbb{F}_2}$ sono esattamente gli elementi di grado d di $\overline{\mathbb{F}_2}$, cioè gli elementi del campo $\mathbb{F}_{2^d}$ che non stanno in nessun suo sottocampo proprio. Poiché un polinomio irriducibile di grado d di $\mathbb{F}_2$ ha d radici distinte in $\overline{\mathbb{F}_2}$, possiamo calcolare il numero dei polinomi irriducibili di grado 2 usando il Principio di Inclusione Esclusione. In particolare, indicando con n_d il numero dei polinomi irriducibili di grado d troviamo

$$
\begin{aligned}
n_1 &= |\mathbb{F}_2| = 2,\\
n_2 &= \frac{1}{2}|\mathbb{F}_{2^2} \setminus \mathbb{F}_2| = \frac{2^2-2}{2} = 1,\\
n_3 &= \frac{1}{3}|\mathbb{F}_{2^3} \setminus \mathbb{F}_2| = \frac{2^3-2}{3} = 2,\\
n_4 &= \frac{1}{4}|\mathbb{F}_{2^4} \setminus \mathbb{F}_{2^2}| = \frac{2^4-2^2}{4} = 3,\\
n_5 &= \frac{1}{5}|\mathbb{F}_{2^5} \setminus \mathbb{F}_2| = \frac{2^5-2}{5} = 6,
\end{aligned}
$$

$$n_6 = \frac{1}{6}|\mathbb{F}_{2^6} \setminus (\mathbb{F}_{2^3} \cup \mathbb{F}_{2^2})| = \frac{(2^6 - (2^3 + 2^2 - 2))}{6} = 9.$$

Esercizio 23 Fattorizzare i seguenti polinomi a coefficienti razionali
(i) $f(x) = 4x^3 + 11x^2 + 19x + 21$;
(ii) $g(x) = x^4 + 8x^2 - 5$.

Soluzione (i) Il polinomio $f(x)$ è di terzo grado e quindi è riducibile se e solo se ammette una radice. Una eventuale radice razionale di $f(x)$ deve essere della forma a/b dove a è un divisore di 21 e b è un divisore di 4. Quindi le possibili radici sono

$$\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm 3, \pm\frac{3}{2}, \pm\frac{3}{4}, \pm 7, \pm\frac{7}{2}, \pm\frac{7}{4}, \pm 21, \pm\frac{21}{2}, \pm\frac{21}{4}.$$

Sostituendo questi valori, si ottiene che effettivamente $f(-7/4) = 0$. Per il Teorema di Ruffini, il polinomio è divisibile in $\mathbb{Q}[x]$ per $x + 7/4$. Ma $f(x)$ è a coefficienti interi e, per il Lemma di Gauss, se è divisibile per un polinomio a coefficienti razionali di primo grado è anche divisibile per un polinomio a coefficienti interi di primo grado, ottenuto dal primo eliminando i denominatori, ossia, è divisibile per $4x + 7$. Eseguendo la divisione, si ottiene

$$4x^3 + 11x^2 + 19x + 21 = (4x + 7)(x^2 + x + 3).$$

Poiché il polinomio $x^2 + x + 3$ non ha radici razionali, la formula precedente è la fattorizzazione del polinomio $f(x)$ in $\mathbb{Q}[x]$.

(ii) Innanzitutto cerchiamo se ci sono radici razionali del polinomio. Analogamente al punto precedente, le eventuali radici possono essere soltanto $\pm 1, \pm 5$. Sostituendo a x questi valori, però, non si ottiene mai $g(x) = 0$, per cui il polinomio $g(x)$ non ha radici razionali; equivalentemente, per il Teorema di Ruffini, $g(x)$ non ha fattori irriducibili di primo grado.

Per cercare gli eventuali fattori di secondo grado, si può sfruttare che il polinomio è biquadratico. Ponendo $y = x^2$ si trova che le radici del polinomio $y^2 + 8y - 5$ sono $-4 \pm \sqrt{21}$, e dunque le radici di $g(x)$ sono

$$\pm\sqrt{-4 + \sqrt{21}}, \quad \pm\sqrt{-4 - \sqrt{21}} = \pm i\sqrt{4 + \sqrt{21}}.$$

Le prime due radici sono reali, le altre due sono immaginarie pure, e complesse coniugate. Dunque un eventuale fattore irriducibile di grado 2 di $g(x)$ in $\mathbb{Q}[x]$, che in particolare deve appartenere a $\mathbb{R}[x]$, deve avere entrambe le radici complesse coniugate, e quindi dovrebbe essere

$$(x - i\sqrt{4 + \sqrt{21}})(x + i\sqrt{4 + \sqrt{21}}) = x^2 + 4 + \sqrt{21}.$$

Ma questo polinomio non ha coefficienti razionali, pertanto non può essere un fattore di $g(x)$ in $\mathbb{Q}[x]$. Concludiamo che $g(x)$ è irriducibile in $\mathbb{Q}[x]$.

Esercizio 24 Fattorizzare il polinomio $f(x) = x^4 + x^3 + x^2 + 1$ in $\mathbb{Q}[x]$.

Soluzione Per il Lemma da Gauss $f(x)$ è irriducibile in $\mathbb{Q}[x]$ se e solo se lo è in $\mathbb{Z}[x]$. Una fattorizzazione di $f(x)$ in $\mathbb{Z}[x]$ si proietta in uno spezzamento, in fattori non necessariamente irriducibili, modulo p, per ogni p numero primo. Modulo 2 la classe di $f(x)$ si fattorizza come $(x+1)(x^3+x+1)$ ed entrambi i fattori scritti sono irriducibili in $(\mathbb{Z}/2\mathbb{Z})[x]$. Otteniamo che $f(x)$ in $\mathbb{Z}[x]$ ha una radice, oppure è irriducibile. Le possibili radici sono ± 1, ma $f(\pm 1) \neq 0$, quindi $f(x)$ è irriducibile.

Esercizio 25 Determinare il polinomio minimo di α^2 su un campo $\mathbb{K}$ conoscendo il polinomio minimo di α.

Soluzione Sia n il grado di α su $\mathbb{K}$. Dalla formula del prodotto dei gradi per le estensioni finite dei campi, abbiamo $[\mathbb{K}(\alpha) : \mathbb{K}] = [\mathbb{K}(\alpha) : \mathbb{K}(\alpha^2)][\mathbb{K}(\alpha^2) : \mathbb{K}]$. Poiché α soddisfa l'equazione $x^2 - \alpha^2 = 0$ su $\mathbb{K}(\alpha^2)$, il primo dei due fattori è uguale a 1 o a 2, e il secondo dei due fattori è uguale a n o a $n/2$.

Sia $\mu_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ il polinomio minimo di α su $\mathbb{K}$. Distinguendo i termini con esponente pari o dispari, possiamo scrivere $\mu_\alpha(x) = p(x^2) + xd(x^2)$, dove $p(x^2)$ è la somma dei termini di $\mu_\alpha(x)$ di grado pari e $xd(x^2)$ è la somma dei termini di $\mu_\alpha(x)$ di grado dispari.

Distinguiamo due casi.

(1) Il polinomio $d(x)$ è nullo, quindi $\mu_\alpha(x) = p(x^2)$. Abbiamo $p(\alpha^2) = 0$ e $\deg p = n/2$, quindi $p(x)$ è il polinomio minimo di α^2 su $\mathbb{K}$.

(2) Il polinomio $d(x)$ non è nullo. In questo caso $\alpha = -p(\alpha^2)/d(\alpha^2)$, quindi α^2 ha grado n su $\mathbb{K}$ perché $\mathbb{K}(\alpha) \subseteq \mathbb{K}(\alpha^2) \subseteq \mathbb{K}(\alpha)$.

Osserviamo che il polinomio

$$g(x^2) = (p(x^2) - xd(x^2))(p(x^2) + xd(x^2)) = p(x^2)^2 - x^2 d(x^2)^2$$

si annulla in α e ha grado $2n$; quindi $g(x)$ è un polinomio che si annulla in α^2 e ha grado n, inoltre il suo primo coefficiente è uguale a $(-1)^n$. Ne segue che il polinomio minimo di α^2 su $\mathbb{K}$ è $(-1)^n g(x)$.

Capitolo 2
Esercizi

2.1 Successioni

1. Sia $a_0, a_1, a_2, \ldots$ la successione definita per ricorrenza da

$$\begin{cases} a_0 = 2,\ a_1 = 3; \\ a_{n+1} = \dfrac{a_n + a_{n-1}}{6} \quad \text{per } n \geq 1. \end{cases}$$

(i) Dimostrare che per ogni $n \geq 2$ si ha $a_n = b_n/6^{n-1}$ con $b_n \equiv -1 \pmod 6$.
(ii) Per $n \geq 0$, sia $c_n = 5a_n + (-1)^n 4/3^{n-1}$. Dimostrare che per ogni $n \geq 0$ si ha $c_n = 22 \cdot 2^{-n}$.

2. Sia $a_0, a_1, a_2, \ldots$ la successione definita da

$$\begin{cases} a_0 = 0,\ a_1 = 1; \\ a_{n+1} = 5a_n - 6a_{n-1} \quad \text{per } n \geq 1. \end{cases}$$

Dimostrare che
(i) $(a_n, 6) = 1$ per ogni $n > 0$;
(ii) $5 \mid a_n$ se e solo se n è pari.

3. Sia $a_1, a_2, a_3, \ldots$ la successione definita da

$$\begin{cases} a_1 = 1,\ a_2 = 2; \\ a_{n+1} = \dfrac{1}{2}a_n + a_{n-1} \quad \text{per } n \geq 2. \end{cases}$$

(i) Dimostrare che $a_{n+1} \geq a_n$ per ogni $n \geq 1$.
(ii) Dimostrare che $a_{2n+2} = 9a_{2n}/4 - a_{2n-2}$ per ogni $n \geq 2$.

4. Si consideri la successione $a_0, a_1, a_2, \ldots$ definita per ricorrenza da

$$\begin{cases} a_0 = 2,\ a_1 = 1; \\ a_{n+1} = a_n + a_{n-1} \quad \text{per } n \geq 1. \end{cases}$$

R. Chirivì et al., *Esercizi scelti di Algebra, Volume 1*,
UNITEXT – La Matematica per il 3+2 107, DOI 10.1007/978-88-470-3961-2_2

Dimostrare che
(i) $a_0^2 + a_1^2 + \cdots + a_n^2 = a_n a_{n+1} + 2$ per ogni $n \geq 0$;
(ii) a_n è pari se e solo se $n \equiv 0 \pmod 3$.

5. Sia $k > 0$ un numero naturale. Dimostrare che esiste un'unica successione di numeri reali $a_0, a_1, a_2, \ldots$ che soddisfa le condizioni

$$\begin{cases} a_0 = 0,\ a_k = 1; \\ a_{n+1} = a_n + a_{n-1} \quad \text{per } n \geq 1 \end{cases}$$

e dimostrare che per questa successione si ha $a_1 = 1/F_k$, dove F_k è il k–esimo numero di Fibonacci.

6. Sia $a_0, a_1, a_2, \ldots$ la successione definita da

$$\begin{cases} a_0 = 9,\ a_1 = 12,\ a_2 = 38; \\ a_{n+2} = 7a_n - 6a_{n-1} \qquad \text{per } n \geq 1. \end{cases}$$

(i) Determinare per quali valori di n si ha $3 \mid a_n$.
(ii) Determinare per quali valori di n si ha $a_{n+1} > a_n$.

7. Definiamo induttivamente $a_0 = 31$, $a_{n+1} = a_n^3$ per $n \geq 0$. Si dimostri che esiste un intero positivo k tale che, per ogni n, $a_{n+k} \equiv a_n \pmod{44}$ e si determini il minimo valore possibile per k.

8. Sia $k \in \mathbb{N}$ e sia $a_1, a_2, a_3, \ldots$ la successione di numeri naturali definita da

$$\begin{cases} a_1 = k, \\ a_{n+1} = a_n + (202, a_n) \quad \text{per } n \geq 1. \end{cases}$$

Dimostrare che esiste un $n_0 \in \mathbb{N}$ tale che per ogni $n \geq n_0$ si ha $202 \mid a_n$.

9. Sia a un numero intero non divisibile per 3 e sia $a_0, a_1, a_2 \ldots$ la successione definita per ricorrenza da

$$\begin{cases} a_0 = 1,\ a_1 = a; \\ a_{n+1} = 5a_n + 3a_{n-1} \quad \text{per } n \geq 1. \end{cases}$$

Dimostrare che $(a_{n+1}, a_n) = 1$ per ogni $n \geq 1$.

10. Per ogni intero $n \geq 0$, sia $a_n = 3^n + 5^n$.
(i) Determinare dei numeri reali h, k tali che $a_{n+1} = ha_n + ka_{n-1}$ per ogni $n \geq 1$.
(ii) Determinare se esistono degli interi positivi n tali che $7 \mid a_n$.

11. Sia $a_0, a_1, a_2, \ldots$ la successione definita da

$$\begin{cases} a_0 = 2,\ a_1 = 3,\ a_2 = 5; \\ a_{n+1} = a_n - a_{n-1} + 2a_{n-2} \quad \text{per } n \geq 2. \end{cases}$$

Dimostrare che $a_n < a_{n+1}$ per ogni $n \geq 0$.

12. Siano h, k numeri interi con $(h, k) = 1$ e sia $a_0, a_1, a_2 \dots$ la successione definita da

$$\begin{cases} a_0 = 1,\ a_1 = 1; \\ a_{n+1} = ha_n + ka_{n-1} \quad \text{per } n \geq 1. \end{cases}$$

(i) Dimostrare che $(a_n, a_{n+1}) = 1$ per ogni $n \geq 0$.

(ii) Posto $h = 35$ e $k = 71$, determinare il massimo comune divisore di tutti i numeri dell'insieme $\{a_n^2 - 1 \mid n = 0, 1, 2, \dots\}$.

13. Indicata con F_n la successione dei numeri di Fibonacci dimostrare che, per ogni $n \geq 0$,

(i) $\binom{n}{0}F_1 + \binom{n}{1}F_2 + \cdots + \binom{n}{n-1}F_n + \binom{n}{n}F_{n+1} = F_{2n+1}$;

(ii) $\binom{n}{1}F_1 + \binom{n}{2}F_2 + \cdots + \binom{n}{n-1}F_{n-1} + \binom{n}{n}F_n = F_{2n}$.

14. Si consideri la successione $a_1, a_2, a_3, \dots$ di numeri naturali così definita

$$\begin{cases} a_1 = 1,\ a_2 = 4; \\ a_{n+1} = a_n + 3a_{n-1} \quad \text{per } n \geq 2. \end{cases}$$

(i) Dimostrare che esistono delle costanti reali α, β tali che, per ogni $n \geq 1$,

$$a_n = \alpha\left(\frac{1+\sqrt{13}}{2}\right)^n + \beta\left(\frac{1-\sqrt{13}}{2}\right)^n.$$

(ii) Determinare tutti i valori di n per cui a_n è un numero pari.

2.2 Combinatoria

15. Sia $X = \{1, 2, \dots, n\}$.

(i) Calcolare il numero di terne ordinate (A, B, C) di sottoinsiemi di X a due a due disgiunti con $A \cup B \cup C = X$.

(ii) Dimostrare che il numero di terne ordinate (A, B, C) di sottoinsiemi di X tali che $A \cup B \cup C = X$ è 7^n.

16. Sia X l'insieme delle coppie (m, n) di interi primi tra loro con $1 \leq m, n \leq 100$. Dimostrare che $|X| + 1 = 2\sum_{k=1}^{100} \phi(k)$.

17. Determinare la cardinalità dell'insieme $X = \{1 \leq n \leq 10000 \mid (n, 18) = 6 \text{ e } n \equiv 2 \pmod 7\}$.

18. Determinare il numero dei divisori positivi di $3^{40} \cdot 5^{25}$ che sono congrui ad 1 modulo 7.

19. Determinare tutti gli interi positivi n per i quali $\phi(n) = 12$.

20. Determinare il numero delle terne di interi (x, y, n) con $0 \leq x, y < 50$, $n \in \mathbb{N}$ tali che $x + y = n^2$.

21. Determinare tutti gli interi positivi n per cui

$$\phi(n) = \frac{2}{5}n.$$

22. Per ogni intero positivo n, sia $d(n)$ il numero dei divisori positivi di n.
(i) Dimostrare che $d(n) + \phi(n) \leq n + 1$ per ogni intero positivo n.
(ii) Caratterizzare tutti gli interi positivi n per i quali $d(n) + \phi(n) = n$.

23. Determinare tutti i numeri naturali $n \leq 120$ tali che $(n, \phi(n)) = 3$.

24. Determinare il numero di terne ordinate (a, b, c) di numeri interi che soddisfano simultaneamente le seguenti proprietà: $1 \leq a, b, c \leq 60$, esattamente due fra i numeri a, b, c sono pari e esattamente uno fra i numeri a, b, c è divisibile per 3.

25. Per ogni intero positivo m, sia $\omega(m)$ il numero dei fattori primi distinti di m. Dimostrare che

$$\frac{\phi(m)}{m} \geq \frac{1}{\omega(m) + 1}.$$

26. Determinare il numero degli interi n che soddisfano simultaneamente le seguenti proprietà: $1000 < n < 10000$, nessuna delle cifre decimali di n è uguale a 9 e almeno due tra le cifre decimali di n sono uguali.

27. Per ogni numero intero $n > 0$ sia S_n l'insieme delle permutazioni di $\{1, \ldots, n\}$.
(i) Determinare la cardinalità dell'insieme

$$\{f \in \mathsf{S}_n \mid f(i) \leq i + 1 \text{ per } 1 \leq i \leq n\}.$$

(ii) Dimostrare che la cardinalità di

$$\{f \in \mathsf{S}_n \mid i - 1 \leq f(i) \leq i + 1 \text{ per } 1 \leq i \leq n\}$$

è uguale all'$(n + 1)$–esimo numero di Fibonacci.

28. Sia $X = \{1, 2, \ldots, 100\}$.
(i) Determinare il numero dei sottoinsiemi di X con 3 elementi, almeno due dei quali congrui tra loro modulo 5.
(ii) Contare le applicazioni $f : X \longrightarrow X$ tali che $f(n) \equiv n + 1 \pmod 5$ per ogni $n \in X$.

29. Sia $X = \{1, 2, \ldots, 100\}$. Calcolare la cardinalità dei seguenti insiemi
(i) $\{(x, y) \in X^2 \mid (xy, 6) = 1\}$;
(ii) $\{(x, y) \in X^2 \mid x < y + 6\}$.

30. Sia $X = \{1, 2, \ldots, 100\}$. Calcolare la cardinalità dei seguenti insiemi
(i) $A = \{f : X \longrightarrow X \mid f$ è iniettiva e $f^2(x) \equiv f(x) \pmod 2 \ \forall x \in X\}$;
(ii) $B = \{f : X \longrightarrow X \mid f^2(x) = 1 \ \forall x \in X\}$.

31. Calcolare la cardinalità dei seguenti insiemi
(i) $X = \{d \in \mathbb{N} \mid d \mid 144000$ e d ha un numero pari di divisori$\}$;
(ii) $Y = \{d \in \mathbb{N} \mid d \mid 144000$ e d è un quadrato ma non è un cubo$\}$.

32. Sia $X = \{1, 2, \ldots, 100\}$. Calcolare la cardinalità dei seguenti insiemi
(i) $\mathcal{A} = \left\{A \subseteq X |\ \sum_{a \in A} a \equiv 0 \pmod 2\right\}$;
(ii) $\mathcal{B} = \left\{A \subseteq X |\ \prod_{a \in A} a \equiv 0 \pmod 8\right\}$.

33. Contare gli interi n, con $2 \leq n \leq 1000$, per cui $\phi(n) \mid n$.

34. Un giocatore esegue infiniti lanci successivi di una moneta. Ad ogni lancio, le probabilità che escano testa o croce sono entrambe uguali ad $1/2$. Il giocatore parte dal punteggio zero e guadagna 2 punti ogni volta che esce croce ed 1 punto ogni volta che esce testa. Per ogni $k \geq 1$, sia x_k il punteggio ottenuto dal giocatore dopo k lanci.

Dimostrare che, per ogni $n \geq 1$, la probabilità che esista un intero k per cui $x_k = n$ è uguale a

$$\frac{2}{3} + \frac{(-1)^n}{3 \cdot 2^n}.$$

35. Per ogni applicazione biiettiva $f : \{1, 2, \ldots, 10\} \longrightarrow \{1, 2, \ldots, 10\}$ sia

$$S(f) = \sum_{i=1}^{10} |f(i) - i|.$$

Determinare il numero delle applicazioni biettive tali che
(i) $S(f) = 2$;
(ii) $S(f) = 3$;
(iii) $S(f) = 4$.

36. Sia $X = \{1, 2, \ldots, 100\}$. Determinare il numero dei sottoinsiemi A di X tali che
(i) A ha 96 elementi e la somma dei suoi elementi è un numero pari;
(ii) A ha 97 elementi e la somma dei suoi elementi è divisibile per 3.

37. Determinare le cardinalità dei tre seguenti insiemi

$$A = \{f : \{1, \ldots, 5\} \to \{1, \ldots, 100\} \mid f(i) < f(i+1)\ \forall\, i = 1, 2, 3, 4\},$$
$$B = \{f \in A \mid \exists i \text{ con } f(i+1) > f(i) + 1\},$$
$$C = \{f \in A \mid f(i+1) > f(i) + 1\ \forall\, i = 1, 2, 3, 4\}.$$

38. (i) Date $4n$ persone, in quanti modi si possono formare n squadre di bridge ciascuna composta da 4 persone?

(ii) Date $4n$ persone, di cui $2n$ uomini e $2n$ donne, in quanti modi si possono formare n squadre di bridge ciascuna composta da 2 uomini e 2 donne?

39. Sia f una permutazione di $\{1, 2, \ldots, n\}$. Supponiamo che per ogni $x, y \in \{1, 2, \ldots, n\}$ valga la proprietà: x divide y se e solo se $f(x)$ divide $f(y)$.

(i) È vero che f manda il prodotto di k primi distinti nel prodotto di k primi distinti?

(ii) È vero che f manda ogni potenza di un primo in una potenza di un primo?

(iii) Supponendo che $n = 10$, quante sono le possibili scelte di f? E se $n = 13$?

40. Consideriamo un mazzo di 40 carte da gioco, 10 per ogni seme di denari, spade, bastoni, coppe.

(i) Quante sono le possibili disposizioni delle carte per cui, all'interno di ciascun seme, le carte siano in ordine crescente di valore?

(ii) Quante sono le possibili disposizioni delle carte per cui tutte le carte di denari precedano nell'ordine tutte le carte di spade?

41. Dato un intero positivo n, quanti sono i sottoinsiemi di $\{1, 2, 3, \ldots, n\}$ che contengono almeno tre numeri della stessa parità?

42. Una 4–colorazione di $\mathbb{Z}/40\mathbb{Z}$ è una funzione $c : \mathbb{Z}/40\mathbb{Z} \to \{0, 1, 2, 3\}$. Quante sono le possibili 4–colorazioni $c : \mathbb{Z}/40\mathbb{Z} \to \{0, 1, 2, 3\}$ tali che, per ogni $x \in \mathbb{Z}$, si abbia $c(\overline{x}) \neq c(\overline{x+10})$?

43. Consideriamo una colorazione di una scacchiera $n \times n$ in cui ogni casella ha colore bianco o nero.

(i) Quante sono le possibili colorazioni in cui nessuna riga è interamente bianca o interamente nera?

(ii) Quante sono le colorazioni in cui ciascuna riga e ciascuna colonna contiene una ed una sola casella nera?

(iii) Supponendo che n sia pari, quante sono le colorazioni in cui ogni riga contiene lo stesso numero di caselle bianche e nere?

44. Dimostrare che per ogni $n \geq 1$ si ha

(i) $\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}$;

(ii) $\sum_{k=0}^{n} k^2\binom{n}{k} = (n + n^2)2^{n-2}$.

45. Calcolare la cardinalità dell'insieme

$$\{(a_1, \ldots, a_{30}) \in \{0, 1\}^{30} \mid a_1 + a_3 + \cdots + a_{29} \leq 2 \text{ e } a_2 + a_4 + \cdots + a_{30} \leq 2\}.$$

46. Sia $X = \{1, 2, \ldots, 100\}$.

(i) Contare il numero dei sottoinsiemi di X con 3 elementi che contengono due elementi la cui somma fa 10.

(ii) Contare il numero dei sottoinsiemi di X con 3 elementi che contengono almeno 2 elementi divisibili per 5.

47. Contare le coppie ordinate $(x, y) \in \mathbb{Z}/2^{100}\mathbb{Z} \times \mathbb{Z}/2^{100}\mathbb{Z}$ tali che $xy = \overline{0}$.

48. Consideriamo l'insieme X di tutte le squadre da 4 persone che si possono formare scegliendole da un insieme di 13 persone.

(i) Fissate due persone p e q, qual è la probabilità che p e q non siano nella stessa squadra?

(ii) Determinare il numero di elementi di un sottoinsieme di X con la seguente proprietà: date comunque due persone, queste stanno nella stessa squadra una e una sola volta.

49. Contare i divisori positivi d di $2^{100}3^{100}$ tali che $d \equiv 4 \pmod 5$.

50. Sia $X = \{1, 2, \ldots, 100\}$.

(i) Determinare il numero di sottoinsiemi di due elementi di X tali che la somma dei loro elementi sia divisibile per 4.

(ii) Determinare il numero di sottoinsiemi di tre elementi di X che non contengono due numeri consecutivi.

51. Sia X l'insieme delle applicazioni da $\{1, 2, \ldots, 10\}$ in sé e siano, per ogni $f \in X$,

$$M_f = \max\{f(x) \mid 1 \leq x \leq 10), \quad m_f = \min\{f(x) \mid 1 \leq x \leq 10\}.$$

(i) Determinare il numero delle applicazioni $f \in X$ per cui $M_f - m_f = 1$.

(ii) Determinare il numero delle applicazioni $f \in X$ per cui $M_f = 10$ e $m_f = 1$.

52. Determinare tutti i numeri naturali n per i quali $\phi(n) = n - 8$.

53. Sia $X = \{1, 2, \ldots, 100\}$.

(i) Determinare il numero delle applicazioni $f : X \longrightarrow X$ che hanno esattamente 10 punti fissi, cioè 10 elementi $x \in X$ per cui $f(x) = x$.

(ii) Determinare il numero delle applicazioni $f : X \longrightarrow X$ tali che

$$\sum_{x \in X} |f(x) - x| = 2.$$

54. Sia $X = \{1, 2, \ldots, 20\}$.

(i) Determinare il numero delle coppie ordinate (A, B) di sottoinsiemi di X tali che $|A| = 5$ e $|A \cup B| = 12$.

(ii) Determinare il numero delle terne ordinate (A, B, C) di sottoinsiemi di X tali che $|(A \cup B) \cap C| = 8$.

55. (i) Contare le stringhe $(a_0, \ldots, a_9)$, con $a_i \in \{0, 1, 2, 3, 4\}$ per ogni i, in cui gli a_i pari sono più degli a_i dispari.

(ii) Determinare il numero delle stringhe $(a_0, \ldots, a_9)$, con $a_i \in \{0, 1, 2, 3, 4\}$ per ogni i, tali che

$$\sum_{i=0}^{9} (-1)^i a_i \equiv 0 \pmod 6.$$

56. Sia $N = \{1, 2, \ldots, 100\}$. Determinare la cardinalità dei seguenti insiemi

(i) $X = \{A \subseteq N \mid \max A - \min A = 60\}$;

(ii) $Y = \{f : N \longrightarrow N \mid f(1) \cdot f(2) \cdots f(100) \not\equiv 0 \pmod{10}\}$.

57. Sia P l'insieme delle parole di lunghezza 3 che si possono scrivere con 26 lettere. Contare le coppie (α, β) con $\alpha, \beta \in P$ tali che α, β non hanno lettere in comune.

58. Sia $X = \{1, 2, \ldots, 100\}$. Calcolare il numero di

(i) coppie (A, B) di sottoinsiemi di X con $|A \cup B| = 40$ e $|A| = 10$;

(ii) sottoinsiemi A di X con $|A| = 5$ e $\prod_{x \in A} x \equiv 0 \pmod 9$.

59. Consideriamo un dado a 6 facce, in cui le facce siano numerate da 1 a 6, ed associamo ad un lancio del dado il punteggio corrispondente al valore della faccia. Calcolare la probabilità che, dopo n lanci dello stesso dado, la somma dei punteggi ottenuti sia un multiplo di 7.

60. (i) Determinare il numero di soluzioni intere positive (x, y) dell'equazione $2x + 3y = 100$.

(ii) Determinare il numero di sottoinsiemi A di tre elementi di $\{1, 2, \ldots, 100\}$ per cui la somma degli elementi di A è uguale a 100.

61. Determinare per quali naturali a esiste un numero naturale n tale che

$$\phi(n) = \frac{a}{43}n.$$

62. Sia $X = \{1, 2, \ldots, 100\}$.

(i) Determinare il numero dei sottoinsiemi di due elementi $\{a, b\}$ di X tali che $ab \equiv a + b \pmod 3$.

(ii) Determinare il numero dei sottoinsiemi di due elementi $\{a, b\}$ di X tali che $ab(a + b) \equiv 0 \pmod 3$.

63. Sia $X = \{1, \ldots, 100\}$ e sia $\mathsf{S}(X)$ l'insieme delle permutazioni di X.

(i) Se $\sigma \in \mathsf{S}(X)$ definiamo, per $i = 0, 1, 2$, l'insieme $X_{i,\sigma} = \{x \in X \mid \sigma(x) - x \equiv i \pmod 3\}$. Dimostrare che, per ogni $\sigma \in \mathsf{S}(X)$, si ha $|X_{1,\sigma}| \equiv |X_{2,\sigma}| \pmod 3$.

(ii) Determinare il numero di permutazioni $\sigma \in \mathsf{S}(X)$ per cui $\sigma \circ \sigma(x) \equiv x \pmod 2$ per ogni $x \in X$.

64. Determinare il numero di terne ordinate di numeri interi positivi (x, y, z) tali che

(i) $xyz = 10^{100}$;

(ii) $x^2yz = 10^{100}$.

65. Sia $X = \{1, 2, \ldots, 10\}$. Contare le applicazioni $f : X \longrightarrow X$ tali che per ogni a, b in X, il numero $f(a) \cdot f(b)$ non è un primo.

66. Consideriamo un insieme di n coppie di gemelli.

(i) In quanti modi possiamo scegliere una squadra composta da 6 persone tra le quali ci sono esattamente due coppie di gemelli?

(ii) Sia $n = 12$. In quanti modi possiamo dividere le 24 persone in 4 squadre da 6 persone in modo che ci siano almeno due gemelli che non sono nella stessa squadra?

67. Sia $X = \{1, 2, \ldots, 100\}$. Calcolare la cardinalità dei seguenti insiemi

(i) $\{A \in \mathcal{P}(X) \mid \sum_{x \in A} x^{100} \equiv 0 \pmod 2\}$;

(ii) $\{(A, B) \in \mathcal{P}(X)^2 \mid 4 \text{ divide esattamente } \prod_{x \in A \cap B} x\}$.

2.3 Congruenze

68. Calcolare, al variare dell'intero a, le soluzioni del seguente sistema di congruenze

$$\begin{cases} 2^{ax} \equiv 13 \pmod{17} \\ (x-a)(x-2) \equiv 0 \pmod{4}. \end{cases}$$

69. Determinare per quali valori interi di a il seguente sistema ha soluzioni

$$\begin{cases} 2^x \equiv a \pmod{9} \\ x \equiv a^2 \pmod{3}. \end{cases}$$

70. Determinare per quali valori dell'intero a il seguente sistema ha soluzioni

$$\begin{cases} 2^x \equiv 3^a \pmod{7} \\ 4x^2 \equiv a^2 \pmod{24}. \end{cases}$$

71. Dire per quali valori di $a \in \mathbb{Z}$ il seguente sistema è risolubile e risolverlo

$$\begin{cases} 3^{x^2-1} \equiv 2^a \pmod{13} \\ x - 1 \equiv 0 \pmod{3}. \end{cases}$$

72. Determinare le soluzioni del sistema di congruenze

$$\begin{cases} 2^x \equiv x \pmod{7} \\ x^2 \equiv 1 \pmod{15}. \end{cases}$$

73. Si determinino i valori naturali di n che soddisfano il sistema

$$\begin{cases} \binom{n}{3} \equiv 0 \pmod{2} \\ \binom{n}{4} \equiv 0 \pmod{2}. \end{cases}$$

74. Risolvere il sistema di congruenze

$$\begin{cases} x^2 \equiv 4 \pmod{14} \\ x \equiv 3 \pmod{5}. \end{cases}$$

75. Risolvere il sistema di congruenze

$$\begin{cases} x^{660} \equiv 1 \pmod{847} \\ x \equiv 11 \pmod{13}. \end{cases}$$

76. Si dica per quali $a \in \mathbb{Z}$ la congruenza $x^3 - a^3 \equiv 0 \pmod{85}$ ha soluzioni diverse da $x \equiv a \pmod{85}$.

77. Risolvere la congruenza $2^x \equiv 5 \pmod{3^3}$. Successivamente risolvere i sistemi

$$\begin{cases} 2^x \equiv 5 \pmod{3^3} \\ x \equiv 2 \pmod{15}, \end{cases} \qquad \begin{cases} 2^x \equiv 5 \pmod{3^4} \\ x \equiv 3 \pmod{15}. \end{cases}$$

78. (i) Per quali interi b la congruenza $81^x \equiv b \pmod{125}$ è risolubile?

(ii) Se $81^x \equiv b_0 \pmod{125}$ ha una soluzione x_0, descrivere l'insieme delle soluzioni.

79. Risolvere la congruenza $2^x \equiv 3 \pmod{125}$. Come si può risolvere la congruenza $2^x \equiv 3 \pmod{625}$?

80. Risolvere il sistema di congruenze

$$\begin{cases} 5^x \equiv 3 & \pmod{11} \\ x^2 \equiv -3 & \pmod{21}. \end{cases}$$

81. Al variare di $a \in \mathbb{Z}$, determinare i valori interi di x per cui

$$\frac{1}{3}x^3 - \frac{8}{21}ax^2 + \frac{3}{7}x + \frac{1}{7}a$$

è un numero intero.

82. Determinare il numero di soluzioni modulo 77 della congruenza $x^{15} \equiv x^{27} \pmod{77}$.

83. Determinare, al variare di $k \in \mathbb{N}$, le soluzioni del sistema di congruenze

$$\begin{cases} x^k \equiv x & \pmod{7} \\ x^3 \not\equiv x & \pmod{7}. \end{cases}$$

84. Determinare per quali valori dell'intero a il seguente sistema di congruenze è risolubile

$$\begin{cases} ax \equiv 4 & \pmod{25} \\ x^2 + a \equiv 0 & \pmod{15} \end{cases}$$

e determinarne le soluzioni per $a = -1$.

85. Al variare di $a \in \mathbb{Z}$ risolvere il seguente sistema di congruenze

$$\begin{cases} ax \equiv 1 & \pmod{9} \\ a^x \equiv 1 & \pmod{9}. \end{cases}$$

86. Determinare, in funzione dell'intero a, le soluzioni del sistema

$$\begin{cases} (6a-1)x \equiv 1 & \pmod{21} \\ x \equiv a & \pmod{35}. \end{cases}$$

87. Determinare per quali valori dell'intero a il seguente sistema di congruenze è risolubile

$$\begin{cases} 9^{ax} \equiv 1 & \pmod{34} \\ x^2 - 9ax \equiv 6 & \pmod{15} \end{cases}$$

e determinarne le soluzioni per $a = 4$.

88. Discutere la risolubilità del seguente sistema di congruenze e risolverlo, al variare dell'intero a

$$\begin{cases} 3x \equiv a & (\text{mod } 42) \\ 6x \equiv 1 & (\text{mod } 35). \end{cases}$$

89. Risolvere il seguente sistema di congruenze

$$\begin{cases} 5^x \equiv 9 & (\text{mod } 2^4) \\ x^2 + 2x + 8 \equiv 0 & (\text{mod } 176). \end{cases}$$

90. Determinare i valori dell'intero a per cui il seguente sistema di congruenze ha soluzione

$$\begin{cases} x^2 \equiv 5a & (\text{mod } 120) \\ 6x \equiv a & (\text{mod } 21). \end{cases}$$

Determinare inoltre le soluzioni del sistema per $a = 45$.

91. Contare le soluzioni della congruenza $x^{100} \equiv a \pmod{77}$ al variare dell'intero a.

92. (i) Contare, al variare dell'intero a, il numero di soluzioni della congruenza $x^a \equiv 1 \pmod{92}$.

(ii) Risolvere, al variare del parametro intero a, il sistema di congruenze

$$\begin{cases} x^a \equiv 1 & (\text{mod } 92) \\ 6x \equiv 8 & (\text{mod } 23). \end{cases}$$

93. Contare, al variare dell'intero a, il numero di soluzioni del sistema di congruenze

$$\begin{cases} 2x \equiv a & (\text{mod } 22) \\ x^2 \equiv 7a & (\text{mod } 84). \end{cases}$$

94. Risolvere il seguente sistema di congruenze, al variare dell'intero a

$$\begin{cases} a^x \equiv 3 & (\text{mod } 8) \\ x^{2a} \equiv 4 & (\text{mod } 9). \end{cases}$$

95. Determinare il numero di coppie ordinate $(x, y) \in \mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/100\mathbb{Z}$ tali che $xy = \overline{0}$.

96. Determinare, in funzione dell'intero a, il numero di soluzioni del sistema di congruenze

$$\begin{cases} 6x \equiv 4a & (\text{mod } 72) \\ 5x \equiv 2 & (\text{mod } 39). \end{cases}$$

97. Risolvere il seguente sistema di congruenze

$$\begin{cases} 8^{x^2-1} \equiv -1 & (\text{mod } 27) \\ x^{22} + 2x \equiv 8 & (\text{mod } 44). \end{cases}$$

98. Al variare di $a \in \mathbb{Z}$, determinare il numero di soluzioni, per un modulo opportuno, del sistema di congruenze

$$\begin{cases} 3^x \equiv 2^a & (\text{mod } 5) \\ x^3 \equiv a+2 & (\text{mod } 24). \end{cases}$$

99. Determinare, al variare di $a \in \mathbb{Z}$, le soluzioni del sistema di congruenze

$$\begin{cases} a^x \equiv 3 & (\text{mod } 7) \\ x^2 \equiv a & (\text{mod } 8). \end{cases}$$

100. Determinare, al variare di $a \in \mathbb{Z}$, le soluzioni del sistema di congruenze

$$\begin{cases} a^x \equiv 1 & (\text{mod } 5) \\ ax \equiv 2 & (\text{mod } 8). \end{cases}$$

101. Determinare, al variare di $a \in \mathbb{Z}$, le soluzioni del sistema di congruenze

$$\begin{cases} 5^{x^2-1} \equiv 2^a & (\text{mod } 13) \\ x^3 \equiv 0 & (\text{mod } 64). \end{cases}$$

102. Determinare per quali valori dell'intero a il seguente sistema

$$\begin{cases} a^x \equiv 11 & (\text{mod } 14) \\ x^a \equiv 1 & (\text{mod } 9) \end{cases}$$

ha soluzione.

103. (i) Determinare l'insieme di tutti gli $x \in \mathbb{Z}$ tali che $3^x \equiv 7 \pmod{10}$.
(ii) Determinare l'insieme di tutti gli $x \in \mathbb{Z}$ tali che $3^x \equiv 4 + x \pmod{10}$.

104. Determinare le soluzioni del seguente sistema di congruenze:

$$\begin{cases} x^{2x+1} \equiv 1 & (\text{mod } 7) \\ 4x \equiv 7 & (\text{mod } 15). \end{cases}$$

105. (i) Sia k un numero naturale. Determinare quanti sono gli $x \in \mathbb{Z}$ con $0 \le x \le k$ tali che: $x \equiv 1 \pmod{n}$ per ogni n con $1 \le n \le 10$.
(ii) Determinare quanti sono gli interi $x \in \mathbb{Z}$ tali che: $x \equiv -1 \pmod{n}$ per ogni intero positivo n.
(iii) Determinare quanti sono gli interi $x \in \mathbb{Z}$ tali che: $x \equiv n \pmod{2n}$ per ogni intero positivo n.

106. Trovare tutte le coppie di numeri interi positivi (x, n) che soddisfano la congruenza $x^n \equiv 39 \pmod{10x}$.

107. Determinare, al variare di $n \in \mathbb{Z}$, il numero di soluzioni della congruenza

$$x^{5n} \equiv 1 \pmod{55}.$$

108. (i) Risolvere la congruenza $x^2 - x + 43 \equiv 0 \pmod{55}$.
(ii) Risolvere il seguente sistema, al variare dell'intero a

$$\begin{cases} x^2 - x + 43 \equiv 0 & (\text{mod } 55) \\ x^{11^4} \equiv x^a & (\text{mod } 5). \end{cases}$$

109. Risolvere le seguenti congruenze:
(i) $x^2 + 2x + 5 \equiv 0 \pmod{65}$;
(ii) $3^{2x} + 2 \cdot 3^x + 5 \equiv 0 \pmod{65}$.

110. Risolvere il seguente sistema di congruenze:

$$\begin{cases} x^2 + 2x + 2 \equiv 0 & (\text{mod } 10) \\ 7x \equiv 20 & (\text{mod } 22). \end{cases}$$

111. Al variare dell'intero a, determinare il numero di soluzioni modulo 180 del seguente sistema di congruenze

$$\begin{cases} ax \equiv 2 & (\text{mod } 12) \\ 9x \equiv a^2 + 2a - 3 & (\text{mod } 81). \end{cases}$$

112. Risolvere il seguente sistema di congruenze:

$$\begin{cases} x^{131} \equiv x & (\text{mod } 55) \\ x^6 + x \equiv 0 & (\text{mod } 125). \end{cases}$$

113. Discutere la risolubilità del seguente sistema di congruenze e risolverlo, al variare dell'intero a

$$\begin{cases} ax \equiv 12 & (\text{mod } 77) \\ 13x \equiv 25 & (\text{mod } 133). \end{cases}$$

114. Determinare per quali valori dell'intero a il seguente sistema di congruenze è risolubile

$$\begin{cases} x^{80} \equiv 2 & (\text{mod } 7) \\ 80^x \equiv 2 & (\text{mod } 7) \\ 7x \equiv a & (\text{mod } 10) \end{cases}$$

e determinarne le soluzioni in funzione di a.

115. Determinare le soluzioni del seguente sistema di congruenze

$$\begin{cases} x^{41} \equiv x & (\text{mod } 700) \\ 45x \equiv 25 & (\text{mod } 700). \end{cases}$$

116. Determinare le soluzioni della congruenza $x^{x+1} \equiv 1 \pmod{27}$.

117. Determinare i valori dell'intero a per cui il sistema di congruenze

$$\begin{cases} ax \equiv 12 & (\text{mod } 27) \\ a^3x^2 \equiv 9 & (\text{mod } 39) \end{cases}$$

è risolubile.

118. Sia a intero, e si consideri il sistema di congruenze

$$\begin{cases} x^2 - 7a \equiv 0 & (\text{mod } 5) \\ a^x \equiv 3 & (\text{mod } 35). \end{cases}$$

(i) Determinare per quali valori di a il sistema è risolubile.
(ii) Determinare, per ogni valore di a, il numero di soluzioni del sistema per un modulo opportuno.

119. Determinare i valori dell'intero a per cui il sistema di congruenze

$$\begin{cases} x^2 + x + 1 \equiv 0 & (\text{mod } 13) \\ ax \equiv 27 & (\text{mod } 78) \end{cases}$$

è risolubile e determinarne le soluzioni.

120. Risolvere il seguente sistema di congruenze

$$\begin{cases} x^2 - 4x + 3 \equiv 0 & (\text{mod } 15) \\ 30x \equiv -6 & (\text{mod } 81). \end{cases}$$

121. Determinare il numero di soluzioni modulo 1001 della congruenza $x^{101} \equiv x \pmod{1001}$.

122. Contare le soluzioni modulo 2^{10} della seguente congruenza $x^5 - 16x \equiv 0 \pmod{2^{10}}$.

123. Determinare i valori dell'intero a per cui il seguente sistema di congruenze ha soluzione

$$\begin{cases} 2^x \equiv 3^{x+a^2} & (\text{mod } 17) \\ 3x \equiv a^{23} & (\text{mod } 24). \end{cases}$$

124. Determinare, al variare dell'intero a, il numero di soluzioni modulo 90 del seguente sistema di congruenze.

$$\begin{cases} 3x \equiv a + 1 & (\text{mod } 9) \\ (x-1)(x-a) \equiv 0 & (\text{mod } 15). \end{cases}$$

125. Determinare per quali valori dell'intero a il seguente sistema di congruenze

$$\begin{cases} x^{27} \equiv x^2 & (\text{mod } 144) \\ 10x \equiv a & (\text{mod } 25) \\ 2^{x-1} \equiv 4 & (\text{mod } 11) \end{cases}$$

è risolubile e determinarne le soluzioni.

126. Determinare tutte le coppie (x, y) di interi tali che

$$\begin{cases} 2^{2y^2-5y+4} \equiv 2 & (\text{mod } 36) \\ (2x^2+17)(2x^2+xy+4x+2y)^{-1} \equiv 1 & (\text{mod } 592) \\ x^{23} + 1 \equiv 0 & (\text{mod } 100). \end{cases}$$

127. Determinare, al variare di $a \in \mathbb{Z}$, le soluzioni del sistema di congruenze

$$\begin{cases} a^x \equiv 1 \pmod{77} \\ ax \equiv 1 \pmod{10}. \end{cases}$$

128. Al variare di $a \in \mathbb{Z}$, determinare le soluzioni in $\mathbb{Z}$ del sistema

$$\begin{cases} 7^x \equiv a \pmod{8} \\ (x+a)^4 \equiv 0 \pmod{200}. \end{cases}$$

129. Determinare al variare di $a \in \mathbb{Z}$ le soluzioni intere del sistema

$$\begin{cases} 7ax \equiv a \pmod{49} \\ x^a \equiv 1 \pmod{3}. \end{cases}$$

130. Determinare il numero di soluzioni intere del sistema

$$\begin{cases} x^3 \equiv 8 \pmod{1000} \\ x \equiv 2 \pmod{3} \end{cases}$$

con $0 \leq x < 3001$.

131. (i) Trovare tutte le soluzioni di

$$x^{36} \equiv x \pmod{9}.$$

(ii) Risolvere il seguente sistema di congruenze

$$\begin{cases} x^{36} \equiv x \pmod{9} \\ x^2 - x \equiv 0 \pmod{64}. \end{cases}$$

132. Contare, al variare di $a \in \mathbb{N}$, il numero di soluzioni modulo 584 della congruenza

$$x^{a+5} - x^a - x^5 + 1 \equiv 0 \pmod{584}.$$

133. Risolvere la seguente congruenza e contarne il numero di soluzioni modulo 10^{10}

$$x^5 - 4x + 400 \equiv 0 \pmod{10^{10}}.$$

2.4 Gruppi

134. Siano $(G, +)$, $(G', +)$ due gruppi abeliani e siano H un sottogruppo proprio di G, H' un sottogruppo proprio di G'. Sia inoltre

$$\mathrm{Hom}(G, G') = \{f : G \to G' \mid f \text{ omomorfismo}\}$$

il gruppo degli omomorfismi da G in G' con l'operazione definita da $(f+g)(x) = f(x)+g(x)$ per ogni $x \in G$. Determinare se i seguenti sottoinsiemi di $\mathrm{Hom}(G, G')$ sono suoi sottogruppi

$$A = \{f \in \mathrm{Hom}(G, G') \mid \mathrm{Ker}(f) \subseteq H\};$$
$$B = \{f \in \mathrm{Hom}(G, G') \mid \mathrm{Ker}(f) \supseteq H\};$$
$$C = \{f \in \mathrm{Hom}(G, G') \mid f(G) \subseteq H'\};$$
$$D = \{f \in \mathrm{Hom}(G, G') \mid f(G) \supseteq H'\}.$$

135. Sia $G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$.
(i) Quanti sono gli elementi di G di ordine 60?
(ii) Quanti sono i sottogruppi ciclici di G di ordine 30?
(iii) Quanti sono gli omomorfismi iniettivi $f : \mathbb{Z}/12\mathbb{Z} \longrightarrow G$?

136. Sia G il gruppo delle applicazioni biettive $f : \mathbb{Z}/72\mathbb{Z} \longrightarrow \mathbb{Z}/72\mathbb{Z}$ della forma $f(x) = ax$ con $(a, 72) = 1$ e sia $H = \{f \in G \mid f(\overline{12}) = \overline{12}\}$.
(i) Dimostrare che H è un sottogruppo di G e calcolarne l'ordine.
(ii) Il sottogruppo H è ciclico?

137. Sia $G = \mathbb{Z}/12\mathbb{Z}$ e siano a, b due elementi di G. Siano inoltre $f : G \longrightarrow G \times G$, $g : G \times G \longrightarrow G$ gli omomorfismi definiti da $f(x) = (ax, bx)$ e $g(y, z) = y + z$.
(i) Quante sono le coppie (a, b) per cui f è iniettivo?
(ii) Quante sono le coppie (a, b) per cui $g \circ f$ è iniettivo?

138. Indicato con p un numero primo, dimostrare che il gruppo $(\mathbb{Z}/p^2\mathbb{Z})^*$ possiede sia elementi di ordine p che elementi di ordine $p-1$.

139. Sia G un gruppo e siano H, K due suoi sottogruppi normali. Dimostrare che $HK = \{hk \mid h \in H, k \in K\}$ è un sottogruppo normale di G.

140. Sia G un gruppo e sia $f : G \longrightarrow G$ un omomorfismo tale che $f \circ f = f$. Dimostrare che
(i) $\mathrm{Ker}(f) \cap \mathrm{Im}(f) = \{e\}$;
(ii) $G = \mathrm{Ker}(f) \cdot \mathrm{Im}(f)$.

141. (i) Contare gli elementi di ordine 2 e di ordine 3 del gruppo $(\mathbb{Z}/49\mathbb{Z})^*$.
(ii) Contare gli omomorfismi da $\mathbb{Z}/6\mathbb{Z}$ in $(\mathbb{Z}/49\mathbb{Z})^*$.

142. Sia G un gruppo, sia H un suo sottogruppo e sia $Z(H) = \{g \in G \mid gh = hg \ \forall h \in H\}$, il centralizzatore di H in G. Dimostrare che
(i) $Z(H)$ è un sottogruppo di G;
(ii) se H è normale in G allora anche $Z(H)$ lo è;
(iii) per ogni omomorfismo di gruppi $f : G \longrightarrow G'$ si ha $f(Z(H)) \subseteq Z(f(H))$;
(iv) dare un esempio di un omomorfismo $f : G \longrightarrow G'$ e di un sottogruppo H di G tali che $Z(H) = G$ e $Z(f(H)) \neq G'$.

143. Sia G un gruppo abeliano e sia H il suo sottoinsieme formato da tutti gli elementi di ordine finito.

(i) Dimostrare che H è un sottogruppo di G e mostrare con un esempio che H può essere infinito.

(ii) Dimostrare che ogni elemento di G/H diverso dall'elemento neutro ha ordine infinito.

(iii) Dimostrare che G/H è isomorfo a G se e solo se H è banale.

(iv) Dimostrare che il nucleo di ogni omomorfismo $G \longrightarrow \mathbb{Z}$ contiene H.

144. Siano G_1 e G_2 gruppi e sia $G_1 \times G_2$ il loro prodotto diretto. Indichiamo con $\pi_1 : G_1 \times G_2 \longrightarrow G_1$ e $\pi_2 : G_1 \times G_2 \longrightarrow G_2$ le proiezioni. Dimostrare che

(i) se H_1 è normale in G_1 e H_2 è normale in G_2 allora $H_1 \times H_2$ è normale in $G_1 \times G_2$;

(ii) se $\mathcal{H}$ è un sottogruppo di $G_1 \times G_2$ allora $\mathcal{H} \subseteq \pi_1(\mathcal{H}) \times \pi_2(\mathcal{H})$;

(iii) se $|G_1| = m$, $|G_2| = n$ e $(m, n) = 1$ allora per ogni $\mathcal{H}$ sottogruppo di $G_1 \times G_2$ si ha $\mathcal{H} = \pi_1(\mathcal{H}) \times \pi_2(\mathcal{H})$.

145. Siano G_1 e G_2 gruppi finiti, sia $f : G_1 \longrightarrow G_2$ un omomorfismo e sia H un sottogruppo di G_1 che contiene il nucleo di f.

(i) Dimostrare che $[G_1 : H] = [f(G_1) : f(H)]$.

(ii) È vero il risultato del primo punto senza l'ipotesi $\mathrm{Ker}(f) \subseteq H$?

(iii) È vero il risultato del primo punto per $G_1 = \mathbb{Z}$ e G_2 gruppo finito?

146. Sia G un gruppo. Un sottogruppo M di G si dice *massimale* se $M \neq G$ e per ogni H sottogruppo di G tale che $M \subsetneq H \subseteq G$ si ha $H = G$. Indichiamo con N l'intersezione di tutti i sottogruppi massimali di G.

(i) Dimostrare che N è un sottogruppo normale di G.

(ii) Sia $G = \mathbb{Z}/n\mathbb{Z}$. Dimostrare che $N = \{\overline{0}\}$ se e solo se n è libero da quadrati.

(iii) Determinare N per $G = \mathbb{Z}/100\mathbb{Z}$.

147. Sia G un gruppo e sia N un suo sottogruppo normale. Sia f un automorfismo di G tale che $f(N) = N$. Ponendo $\varphi(gN) = f(g)N$ per ogni $g \in G$, definiamo un automorfismo di G/N?

148. Sia $G = (\mathbb{Z}/35\mathbb{Z})^*$.

(i) Per ogni intero positivo n, determinare il numero di elementi di G di ordine n.

(ii) Determinare il numero di sottogruppi di G di ordine 6.

149. Sia G un gruppo e siano $f, g : G \longrightarrow \mathbb{Z}/12\mathbb{Z}$ due omomorfismi.

(i) Dimostrare che l'insieme $\{x \in G \mid f(x) = g(x)\}$ è un sottogruppo normale di G.

(ii) Se $G = \mathsf{S}_3 \times \mathbb{Z}/2\mathbb{Z}$ e $H = \langle((123), \overline{0})\rangle$, descrivere tutti gli omomorfismi $f : G \longrightarrow \mathbb{Z}/12\mathbb{Z}$ tali che $f(h) = \overline{0}$ per ogni $h \in H$.

150. Dati due primi p, q con $p < q$ siano $G = (\mathbb{Z}/pq\mathbb{Z})^*$, $G^{(2)} = \{x^2 \mid x \in G\}$ e $G^{(3)} = \{x^3 \mid x \in G\}$.

(i) Determinare gli ordini dei sottogruppi $G^{(2)}$ e $G^{(3)}$.

(ii) Per quali p, q il sottogruppo $G^{(2)}$ è ciclico?

(iii) Per quali p, q il sottogruppo $G^{(3)}$ è ciclico?

151. Sia $(G,+)$ un gruppo abeliano e siano H, K due sottogruppi di G tali che $|G/H| = m$, $|G/K| = n$, con $(m,n) = 1$. Dimostrare che

(i) $G = H + K$;

(ii) $G/(H \cap K) \simeq G/H \times G/K$.

152. Sia $G = \mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Determinare il numero degli omomorfismi $f : G \longrightarrow G$. Sia inoltre, per ogni $n \in \mathbb{N}$, $f_n : G \to G$ l'omomorfismo definito da $f_n(x) = nx$ per ogni $x \in G$.

(i) Per quali valori di n il nucleo di f_n è un gruppo ciclico?

(ii) Per quali valori di n l'immagine di f_n è un gruppo ciclico?

153. Sia G un gruppo abeliano finito, H un suo sottogruppo ciclico tale che G/H è anch'esso ciclico. Sia $m = \mathrm{ord}(H)$, $n = \mathrm{ord}(G/H)$.

(i) Dimostrare che se $(m,n) = 1$ allora G è ciclico.

(ii) Dare un esempio in cui la tesi non è vera se $(m,n) > 1$.

154. Sia n un intero positivo, sia G un gruppo di ordine n e sia $f_k : G \longrightarrow G$ l'applicazione definita da $f_k(x) = x^k$ per ogni $x \in G$.

(i) Dimostrare che se f_{n-1} è un omomorfismo allora G è abeliano.

(ii) Dimostrare che se $n = 62$ e f_8 è un omomorfismo allora G è abeliano.

(iii) Dare un esempio di un gruppo finito e di un intero k per cui f_k non è un omomorfismo.

155. Sia G un gruppo abeliano finito di ordine n. Per ogni divisore primo p di n, sia G_p l'insieme degli elementi di G di ordine una potenza di p.

(i) Dimostrare che G_p è un sottogruppo di G di ordine una potenza di p.

(ii) Dimostrare che tutti gli elementi di G/G_p hanno ordine relativamente primo con p.

(iii) Se $n = p^a q^b$, con p, q primi distinti e $a, b \in \mathbb{N}$, dimostrare che G/G_p è isomorfo a G_q.

156. Sia L il sottogruppo additivo dei numeri razionali costituito dagli elementi che si possono scrivere nella forma $m/10^n$ per qualche $m \in \mathbb{Z}, n \in \mathbb{N}$. Al variare di k fra gli interi positivi, si determini

(i) quanti sono gli elementi di ordine k in $\mathbb{Q}/L$;

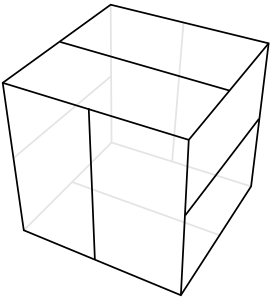
(ii) quante sono le soluzioni dell'equazione $kx = 0$ in $\mathbb{Q}/L$.

157. Sia G il gruppo dei movimenti rigidi dello spazio che portano un cubo in se stesso.

(i) Stabilire se G ha sottogruppi di ordine 3.

(ii) Si bisechi ciascuna faccia del cubo come in figura, con segmenti paralleli su facce opposte. Si calcoli l'indice del sottogruppo H di G costituito dai movimenti che preservano la figura.

(iii) H è normale in G?



158. Sia G il gruppo $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

(i) Determinare il numero dei sottogruppi ciclici di G.

(ii) Determinare il numero degli elementi $x \in G$ tali che $G/\langle x \rangle$ è un gruppo ciclico.

159. Sia G l'insieme di tutte le biezioni $f : \mathbb{Z}/60\mathbb{Z} \longrightarrow \mathbb{Z}/60\mathbb{Z}$ tali che per ogni $x \in \mathbb{Z}$ si abbia $f(\overline{x}) \equiv \overline{x} \pmod{20}$.

(i) Dimostrare che G è un gruppo con l'operazione di composizione e calcolarne la cardinalità.

(ii) Per ciascun $m \in \{6, 8, 10, 12\}$ stabilire se G possiede un sottogruppo di ordine m e se possiede un sottogruppo ciclico di ordine m.

160. Sia $(G, +)$ un gruppo abeliano finito e supponiamo che $3G = \{3x \mid x \in G\}$ sia un sottogruppo ciclico di G. Dimostrare che ogni sottogruppo di G di ordine relativamente primo con 3 è ciclico.

161. Sia n un naturale, contare il numero di omomorfismi e di omomorfismi iniettivi da $\mathbb{Z}/n\mathbb{Z}$ in $\mathbb{Z}/10 \times \mathbb{Z}/20\mathbb{Z}$.

162. Indichiamo con G il gruppo $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$ e sia $f : G \longrightarrow G$ l'omomorfismo definito da $f(g) = 78g$ per ogni $g \in G$.

(i) Determinare le cardinalità del nucleo e dell'immagine di f.

(ii) Determinare il massimo ordine di un elemento dell'immagine.

163. Siano $(G, +)$ un gruppo abeliano e sia $Q = \{2g \mid g \in G\}$.

(i) Dimostrare che Q è un sottogruppo di G.

(ii) Per quali valori di $m \in \{1, 2, 3, 4\}$ si può avere $|G/Q| = m$? Per i valori per cui questo è possibile dare un esempio che lo mostri, e per gli altri dimostrare che non è possibile.

164. Sia G il gruppo $\mathbb{Z}/99\mathbb{Z} \times \mathbb{Z}/33\mathbb{Z}$.

(i) Determinare il numero di elementi di ordine 11 e il numero di sottogruppi di ordine 11 di G.

(ii) Dire se esiste un sottogruppo H di G di ordine 11 tale che G/H sia ciclico.

(iii) Dire se esiste un omomorfismo suriettivo da G in $\mathbb{Z}/121\mathbb{Z}$.

165. Siano G un gruppo, H un suo sottogruppo normale di ordine n e sia m un intero positivo primo con n. Dimostrare che G/H ha elementi di ordine m se e solo se G ha elementi di ordine m.

166. Sia dato il gruppo $G = \mathbb{Z}/8\mathbb{Z} \times Z/12\mathbb{Z}$.
(i) Determinare tutti i sottogruppi di G che hanno ordine 4.
(ii) Determinare tutti i sottogruppi di G che hanno ordine 48.

167. Sia p un numero primo e siano $G_1 = (Z/p\mathbb{Z})^*$, $G_2 = (\mathbb{Z}/p^2\mathbb{Z})^*$.
(i) Esistono omomorfismi suriettivi da G_2 a G_1?
(ii) Esistono omomorfismi iniettivi da G_1 in G_2?

168. Sia $(G, +)$ un gruppo abeliano finito e siano p un numero primo ed a un numero naturale tali che p^a è la massima potenza di p che divida $|G|$.
(i) Dimostrare che $H = \{x \in G \mid p^a x = 0\}$ è un sottogruppo di G.
(ii) Dimostrare che G/H non ha elementi di ordine p.
(iii) Dimostrare che $|H| = p^a$.

169. Siano m, n due numeri interi positivi, sia G il gruppo $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ e sia $\mathbb{C}^*$ il gruppo moltiplicativo dei numeri complessi diversi da zero.

(i) Indichiamo con $\mathrm{Hom}(G, \mathbb{C}^*)$ l'insieme degli omomorfismi definiti su G e a valori in $\mathbb{C}^*$. Dimostrare che, per ogni f e g in $\mathrm{Hom}(G, \mathbb{C}^*)$ l'applicazione $G \ni x \longmapsto (fg)(x) \doteq f(x) \cdot g(x) \in \mathbb{C}^*$ è ancora un omomorfismo e che con l'operazione $(f, g) \longmapsto fg$, l'insieme $\mathrm{Hom}(G, \mathbb{C}^*)$ è un gruppo.

(ii) Determinare tutte le coppie (m, n) per cui $\mathrm{Hom}(G, \mathbb{C}^*)$ contiene un omomorfismo iniettivo.

170. Sia $(G, +)$ un gruppo abeliano finito di ordine n e, per ogni numero primo p, sia pG il sottogruppo di G definito da $pG = \{px \mid x \in G\}$. Dimostrare che
(i) se p e q sono due primi distinti, allora $G = pG + qG$;
(ii) se p e q sono due primi distinti, allora $G = pG \cup qG$ se e solo se $pq \nmid n$;
(iii) se p, q, r sono tre primi dispari distinti, allora $G = pG \cup qG \cup rG$ se e solo se $pqr \nmid n$.

171. Determinare il minimo e il massimo numero di elementi di ordine primo in un gruppo G, al variare di G tra i gruppi abeliani di ordine 200.

172. Siano G un gruppo abeliano finito di ordine n, e siano p, q due numeri primi distinti che dividono n. Siano, inoltre, h_p, h_q e h_{pq} il numero dei sottogruppi di G di ordine p, q e pq, rispettivamente. Analogamente, siano m_p, m_q e m_{pq} il numero di elementi di G di ordine p, q e pq, rispettivamente.

Dimostrare che $h_{pq} = h_p h_q$ e $m_{pq} = m_p m_q$.

173. Sia G in gruppo, sia p un numero primo e siano H e K due distinti sottogruppi normali di indice p tali che $H \cap K = \{e\}$.
(i) Dimostrare che G è isomorfo a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
(ii) Determinare il numero di sottogruppi di G di ordine p.

174. Sia G un gruppo abeliano, sia k un intero positivo e poniamo $G^k = \{g^k \mid g \in G\}$.

(i) Mostrare che G^k è un sottogruppo di G e che nel gruppo G/G^k tutti gli elementi hanno ordine finito.

(ii) Sia G un gruppo ciclico di ordine n, calcolare la cardinalità di G/G^k.
(iii) Dare un esempio di un gruppo G tale che $G/G^{10} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.

175. Siano m e n interi positivi e indichiamo con $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ il gruppo degli omomorfismi da $\mathbb{Z}/m\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$ con l'operazione di somma.
(i) Dimostrare che $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/d\mathbb{Z}$, dove d è il massimo comun divisore di m e n.
(ii) Determinare il sottogruppo di ordine 12 di $\mathrm{Hom}(\mathbb{Z}/360\mathbb{Z}, \mathbb{Z}/420\mathbb{Z})$.

176. Sia G un gruppo e sia $\Delta = \{(x, x) \mid x \in G\}$.
(i) Dimostrare che Δ è un sottogruppo di $G \times G$.
(ii) Dimostrare che Δ è normale in $G \times G$ se e solo se G è abeliano.
(iii) Dimostrare che, se G è abeliano, $G \times G/\Delta$ è isomorfo a G.

177. Sia $(G, +)$ un gruppo abeliano finito di ordine n. Dimostrare che
(i) per ogni numero primo p che divide n, l'insieme

$$G_p = \{x \in G \mid \exists k \in \mathbb{N} \text{ tale che } p^k x = 0\}$$

è un sottogruppo di G;
(ii) se $x, y \in G$ hanno ordine rispettivamente a e b con $(a, b) = 1$, allora $\mathrm{ord}(x + y) = ab$;
(iii) G è ciclico se e solo se, per ogni primo p che divide n, G_p è un sottogruppo ciclico di G.

178. Siano $G = \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, $G' = \mathbb{Z}/36\mathbb{Z}$.
(i) Dimostrare che, dati omomorfismi $f, g \in \mathrm{Hom}(G, G')$, ponendo $(f + g)(x) = f(x) + g(x)$ per ogni $x \in G$, si ha un omomorfismo da G in G' e che con l'operazione

$$\mathrm{Hom}(G, G') \times \mathrm{Hom}(G, G') \ni (f, g) \longmapsto f + g \in \mathrm{Hom}(G, G')$$

l'insieme $\mathrm{Hom}(G, G')$ è un gruppo. Calcolare inoltre la cardinalità di $\mathrm{Hom}(G, G')$.
(ii) Determinare il numero degli omomorfismi suriettivi da G in G'.
(iii) Dimostrare che, per ogni $(a, b) \in G$, l'applicazione $\varphi_{(a,b)} : \mathrm{Hom}(G, G') \longrightarrow G'$ definita da $\varphi_{(a,b)}(f) = f(a, b)$ è un omomorfismo. Determinare inoltre la cardinalità del nucleo e dell'immagine di $\varphi_{(\overline{1},\overline{1})}$.

179. Sia $(G, +)$ un gruppo abeliano, e siano H, K due sottogruppi di G tali che $[G : H] = m$, $[G : K] = n$. Poniamo $d = [G : H \cap K]$. Dimostrare che
(i) $d \leq mn$;
(ii) $d \mid mn$;
(iii) $d = mn$ se e solo se $H + K = G$.

180. Sia G il sottogruppo del gruppo additivo $\mathbb{Q}$ dei numeri razionali definito da

$$G = \left\{ \frac{a}{b} \mid a \in \mathbb{Z},\ (b, 10) = 1 \right\}.$$

(i) Dimostrare che G non possiede sottogruppi isomorfi a $\mathbb{Z} \times \mathbb{Z}$.

(ii) Dimostrare che G possiede infiniti quozienti ciclici.

(iii) Dimostrare che G non possiede quozienti ciclici di ordine 3.

181. Siano G e H due gruppi ciclici non banali, e sia $f : G \longrightarrow H$ un omomorfismo iniettivo. Dimostrare che le seguenti condizioni sono necessarie e sufficienti per l'esistenza di un omomorfismo $g : H \longrightarrow G$ tale che $g \circ f$ sia un isomorfismo.

(i) Se G è finito, allora anche H è finito e, posti $|G| = a$, $|H| = b$, si ha $a \,|\, b$ e $(a, b/a) = 1$.

(ii) Se G è infinito, allora $H \simeq \mathbb{Z}$ e f è suriettivo.

182. Un sottogruppo M di un gruppo G si dice *massimale* se $M \neq G$ e per ogni L sottogruppo di G tale che $M \subsetneq L \subseteq G$ si ha $L = G$.

(i) Siano K, M due sottogruppi di un gruppo G tali che $K \trianglelefteq G$ e $K \subseteq M$. Dimostrare che M è un sottogruppo massimale di G se e solo se M/K è un sottogruppo massimale di G/K.

(ii) Dimostrare che in un gruppo abeliano finito G ogni sottogruppo $H \neq G$ è contenuto in un sottogruppo massimale di G.

(iii) Dimostrare che in un gruppo abeliano finito diverso dal solo elemento neutro i sottogruppi massimali sono tutti e soli quelli che hanno indice primo.

183. (i) Contare gli omomorfismi e gli omomorfismi iniettivi da $\mathbb{Z}/12\mathbb{Z}$ nel gruppo $\mathbb{Z}/4\mathbb{Z} \times \mathsf{S}_3$.

(ii) Descrivere tutti gli omomorfismi $\varphi : \mathbb{Z}/12\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \times \mathsf{S}_3$ per cui $\varphi(\overline{10})$ ha ordine 3.

184. Sia $G = (\mathbb{Z}/1000\mathbb{Z})^*$.

(i) Dimostrare che G non è un gruppo ciclico.

(ii) Sia $H = \{g \in G \mid \mathrm{ord}(g) \text{ è una potenza di } 2\}$; provare che H è un sottogruppo di G e calcolarne l'ordine.

(iii) Dimostrare che G ha un elemento di ordine 25 e dedurre da ciò che G/H è ciclico.

185. Sia G un gruppo abeliano e per ogni $k \in \mathbb{N}$ poniamo $G^k = \{g^k \mid g \in G\}$.

(i) Dimostrare che G^k è un sottogruppo di G per ogni k.

(ii) Supponendo che G sia finito di cardinalità n, caratterizzare gli interi k tali che $G^k = G$.

(iii) Dare un esempio di un gruppo G per cui $G^k \neq G$ per ogni $k > 1$.

(iv) Dare un esempio di un gruppo non banale G tale che $G^k = G$ per ogni $k \geq 1$.

186. Sia $G = \mathbb{Z}/3\mathbb{Z} \times \mathsf{S}_3$ con la struttura di gruppo data dal prodotto diretto.

(i) Determinare i possibili ordini dei sottogruppi di G.

(ii) Contare i sottogruppi ciclici di G.

2.5 Anelli e campi

187. Sia $f(x) = x^4 + x^3 - 3 \in \mathbb{F}_7[x]$. Determinare il numero di divisori di zero e l'inverso di $\overline{x+1}$ in $\mathbb{F}_7[x]/(f(x))$.

188. Sia m un numero intero e consideriamo il polinomio $f_m(x) = (x^2 - m)(x^4 - 25)$. Determinare, per ogni valore intero di m, il grado del campo di spezzamento di $f_m(x)$ su $\mathbb{Q}$.

189. Siano $f(x) = x^3 + 3x - 1$, $g(x) = x^2 - 2$.

(i) Detta α una radice complessa di $f(x)$, determinare il polinomio minimo di $1/(\alpha + 2)$ su $\mathbb{Q}$.

(ii) Determinare l'insieme dei numeri primi p per i quali i polinomi $f(x)$, $g(x)$, considerati con coefficienti in $\mathbb{F}_p$, hanno una radice comune.

190. Sia $f(x) = x^6 + 4x^3 + 2$.

(i) Detta α una radice complessa di $f(x)$, determinare il polinomio minimo di $1/\alpha^2$ su $\mathbb{Q}$.

(ii) Determinare il campo di spezzamento di $f(x)$ su $\mathbb{F}_7$.

191. Determinare il grado del campo di spezzamento di $x^6 - 4$ su $\mathbb{Q}$ e su $\mathbb{F}_{11}$.

192. Determinare tutti i numeri primi p per i quali il polinomio $x^6 + 1 \in \mathbb{F}_p[x]$ ha almeno una radice in $\mathbb{F}_p$.

193. Sia α una radice complessa di $x^4 - 2x^3 + x - 1$.

(i) Determinare un polinomio $g(x) \in \mathbb{Q}[x]$ tale che $\alpha^2 g(\alpha) = 1$.

(ii) Determinare, al variare dell'intero k, il grado $[\mathbb{Q}(\alpha^2 + k\alpha) : \mathbb{Q}]$.

194. Sia $\alpha \in \mathbb{C}$ una radice del polinomio $x^4 + 2x^2 + 2$. Calcolare il polinomio minimo di $\alpha^2 + 1$ e di $1/(\alpha + 2)$ su $\mathbb{Q}$.

195. Calcolare il grado del campo di spezzamento del polinomio $(x^3 - 2)(x^4 - 3)$ su $\mathbb{Q}$, su $\mathbb{F}_3$ e su $\mathbb{F}_{11}$.

196. Sia $\alpha = \sqrt{5} + i \in \mathbb{C}$.

(i) Calcolare il polinomio minimo $f(x)$ di α su $\mathbb{Q}$.

(ii) Calcolare il grado del campo di spezzamento del polinomio $f(x)$ su $\mathbb{Q}$ e su $\mathbb{F}_7$.

197. Sia $\alpha \in \mathbb{C}$ una radice del polinomio $x^4 - x - 1$. Determinare il polinomio minimo di $2\alpha - 1$ e di α^2 su $\mathbb{Q}$.

198. Determinare il grado del campo di spezzamento di $x^4 - 6x^2 - 3$ su $\mathbb{Q}$ e su $\mathbb{F}_{13}$.

199. Sia $\alpha = \sqrt{2 + \sqrt{7}} \in \mathbb{C}$.

(i) Determinare il grado di $\mathbb{Q}(\alpha)$ su $\mathbb{Q}$.

(ii) Determinare il grado del campo di spezzamento del polinomio minimo di α su $\mathbb{Q}$.

200. Sia $\alpha = \sqrt{2 + i\sqrt{2}}$.

(i) Determinare il polinomio minimo di α e di α^2+1 su $\mathbb{Q}$.
(ii) Determinare un polinomio $f(x) \in \mathbb{Q}[x]$ tale che $f(\alpha) = (\alpha^2+2\alpha)^{-1}$.

201. Determinare il grado del campo di spezzamento di x^8-4 su $\mathbb{Q}$ e su $\mathbb{F}_3$.

202. Determinare il grado del campo di spezzamento di x^4+26 su $\mathbb{Q}$, $\mathbb{F}_5$ e su $\mathbb{F}_7$.

203. Determinare il grado del campo di spezzamento di x^6-12x^3+27 su $\mathbb{Q}$ e su $\mathbb{F}_5$.

204. Determinare il polinomio minimo di $\sqrt{2+\sqrt{3}}$ su $\mathbb{Q}$ ed il grado del campo di spezzamento di tale polinomio.

205. Sia $f(x)$ il polinomio $(x^3-7)(x^2+3)$.
(i) Determinare il grado del campo di spezzamento di $f(x)$ su $\mathbb{Q}$.
(ii) Determinare il numero di divisori di zero in $\mathbb{F}_5[x]/(f(x))$.

206. Determinare il grado del campo di spezzamento di $2x^4+6x^2-5$ su $\mathbb{Q}$ e su $\mathbb{F}_{19}$.

207. Siano $\mathbb{K} \subseteq \mathbb{F}$ due campi, $f(x) = x^5+3x+3 \in \mathbb{K}[x]$ e α una radice di $f(x)$ in $\mathbb{F}$. Calcolare i possibili valori di $[\mathbb{K}(\alpha):\mathbb{K}]$ e $[\mathbb{K}(\alpha^7):\mathbb{K}]$ per $\mathbb{K}=\mathbb{Q}$ e per $\mathbb{K}=\mathbb{F}_2$.

208. Sia $\mathbb{K}$ un campo, $f(x) \in \mathbb{K}[x]$ un polinomio di grado positivo e $A = \mathbb{K}[x]/(f(x))$. Dimostrare che ogni divisore di zero è nilpotente se e solo se $f(x)$ è potenza di un polinomio irriducibile.

209. Contare il numero dei divisori di zero che non sono nilpotenti nell'anello $\mathbb{F}_5[x]/(x^3-2x+1)$.

210. Sia $x^4-a \in \mathbb{Z}[x]$ un polinomio *riducibile*. Dimostrare che
(i) se $a>0$, allora esiste $b \in \mathbb{N}$ tale che $a=b^2$;
(ii) se $a<0$, allora esiste $c \in \mathbb{N}$ tale che $a=-c^2$; inoltre, esiste $d \in \mathbb{N}$ tale che $c=2d^2$.

211. Calcolare il grado del campo di spezzamento del polinomio x^4+5x^2+5 su $\mathbb{Q}$ e su $\mathbb{F}_{11}$.

212. Sia $\alpha \in \mathbb{C}$ una radice del polinomio x^3-x^2-2x-1 e sia $\beta = \alpha^4-3\alpha^2$. Determinare
(i) il polinomio minimo di β su $\mathbb{Q}$;
(ii) un polinomio $g(x)$ a coefficienti razionali tale che $\beta g(\alpha)=1$.

213. Determinare il grado del campo di spezzamento del polinomio $(x^2+3)(x^3-5)$ su $\mathbb{Q}$.

214. Sia $f(x)$ il polinomio $x^{15}-1$.
(i) Fattorizzare e determinare il grado del campo di spezzamento di $f(x)$ su $\mathbb{F}_3$ e $\mathbb{F}_5$.
(ii) Quali sono i possibili gradi del campo di spezzamento $\mathbb{K}$ di $f(x)$ su $\mathbb{F}_p$ con p primo diverso da 3 e 5?

(iii) Per ogni grado d del punto precedente trovare un primo p, diverso da 3 e 5, per cui $[\mathbb{K} : \mathbb{F}_p] = d$.

215. Determinare il grado del campo di spezzamento del polinomio $(x^2+2)(x^4-2)$ su $\mathbb{Q}$ e su $\mathbb{F}_7$.

216. Sia $\mathbb{K}$ un campo, e siano α, β radici, rispettivamente, di x^2-5 e x^2+5 in una chiusura algebrica di $\mathbb{K}$.

(i) Determinare il grado del polinomio minimo di $\alpha+\beta$ su $\mathbb{K}$, per $\mathbb{K}=\mathbb{Q}$.

(ii) Sia $\mathbb{K}=\mathbb{F}_p$; quali sono i gradi che può avere il polinomio minimo di $\alpha+\beta$ su $\mathbb{F}_p$ al variare di p? Dare un esempio per ogni possibile grado.

(iii) Qual è in grado del polinomio minimo di $\alpha+\beta$ su $\mathbb{F}_{2011}$.

217. Sia $\mathbb{K}$ un campo e sia α una radice di $f(x)=x^4-3$ in una qualche chiusura algebrica di $\mathbb{K}$.

(i) Determinare il grado di $\mathbb{K}(\alpha)$ su $\mathbb{K}$, per $\mathbb{K}=\mathbb{Q}$ e per $\mathbb{K}=\mathbb{Q}(\sqrt{-3})$.

(ii) Determinare il grado del campo di spezzamento di $f(x)$ su $\mathbb{K}$ per $\mathbb{K}=\mathbb{Q}$ e per $\mathbb{K}=\mathbb{Q}(\sqrt{-3})$.

218. Sia $f(x)=x^5+x^2-x+4$.

(i) Determinare il campo di spezzamento di $f(x)$ su $\mathbb{F}_2$ e su $\mathbb{F}_3$.

(ii) Determinare, al variare di k tra gli interi positivi, i gradi dei fattori irriducibili di $f(x)$ su $\mathbb{F}_{3^k}$.

219. Sia α una radice del polinomio $x^4+2x^3+2x^2+x+3$. Determinare il polinomio minimo di $\alpha+1$ e di $\alpha^2+\alpha$ su $\mathbb{Q}$.

220. Sia $f(x)=x^4+3x^2+1\in\mathbb{Q}[x]$, e sia $\alpha\in\mathbb{C}$ una radice complessa di $f(x)$. Determinare

(i) il grado $[\mathbb{Q}(\alpha):\mathbb{Q}]$;

(ii) il grado del campo di spezzamento di $f(x)$ su $\mathbb{Q}$;

(iii) il polinomio minimo di $1/(\alpha+1)$ su $\mathbb{Q}$.

221. Determinare il grado del campo di spezzamento di x^4-4x^2+2 su $\mathbb{Q}$, su $\mathbb{Q}(i)$ e su $\mathbb{F}_7$.

222. Siano $\mathbb{K},\mathbb{E},\mathbb{F}$ i campi di spezzamento su $\mathbb{Q}$ di $x^{24}-1$, di x^8-1 e di x^3-1 rispettivamente.

(i) Dimostrare che $\mathbb{K}=\mathbb{E}\mathbb{F}$.

(ii) Determinare una base di $\mathbb{K}\cap\mathbb{R}$ come spazio vettoriale su $\mathbb{Q}$.

223. (i) Determinare i valori di $n\in\mathbb{N}$ per cui il polinomio $x^{2n}+x^n+1$ è divisibile per x^2+x+1 in $\mathbb{Q}[x]$.

(ii) Determinare il grado del campo di spezzamento del polinomio x^8+x^4+1 su $\mathbb{Q}$ e su $\mathbb{F}_7$.

224. Detta α una radice complessa di $x^4-x^3+x^2-x+1$, determinare, al variare di $c\in\mathbb{Q}$, il grado $[\mathbb{Q}(\alpha+c\alpha^{-1}):\mathbb{Q}]$.

225. Sia $f(x)=x^3+3x+1$.

(i) Determinare il grado del campo di spezzamento di $f(x)$ su $\mathbb{Q}$.

(ii) Determinare per quali numeri primi p il polinomio $f(x)$, considerato come polinomio a coefficienti in $\mathbb{F}_p$, ha una radice multipla in $\mathbb{F}_p$.

226. Sia $f(x) = x^9 - 1$.

(i) Dimostrare che $f(x)$ ha un fattore irriducibile di grado 6 su $\mathbb{F}_{11}$.

(ii) Determinare il grado del campo di spezzamento di $f(x)$ su $\mathbb{Q}$ e su $\mathbb{Q}(\zeta)$, dove $\zeta \in \mathbb{C}$ è una radice terza primitiva dell'unità.

227. Sia $\alpha \in \mathbb{C}$ una radice del polinomio $f(x) = x^4 + x + 1$.

(i) Determinare il polinomio minimo di $1/(\alpha + 1)$ e di α^2 su $\mathbb{Q}$.

(ii) Determinare il campo di spezzamento del polinomio $f(x)$ su $\mathbb{F}_5$.

228. Siano p un primo, $a \in \mathbb{F}_p^*$ e $f(x) = (x^4 - a)(x^4 + a) \in \mathbb{F}_p[x]$.

(i) Dimostrare che se $p \equiv 3 \pmod 4$ il campo di spezzamento di $f(x)$ su $\mathbb{F}_p$ ha grado 2.

(ii) Mostrare che si possono scegliere a e p con $p \equiv 1 \pmod 4$ tali che il campo di spezzamento di $f(x)$ su $\mathbb{F}_p$ abbia grado 1, 2 o 4.

229. Sia p un primo dispari, e sia $f(x) = x^6 + ax^3 + b \in \mathbb{F}_p[x]$.

(i) Dimostrare che il grado del campo di spezzamento di $f(x)$ su $\mathbb{F}_{p^2}$ può essere solo 1 o 3.

(ii) Provare che il grado del campo di spezzamento di $f(x)$ su $\mathbb{F}_p$ non può essere né 4 né 5.

(iii) Dimostrare che se $p \equiv 2 \pmod 3$ il grado del campo di spezzamento di $f(x)$ su $\mathbb{F}_p$ non può essere 3.

230. Sia $f(x) = (x^{15} - 1)(x^{12} - 1)$.

(i) Determinare, il grado del campo di spezzamento di $f(x)$ su $\mathbb{F}_2$ e su $\mathbb{F}_7$.

(ii) Determinare quali sono i possibili valori del grado del campo di spezzamento di $f(x)$ su $\mathbb{F}_p$ al variare di p fra i numeri primi.

231. Determinare il numero di soluzioni di $2x^4 - 41x^3 + 201x^2 - 71x - 91 = 0$ in $\mathbb{Z}/1635\mathbb{Z}$, ed esibire almeno 6 soluzioni distinte.

232. Sia $\alpha \in \mathbb{C}$ una radice di $x^3 - x - 1$.

(i) Scrivere $1/(\alpha + 2)$ come un polinomio in α a coefficienti razionali.

(ii) Determinare i gradi $[\mathbb{Q}(\alpha^2) : \mathbb{Q}]$ e $[\mathbb{Q}(\alpha^3) : \mathbb{Q}]$.

233. Sia $\alpha \in \mathbb{C}$ una radice del polinomio $f(x) = x^4 - 3x - 5$.

(i) Provare che $f(x)$ è irriducibile in $\mathbb{Q}[x]$.

(ii) Trovare il polinomio minimo di $2\alpha - 3$ su $\mathbb{Q}$.

(iii) Trovare il polinomio minimo di α^2 su $\mathbb{Q}$.

234. Dimostrare che l'anello $\mathbb{Z}[x]/(2x^2 + 17, x^2 + 6)$ è uno spazio vettoriale di dimensione 2 su $\mathbb{F}_5$.

235. Sia $\mathbb{K}$ il campo $\mathbb{Q}(\sqrt[3]{2}, i)$.

(i) Determinare il grado $[\mathbb{K} : \mathbb{Q}]$.

(ii) È vero che $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2} + i)$?

(iii) Determinare il polinomio minimo di $\sqrt[3]{2} + i$ su $\mathbb{Q}$.

236. (i) Calcolare i gradi $[\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q}]$ e $[\mathbb{Q}(\sqrt{3}-\sqrt{5}):\mathbb{Q}]$.
(ii) Trovare i polinomi minimi di $\sqrt{3}-\sqrt{5}$ e di $\sqrt{\sqrt{3}-\sqrt{5}}-1$ su $\mathbb{Q}$.

237. Determinare la fattorizzazione in irriducibili del polinomio $x^7+x^6+x^5+x^4+x^3+x^2+x+1$ in $\mathbb{C}[x]$, $\mathbb{Z}[x]$, $\mathbb{F}_5[x]$ e $\mathbb{F}_{17}[x]$.

238. Sia $f(x)=x^4+5x^3+5x^2-x+4$.
(i) Fattorizzare il polinomio $f(x)$ in $\mathbb{F}_7[x]$.
(ii) Contare i divisori di zero e gli elementi invertibili dell'anello $\mathbb{F}_7[x]/(f(x))$.

239. Sia $\alpha=2+\sqrt{5+\sqrt{-5}}\in\mathbb{C}$. Determinare $[\mathbb{Q}(\alpha):\mathbb{Q}]$ e $[\mathbb{Q}(\alpha^2):\mathbb{Q}]$.

240. Sia $f(x)=x^4+3x^3+x+1$.
(i) Calcolare il grado del campo di spezzamento di $f(x)$ su $\mathbb{F}_{2^k}$ e su $\mathbb{F}_{3^k}$ al variare dell'intero positivo k.
(ii) Sia $\alpha\in\mathbb{C}$ una radice di $f(x)$, determinare $[\mathbb{Q}(\alpha):\mathbb{Q}]$.

241. Determinare il grado del campo di spezzamento di $f(x)=x^4-2$ su $\mathbb{Q}$, su $\mathbb{F}_3$ e su $\mathbb{F}_{17}$.

Capitolo 3
Soluzioni

3.1 Successioni

1. (i) Procediamo per induzione. Verifichiamo i primi due casi in quanto il passo induttivo usa i due casi precedenti. Se $n = 2$ abbiamo $a_2 = 5/6$ e quindi l'asserto è vero con $b_2 = 5 \equiv -1 \pmod 6$. Per $n = 3$ si ha $a_3 = 17/36$ e quindi l'asserto è vero con $b_3 = 17 \equiv -1 \pmod 6$.

Supponiamo ora che $a_m = b_m/6^{m-1}$ con $b_m \equiv -1 \pmod 6$ per ogni $m \leq n$ e dimostriamo che anche a_{n+1} è della stessa forma. Dalla definizione si ha

$$a_{n+1} = \frac{a_n + a_{n-1}}{6} = \frac{1}{6}\left(\frac{b_n}{6^{n-1}} + \frac{b_{n-1}}{6^{n-2}}\right) = \frac{b_n + 6b_{n-1}}{6^n}.$$

Quindi basta porre $b_{n+1} = b_n + 6b_{n-1}$ e si ha anche $b_{n+1} \equiv b_n \equiv -1 \pmod 6$.

(ii) Procediamo per induzione. Anche qui verifichiamo i primi due casi. Se $n = 0$ abbiamo $c_0 = 5a_0 + (-1)^0 4/3^{-1} = 22$ e, se $n = 1$, abbiamo $c_1 = 5a_1 + (-1)^1 4/3^0 = 15 - 4 = 11$; quindi l'asserto è vero per i primi due valori di n. Supponiamo ora che $c_m = 22 \cdot 2^{-m}$ per ogni $m \leq n$. Allora

$$\begin{aligned}
c_{n+1} &= 5a_{n+1} + (-1)^{n+1}\frac{4}{3^n} \\
&= \frac{1}{6}(5a_n + 5a_{n-1}) - (-1)^n \frac{4}{3^n} \\
&= \frac{1}{6}\left(c_n - (-1)^n \frac{4}{3^{n-1}} + c_{n-1} - (-1)^{n-1}\frac{4}{3^{n-2}}\right) - (-1)^n \frac{4}{3^n} \\
&= \frac{22}{6}(2^{-n} + 2^{-(n-1)}) + (-1)^n\left(-\frac{2}{3^n} + \frac{2}{3^{n-1}} - \frac{4}{3^n}\right) \\
&= \frac{22}{2^{n+1}}
\end{aligned}$$

come richiesto.

R. Chirivì et al., *Esercizi scelti di Algebra, Volume 1*,
UNITEXT – La Matematica per il 3+2 107, DOI 10.1007/978-88-470-3961-2_3

2. (i) Per induzione su n. Se $n = 1$, $a_1 = 1$ e quindi la tesi è verificata. Supponendo la tesi vera per n, abbiamo

$$(a_{n+1}, 6) = (5a_n - 6a_{n-1}, 6) = (5a_n, 6) = (a_n, 6) = 1.$$

(ii) Per induzione su n. Per $n = 0, 1$ la tesi è vera per la definizione di a_0, a_1. Supponiamo la tesi vera per tutti gli a_i con $i \leq n$. Dalla definizione

$$a_{n+1} = 5a_n - 6a_{n-1}$$

abbiamo che $5 \mid a_{n+1}$ se e solo se $5 \mid a_{n-1}$. La tesi è quindi dimostrata.

3. (i) Dimostriamo per induzione su n sia la tesi che la disuguaglianza $a_n \geq \frac{1}{2}a_{n+1}$.

Per $n = 1$, da $a_1 = 1$, $a_2 = 2$ segue immediatamente che entrambe le disuguaglianze sono verificate.

Supponiamo ora le due disuguaglianze vere per $n - 1$. Poiché $a_{n+1} = a_n/2 + a_{n-1}$, dall'ipotesi induttiva $a_{n-1} \geq a_n/2$ segue $a_{n+1} \geq a_n$. Inoltre, utilizzando l'ipotesi induttiva $a_{n-1} \leq a_n$, abbiamo $a_{n+1} \leq 3a_n/2$; quest'ultima quantità è minore di $2a_n$ in quanto, visto che vale $a_1 \leq a_2 \leq \cdots \leq a_n$, a_n è positivo.

⟦Alternativamente, dimostriamo direttamente la disuguaglianza richiesta, ma sfruttando l'ipotesi induttiva per due valori consecutivi di n. Pertanto verifichiamo *due* casi iniziali: $a_2 = 2 \geq 1 = a_1$ e $a_3 = 2 \geq 2 = a_2$. Supposta vera la tesi per $n - 1$ e n, si ha $a_{n+1} = a_n/2 + a_{n-1} \geq a_{n-1}/2 + a_{n-2} = a_n$.⟧

(ii) Per dimostrare la tesi utilizziamo le tre ricorrenze

$$a_{2n} = \frac{1}{2}a_{2n-1} + a_{2n-2},$$

$$a_{2n+1} = \frac{1}{2}a_{2n} + a_{2n-1},$$

$$a_{2n+2} = \frac{1}{2}a_{2n+1} + a_{2n}$$

che sono tutte vere per $n \geq 2$. Ricavando a_{2n-1} dalla prima equazione e sostituendo nella seconda si ottiene $a_{2n+1} = 5a_{2n}/2 - 2a_{2n-2}$. Sostituendo questa espressione di a_{2n+1} nella terza equazione si ottiene la tesi.

4. (i) Per induzione su n. Per $n = 0$ e $n = 1$ l'uguaglianza si verifica facilmente. Supponendo la tesi vera per n, abbiamo $a_0^2 + a_1^2 + \cdots + a_n^2 + a_{n+1}^2 = a_n a_{n+1} + 2 + a_{n+1}^2 = a_{n+1}(a_n + a_{n+1}) + 2 = a_{n+1}a_{n+2} + 2$, cioè la tesi per $n + 1$.

(ii) Per induzione su n. Per $n = 0, 1, 2$ la tesi si verifica direttamente. Supponiamo la tesi vera per tutti gli a_i con $i \leq n$. Usando due volte la regola di ricorrenza, otteniamo $a_{n+3} = 2a_{n+1} + a_n$, per ogni $n \geq 0$, quindi $2 \mid a_{n+3}$ se e solo se $2 \mid a_n$ e quindi se e solo se $n \equiv 0 \pmod 3$.

5. Consideriamo la successione $a_n = F_n/F_k$. Essa soddisfa le condizioni date, in quanto $a_0 = F_0/F_k = 0$, $a_k = F_k/F_k = 1$ e

$$a_{n+1} = \frac{F_{n+1}}{F_k} = \frac{F_n + F_{n-1}}{F_k} = a_n + a_{n-1} \text{ per } n \geq 1.$$

Quindi una successione che soddisfi le condizioni date esiste.

Dimostriamo ora che per ogni tale successione come nel testo si ha $a_1 = 1/F_k$. Supponiamo infatti che $a_0, a_1, \dots$ sia una successione che soddisfa le condizioni e dimostriamo per induzione che questa successione coincide con la successione $b_n = a_1 F_n$.

L'uguaglianza è vera per $n = 0$ e $n = 1$ per costruzione. Supponendo che essa sia vera per tutti i numeri minori o uguali a n, si ha $a_{n+1} = a_n + a_{n-1} = a_1 F_n + a_1 F_{n-1} = a_1 F_{n+1}$. Da questo segue che necessariamente $1 = a_k = b_k = a_1 F_k$, ossia che $a_1 = 1/F_k$.

Infine, dimostriamo l'unicità della successione. Poiché abbiamo visto che per una tale successione si deve avere $a_0 = 0$ e $a_1 = 1/F_k$, l'induzione precedente prova che necessariamente $a_n = F_n/F_k$ per ogni n.

6. (i) Per le condizioni iniziali, $3 \mid a_0$, $3 \mid a_1$, $3 \nmid a_2$. Supponiamo ora $n \geq 1$ e osserviamo che $3 \mid 6a_{n-1}$ per ogni n. Se $3 \mid a_n$ allora $3 \mid 7a_n$ e quindi $3 \mid 7a_n - 6a_{n-1} = a_{n+2}$. Viceversa, se $3 \mid a_{n+2}$, allora $3 \mid a_{n+2} + 6a_{n-1} = 7a_n$; poiché 3 è primo e $3 \nmid 7$ si ha che $3 \mid a_n$. Ne segue che, per $n \geq 1$, $3 \mid a_n$ se e solo se $3 \mid a_{n+2}$ e quindi gli interi n cercati sono lo zero e tutti i naturali dispari.

(ii) Per $n = 0$ si ha $a_1 > a_0$. Dimostriamo per induzione che, se $n \geq 1$, si ha $a_{n+1} > a_n$ se n è dispari e $a_{n+1} < a_n$ se n è pari.

Consideriamo i primi 3 casi iniziali: dalla formula ricorsiva si ottiene $a_3 = 30$, $a_4 = 194$, per cui $a_2 > a_1$, $a_3 < a_2$ e $a_4 > a_3$. Ora supponiamo $n \geq 2$ e utilizziamo la formula ricorsiva per ottenere

$$a_{n+2} - a_{n+1} = 7a_n - 6a_{n-1} - 7a_{n-1} + 6a_{n-2} = 7(a_n - a_{n-1}) - 6(a_{n-1} - a_{n-2}).$$

Se $n + 1$ è dispari, $n - 1$ è dispari e quindi per ipotesi induttiva $a_n - a_{n-1} > 0$, mentre $n - 2$ è pari e, sempre per ipotesi induttiva, $a_{n-1} - a_{n-2} < 0$. Ne segue che $a_{n+2} - a_{n+1}$ è somma di due addendi positivi e quindi è positivo.

Viceversa, se $n + 1$ è pari, l'ipotesi induttiva dice che $a_n - a_{n-1} < 0$ e $a_{n-1} - a_{n-2} > 0$, da cui $a_{n+2} - a_{n+1}$ è somma di due addendi negativi e quindi è negativo.

7. Dimostriamo innanzitutto, per induzione su n, che $a_n = 31^{3^n}$ per ogni n. Per $n = 0$ si verifica che $31^{3^0} = 31^1 = 31 = a_0$. Supposta la tesi vera per n si ha che $a_{n+1} = a_n^3 = (31^{3^n})^3 = 31^{3^{n+1}}$.

Poiché $(31, 44) = 1$ le potenze di 31 sono periodiche modulo 44, ed il minimo periodo è l'ordine di 31 nel gruppo $(\mathbb{Z}/44\mathbb{Z})^*$, e quindi un divisore di $\phi(44) = 20$. Inoltre tale ordine è anche il minimo comune multiplo fra l'ordine di 31 modulo 4 e modulo 11.

Ora $31 \equiv -1 \pmod 4$ e quindi il primo ordine è 2. Inoltre $31 \equiv -2 \pmod{11}$ e, visto che $-2 \not\equiv 1 \pmod{11}$ mentre $(-2)^5 = -32 \equiv 1 \pmod{11}$, il secondo ordine cercato è 5. Ne segue che l'ordine di 31 in $(\mathbb{Z}/44\mathbb{Z})^*$ è uguale a 10.

Abbiamo dunque che $31^{3^{n+k}} \equiv 31^{3^n} \pmod{44}$ se e solo se $3^{n+k} \equiv 3^n \pmod{10}$. Visto che l'ordine di 3 in $(\mathbb{Z}/10\mathbb{Z})^*$ è 4, la successione $a_n = 31^{3^n}$ modulo 44 è periodica, con minimo periodo 4.

⟦Poiché l'ordine di 3 in $(\mathbb{Z}/20\mathbb{Z})^*$ è ancora uguale a 4, la sola osservazione che l'ordine di 31 in $(\mathbb{Z}/44\mathbb{Z})^*$ divide 20 è sufficiente per dire che k è al più 4, e basta escludere per verifica diretta i casi $k = 1$ e $k = 2$ per ottenere il risultato.⟧

8. Osserviamo che $202 = [2, 101] \mid a_n$ se e solo se $2 \mid a_n$ e $101 \mid a_n$.

Inoltre, per $p = 2$ e per $p = 101$, se $p \mid a_{n_0}$ allora $p \mid a_n$ per ogni $n \geq n_0$. Infatti, per induzione su n: per $n = n_0$ è vero per ipotesi, inoltre, se $p \mid a_n$ si ha $p \mid (202, a_n)$ e quindi $p \mid a_{n+1} = a_n + (202, a_n)$.

Ci siamo quindi ridotti a dimostrare che esiste m tale che $2 \mid a_m$ ed esiste un n tale che $101 \mid a_n$.

Consideriamo il primo 2: se k è pari allora anche $(202, k)$ è pari, e se k è dispari lo è anche $(202, k)$ e quindi $a_2 = k + (202, k)$ è sempre pari.

Mostriamo ora che esiste n tale che $101 \mid a_n$. Infatti sia $n \geq 2$, se $101 \nmid a_n$, e quindi per quanto detto precedentemente $101 \nmid a_m$ per ogni $m \leq n$, è facile calcolare che $a_{n+1} = a_2 + 2(n-1)$. Poiché la congruenza $2(n-1) + a_2 \equiv 0 \pmod{101}$ è risolubile ed ha soluzione $n \equiv -51a_2 + 1 \pmod{101}$, per un $n \geq 0$ che risolve tale congruenza si ha $101 \mid a_{n+1}$.

9. In primo luogo osserviamo che $3 \nmid a_n$ per ogni $n \geq 0$. Per $n = 0$ ed $n = 1$ questa proprietà è vera per ipotesi; per $n > 1$ si dimostra per induzione, dato che, se per assurdo avessimo che $3 \mid a_{n+1}$, avremmo che $3 \mid 5a_n$ e, dato che $(3, 5) = 1$, $3 \mid a_n$, che dà una contraddizione.

Dimostriamo ora la tesi ancora per induzione su n. Se $n = 1$ abbiamo $a_2 = 5a + 3$ e quindi $(a_2, a_1) = (5a + 3, a) = (3, a) = 1$. Supponiamo ora $(a_n, a_{n-1}) = 1$ per qualche $n \geq 2$, e sia d un divisore comune di a_{n+1} e a_n. Allora d divide anche $a_{n+1} - 5a_n = 3a_{n-1}$. Ma, poiché $d \mid a_n$, si ha $(d, 3) = 1$ e quindi $d \mid a_{n-1}$. In definitiva, $d \mid (a_n, a_{n-1}) = 1$.

10. (i) Per calcolo diretto, si trova che $a_0 = 2$, $a_1 = 8$, $a_2 = 34$, $a_3 = 152$. I numeri h e k cercati devono dunque soddisfare il seguente sistema

$$\begin{cases} 34 = 8h + 2k \\ 152 = 34h + 8k. \end{cases}$$

Risolvendo il sistema, si vede che l'unica possibilità è $h = 8$, $k = -15$. D'altra parte, questi valori vanno bene per ogni $n \geq 1$, in quanto

$$8(3^n + 5^n) - 15(3^{n-1} + 5^{n-1}) = (3 + 5)(3^n + 5^n) - 5 \cdot 3^n - 3 \cdot 5^n = 3^{n+1} + 5^{n+1}.$$

(ii) Osserviamo che 5 è l'inverso moltiplicativo di 3 modulo 7, quindi $7 \mid a_n$ equivale a $3^n + 3^{-n} \equiv 0 \pmod 7$, ossia, visto che 3 è invertibile modulo 7, a $3^{2n} + 1 \equiv 0 \pmod 7$. Esaminando le potenze di 3, si vede che $3^k + 1 \equiv 0 \pmod 7$ se e solo se $k \equiv 3 \pmod 6$. In particolare, i valori ammissibili di k sono tutti dispari, mentre si dovrebbe avere $k = 2n$ affinché 7 divida a_n. Pertanto non esiste alcun intero con la proprietà richiesta.

⟦Si può, alternativamente, osservare che $(\mathbb{Z}/7\mathbb{Z})^*$ ha sei elementi e, valutando $3^n + 3^{-n} \pmod 7$ per $n = 0, 1, 2, 3, 4, 5$, concludere che non esiste alcun n per cui $7 \mid a_n$.⟧

11. La formula ricorsiva dice che $a_n < a_{n+1}$ se e solo se $-a_{n-1} + 2a_{n-2} > 0$, ossia $a_{n-1} < 2a_{n-2}$. Dimostreremo per induzione che entrambe le disuguaglianze $a_n < a_{n+1}$ e $a_{n+1} < 2a_n$ sono vere per ogni $n \geq 0$. Dai casi iniziali assegnati si

ha immediatamente che le due disuguaglianze sono vere per $n = 0, 1$. Supponiamo ora le due tesi vere per tutti gli indici minori di n, e dimostriamole per l'indice n usando la formula ricorsiva.

Per ipotesi induttiva $a_{n-1} < 2a_{n-2}$, da cui $a_{n+1} = a_n - a_{n-1} + 2a_{n-2} > a_n - 2a_{n-2} + 2a_{n-2} = a_n$ e quindi $a_n < a_{n+1}$.

Per ipotesi induttiva abbiamo $a_{n-2} < a_{n-1} < a_n$, da cui $a_{n+1} = a_n - a_{n-1} + 2a_{n-2} < a_n - a_{n-1} + 2a_{n-1} = a_n + a_{n-1} < 2a_n$ e ricaviamo $a_{n+1} < 2a_n$.

12. (i) Dimostriamo la tesi per induzione su n. Per $n = 0$ si ha $(a_0, a_1) = (1, 1) = 1$, e quindi la tesi è vera. Sia ora $n > 0$, e supponiamo che la tesi sia vera per tutti i numeri minori di n. Abbiamo

$$(a_n, a_{n+1}) = (a_n, ha_n + ka_{n-1}) = (a_n, ka_{n-1}) = (a_n, k)$$

dove l'ultima uguaglianza è vera per l'ipotesi induttiva. Quindi la tesi è dimostrata se facciamo vedere che $(a_n, k) = 1$ per ogni $n \geq 0$. Anche a questo scopo usiamo l'induzione su n.

Se $n = 0, 1$, abbiamo $(a_0, k) = (a_1, k) = (1, k) = 1$. Supponiamo il risultato vero fino ad n e dimostriamolo per $n + 1$. Abbiamo

$$(a_{n+1}, k) = (ha_n + ka_{n-1}, k) = (ha_n, k) = (h, k) = 1$$

dove la penultima uguaglianza è vera per ipotesi induttiva. La dimostrazione è quindi completa.

(ii) Consideriamo i primi valori di $b_n = a_n^2 - 1$, risulta $b_0 = 0$, $b_1 = 0$, $b_2 = 106^2 - 1 = 105 \cdot 107$ e quindi il massimo comune divisore cercato è un divisore di $105 \cdot 107$. Inoltre, abbiamo $a_2 \equiv 1 \pmod{105}$, mentre $a_2 \equiv -1 \pmod{107}$.

Considerando la congruenza modulo 105 si ottiene immediatamente, per induzione su n, che $a_{n+1} = 35a_n + 71a_{n-1} \equiv 35 + 71 \equiv 1 \pmod{105}$, e quindi $b_n \equiv 1^2 - 1 \equiv 0 \pmod{105}$ per ogni $n \geq 0$.

Considerando la congruenza modulo 107 otteniamo

$$a_3 \equiv -35 + 71 = 36 \pmod{107}$$

e quindi $b_3 \equiv 36^2 - 1 \equiv 35 \cdot 37 \not\equiv 0 \pmod{107}$ e, poiché 107 è un numero primo, $(b_3, 107) = 1$.

Ne segue che il massimo comune divisore cercato è 105.

13. Dimostriamo entrambi gli enunciati per induzione. Se $n = 0$, allora (i) e (ii) corrispondono, rispettivamente, a $F_1 = F_1$ e a $0 = F_0$, pertanto sono banalmente verificate.

Supponiamo ora che *entrambe* (i) e (ii) siano verificate per $0, 1, \ldots, n$, e dimostriamole per $n + 1$.

Per la (i), vogliamo dimostrare che $\sum_{i=0}^{n+1} \binom{n+1}{i} F_{i+1} = F_{2n+3}$. Abbiamo:

$$\sum_{i=0}^{n+1} \binom{n+1}{i} F_{i+1} = \sum_{i=0}^{n+1} \left(\binom{n}{i} + \binom{n}{i-1} \right) F_{i+1}$$

$$= \sum_{i=0}^{n+1} \binom{n}{i} F_{i+1} + \sum_{i=0}^{n+1} \binom{n}{i-1} F_{i+1} .$$

Poiché $\binom{n}{n+1} = 0$, la prima delle due somme precedenti è $\sum_{i=0}^{n} \binom{n}{i} F_{i+1}$, e cioè F_{2n+1}. Per quanto concerne la seconda somma, ponendo $j = i - 1$ e osservando che $\binom{n}{-1} = 0$, abbiamo

$$\begin{aligned} \sum_{i=0}^{n+1} \binom{n}{i-1} F_{i+1} &= \sum_{j=0}^{n} \binom{n}{j} F_{j+2} = \sum_{j=0}^{n} \binom{n}{j} (F_j + F_{j+1}) \\ &= \sum_{j=0}^{n} \binom{n}{j} F_j + \sum_{j=0}^{n} \binom{n}{j} F_{j+1} \\ &= F_{2n} + F_{2n+1} . \end{aligned}$$

In definitiva, abbiamo

$$\sum_{i=0}^{n+1} \binom{n+1}{i} F_{i+1} = F_{2n+1} + F_{2n} + F_{2n+1} = F_{2n+2} + F_{2n+1} = F_{2n+3} .$$

Per quanto riguarda la (ii), abbiamo

$$\begin{aligned} \sum_{i=1}^{n+1} \binom{n+1}{i} F_i &= \sum_{i=1}^{n} \binom{n+1}{i} F_i + \binom{n+1}{n+1} F_{n+1} \\ &= \sum_{i=1}^{n} \left(\binom{n}{i} + \binom{n}{i-1} \right) F_i + \binom{n}{n} F_{n+1} \\ &= \sum_{i=1}^{n} \binom{n}{i} F_i + \sum_{j=0}^{n} \binom{n}{j} F_{j+1} = F_{2n} + F_{2n+1} = F_{2n+2} . \end{aligned}$$

14. (i) Per prima cosa osserviamo che il sistema

$$\begin{cases} \alpha + \beta = a_1 = 1 \\ \dfrac{1+\sqrt{13}}{2} \alpha + \dfrac{1-\sqrt{13}}{2} \beta = a_2 = 4 \end{cases}$$

che si ottiene per $n = 1$ e $n = 2$ ha sicuramente soluzione visto che le due equazioni sono indipendenti.

⟦Svolgendo esplicitamente i calcoli si trova subito $\alpha = 1 + \sqrt{13}/26$ e $\beta = 1 - \sqrt{13}/26$.⟧

Proviamo ora, per induzione, che le soluzioni α e β di questo sistema verificano la proprietà richiesta per ogni $n \geq 1$. I passi base $n = 1$ e $n = 2$ sono ovviamente

veri. Per il passo induttivo, sia $n \geq 2$ e assumiamo la tesi vera per ogni intero minore o uguale ad n. Allora risulta

$$\begin{aligned} a_n + 3a_{n-1} &= \alpha\left(\frac{1+\sqrt{13}}{2}\right)^{n-1}\left(\frac{1+\sqrt{13}}{2}+3\right) \\ &\quad + \beta\left(\frac{1-\sqrt{13}}{2}\right)^{n-1}\left(\frac{1-\sqrt{13}}{2}+3\right) \\ &= \alpha\left(\frac{1+\sqrt{13}}{2}\right)^{n-1}\left(\frac{7+\sqrt{13}}{2}\right) + \beta\left(\frac{1-\sqrt{13}}{2}\right)^{n-1}\left(\frac{7-\sqrt{13}}{2}\right) \\ &= \alpha\left(\frac{1+\sqrt{13}}{2}\right)^{n+1} + \beta\left(\frac{1-\sqrt{13}}{2}\right)^{n+1} \end{aligned}$$

e quindi la tesi è vera anche per $n+1$.

(ii) Facciamo vedere che a_n è pari se e solo se $n \equiv 2 \pmod 3$. Infatti, usando due volte la definizione ricorsiva della succisione data, otteniamo $a_n = 4a_{n-2} + 3a_{n-3}$ per ogni $n \geq 4$. Quindi a_n è pari se e solo se a_{n-3} è pari; in altre parole, la parità del termine a_n dipende solo dalla classe di resto modulo 3 di n. Ma allora il nostro asserto è subito provato osservando che a_1 è dispari, a_2 è pari e $a_3 = a_2 + 3a_1 = 7$ è ancora dispari.

3.2 Combinatoria

15. (i) Ogni elemento $x \in X$ deve essere in A o B o C e le tre possibilità si escludono a vicenda visto che A, B e C hanno intersezione a due a due vuota. Il numero di terne cercate è quindi 3^n.

(ii) Ragioniamo come nel primo punto. Ogni elemento $x \in X$ deve essere in uno degli insiemi

$$A \setminus (B \cup C), \quad B \setminus (A \cup C), \quad C \setminus (A \cup B), \quad (A \cap B) \setminus C,$$
$$(A \cap C) \setminus B, \quad (B \cap C) \setminus A, \quad A \cap B \cap C.$$

Ovviamente queste 7 possibilità si escludono a vicenda. Il numero di terne è quindi 7^n come richiesto.

16. Osserviamo, per prima cosa, che la sola coppia di elementi uguali in X è la coppia $(1,1)$. Quindi possiamo dividere X nei seguenti sottoinsiemi disgiunti: $\{(1,1)\}$, $X_1 = \{(m,n) \mid 1 \leq m < n \leq 100,\ (m,n) = 1\}$ e $X_2 = \{(m,n) \mid 1 \leq n < m \leq 100,\ (m,n) = 1\}$.

E' anche chiaro che X_1 e X_2 hanno lo stesso numero di elementi in quanto la mappa $X_1 \ni (m,n) \longmapsto (n,m) \in X_2$ è una biezione tra essi.

Inoltre, raggruppando assieme tutti gli elementi con n nella seconda coordinata, per $n = 1, 2, \ldots, 100$, abbiamo $|X_1| = \sum_{n=2}^{100} \phi(n)$.

Allora possiamo concludere

$$|X| = 1 + |X_1| + |X_2| = 1 + 2|X_1| = 1 + 2\sum_{n=2}^{100} \phi(n) = 2\sum_{n=1}^{100} \phi(n) - 1$$

che è quanto dovevamo provare.

17. Per prima cosa determiniamo l'insieme di tutti gli interi n che soddisfano le condizioni $(n, 18) = 6$ e $n \equiv 2 \pmod 7$; senza, cioè, considerare i vincoli dati dalle disuguaglianze.

La prima condizione può essere riscritta come 6 divide n, 9 non divide n, cioè $n = 6h$ e $h \not\equiv 0 \pmod 3$ per qualche intero h. Ora la seconda condizione diventa $6h \equiv 2 \pmod 7$, cioè $h \equiv -2 \pmod 7$ e quindi abbiamo $h = 7k - 2$ per qualche intero k. Possiamo ora riusare quanto appena trovato per riscrivere $h \not\equiv 0 \pmod 3$ come $7k - 2 \not\equiv 0 \pmod 3$, cioè $k \not\equiv -1 \pmod 3$, e quindi $k = 3u$ o $k = 3u + 1$ per qualche intero u. Sostituendo a ritroso arriviamo a $n = 6h = 6(7k - 2) = 6(7 \cdot 3u - 2) = 126u - 12$ o $n = 6h = 6(7k - 2) = 6(7 \cdot (3u + 1) - 2) = 126u + 30$.

Imponiamo allora le condizioni $1 \le n \le 10000$ per trovare: nel primo caso $1 \le 126u - 12 \le 10000$ e quindi $1 \le u \le 79$, per un totale di 79 soluzioni; nel secondo caso $1 \le 126u + 30 \le 10000$ e quindi $0 \le u \le 79$, per un totale di 80 soluzioni.

Concludiamo che l'insieme assegnato ha quindi $79 + 80 = 159$ elementi.

18. I divisori positivi di $3^{40} \cdot 5^{25}$ sono gli interi della forma $3^n 5^m$ con $0 \le n \le 40$, $0 \le m \le 25$.

La congruenza richiesta diventa ora $3^n 5^m \equiv 1 \pmod 7$. Le potenze di 3 modulo 7 sono, nell'ordine, 1, 3, 2, -1, -3 e -2, poi si riparte da 1. In particolare, $5 \equiv -2 \equiv 3^5 \pmod 7$. Quindi possiamo riscrivere la congruenza su n e m come $3^{n+5m} \equiv 1 \pmod 7$.

Abbiamo appena visto che 3 ha ordine moltiplicativo 6 modulo 7 e quindi abbiamo $n + 5m \equiv 0 \pmod 6$, cioè $n \equiv m \pmod 6$.

Allora per trovare la cardinalità richiesta dobbiamo contare il numero di coppie (n, m) con $0 \le n \le 40$, $0 \le m \le 25$ e $n \equiv m \pmod 6$.
Visto che $40 = 6 \cdot 6 + 4$ abbiamo $7 = 6 + 1$ soluzioni per ogni m congruo a $0, \ldots, 4$ modulo 6 e, visto che $25 = 4 \cdot 6 + 1$, tali possibili m sono 22 per un totale di 154 soluzioni.
A queste dobbiamo aggiungere quelle con $m \equiv 5 \pmod 6$: per ogni tale m abbiamo 6 possibili valori di n e, visto che m può essere 5, 11, 17 o 23 otteniamo altre 24 soluzioni.

In conclusione la cardinalità cercata è $154 + 24 = 178$.

19. Soluzione 1. Procediamo in diversi passi.

Se n fosse una potenza di due, diciamo $n = 2^a$, allora anche $\phi(n) = 2^{a-1}$ lo sarebbe. Quindi esiste un primo dispari che divide n.

Se p è un primo che divide n allora $p - 1$ divide 12 quindi $p - 1$ può essere 1, 2, 3, 4, 6 o 12. Ma essendo p primo le possibilità sono $p = 2, 3, 5, 7, 13$.

Se q è un primo e q^2 divide n allora q divide anche $\phi(n)$. Quindi tale primo può essere solo 2 o 3.

Se 5 divide n, allora 5^2 non divide n per quanto appena provato e quindi $n = 5m$ con $(5, m) = 1$. Allora si ha $12 = \phi(n) = 4\phi(m)$ e quindi $\phi(m) = 3$ che è impossibile in quanto la funzione di Eulero assume solo 1 come valore dispari.

Se 7 divide n, allora 7^2 non divide n e quindi $n = 7m$ con $(7, m) = 1$. Allora si ha $12 = \phi(n) = 6\phi(m)$ e quindi $\phi(m) = 2$.

Sia ora q un primo che divide m allora $q - 1$ divide $\phi(m) = 2$ e quindi si hanno le sole possibilità $q = 2$ e $q = 3$. Inoltre 9 non può dividere m perché altrimenti 3 dividerebbe $\phi(m) = 2$. Allo stesso modo 8 non può dividere m perché altrimenti 4 dividerebbe $\phi(m)$. Quindi si ha $m = 2^a 3^b$ con $a = 0,\ 1,\ 2$ e $b = 0,\ 1$. Per verificare diretta di questi sei valori vediamo che $\phi(m) = 2$ per $m = 3,\ 4,\ 6$.

Allora abbiamo le tre possibilità $n = 21$, $n = 28$ e $n = 42$.

Se 13 divide n, si ha che 13^2 non divide n e quindi $m = 13n$ con $(13, m) = 1$. Allora $12 = \phi(n) = 12\phi(m)$ e quindi $\phi(m) = 1$ da cui $m = 1$ o $m = 2$. Abbiamo le due soluzioni $n = 13$ e $n = 26$.

Se nessuno dei casi precedenti si verifica allora $n = 2^a 3^b$ con a e b naturali e $b > 0$. In tal caso $12 = \phi(n) = 2^{a-1} \cdot 2 \cdot 3^{b-1} = 2^a 3^{b-1}$ e quindi $a = 2$ e $b = 2$, cioè $n = 36$.

Possiamo allora concludere che $\phi(n) = 12$ se e solo se n è un elemento dell'insieme $\{13,\ 21,\ 26,\ 28,\ 36,\ 42\}$.

Soluzione 2. Sia $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ la fattorizzazione di n in prodotto di primi. Per la moltiplicatività della funzione di Eulero, $\phi(n) = \prod_{i=1}^{k} \phi(p_i^{\alpha_i})$. Salvo il caso $p_i^{\alpha_i} = 2$, $\phi(p_i^{\alpha_i}) = (p_i - 1)p_i^{\alpha_i}$ è sempre un numero pari, quindi abbiamo solo le possibilità di scomporre 12 come $1 \cdot 2 \cdot 6$, $2 \cdot 6$, $1 \cdot 12$, 12, dove il fattore 1 può comparire solo se $2|n$ ma $4 \nmid n$.

Consideriamo il caso $\phi(p_i^{\alpha_i}) = 2$: se $p_i = 2$ abbiamo solo il caso $p_i^{\alpha_i} = 4$, altrimenti abbiamo solo il caso $p_i^{\alpha_i} = 3$.

Consideriamo il caso $\phi(p_i^{\alpha_i}) = 6$: se $p_i = 3$ abbiamo solo il caso $p_i^{\alpha_i} = 9$, altrimenti abbiamo solo il caso $p_i^{\alpha_i} = 7$.

Consideriamo infine il caso $\phi(p_i^{\alpha_i}) = 12$: è immediato verificare che $p_i \neq 2, 3$ quindi necessariamente $p_i - 1 = 12$, ossia $p_i^{\alpha_i} = 13$.

Tendendo conto che i fattori $p_i^{\alpha_i}$ devono essere primi fra loro, abbiamo dunque solo le seguenti possibilità per n: $4 \cdot 9 = 36$, $4 \cdot 7 = 28$, $3 \cdot 7 = 21$, $2 \cdot 3 \cdot 7 = 42$, 13, $2 \cdot 13 = 26$. Esse soddisfano tutte la condizione data.

20. Visto che $n^2 = x + y \leq 49 + 49 = 98$ abbiamo $n \leq 9$. Consideriamo prima il caso $n \leq 7$.

Allora tutte le terne $(h, n^2 - h, n)$ con $h = 0, \ldots, n^2$ risolvono le nostre condizioni. Per ogni $n \leq 7$ abbiamo quindi $n^2 + 1$ terne.

Se invece $n = 8$ allora abbiamo le terne $(h, 64 - h, 8)$ con $h = 15, \ldots, 49$, questo per rispettare il vincolo $0 \leq x, y < 50$. In tutto $49 - 15 + 1 = 35$ terne.

Analogamente per $n = 9$ abbiamo le terne $(h, 81 - h, 9)$ con $h = 32, \ldots, 49$ e quindi $49 - 32 + 1 = 18$ terne.

Il numero totale richiesto di terne è quindi: $1 + 2 + 5 + 10 + 17 + 26 + 37 + 50 + 35 + 18 = 201$.

21. La formula per la funzione ϕ di Eulero si può riscrivere come

$$\frac{\phi(n)}{n} = \prod_{p|n} \frac{p-1}{p}.$$

Se q è il più grande primo che divide n, allora q è anche il più grande primo che divide il denominatore di $\phi(n)/n$: infatti, q appare al denominatore di $(q-1)/q$ e non può essere cancellato da nessun numeratore di $(p-1)/p$ in quanto $p-1 < q$.

Quindi, se $\phi(n)/n = 2/5$, necessariamente il più grande primo che divide n è 5. Consideriamo gli interi n di questo tipo. Se n è divisibile per 2 e per 5, ma non per 3, si ha

$$\frac{\phi(n)}{n} = \frac{1}{2} \cdot \frac{4}{5} = \frac{2}{5}$$

e dunque la condizione è soddisfatta. In tutti gli altri casi, cioè per n non divisibile per 2 o divisibile per 3, un semplice calcolo dice che la condizione non è soddisfatta.

22. Siano $D = \{1 \le d \le n \mid d \text{ divide } n\}$ e $\Phi = \{1 \le k \le n \mid (k,n) = 1\}$. Se $x \in D \cap \Phi$ si ha $x = (x,n) = 1$, da cui $|D \cap \Phi| = 1$.

Per dimostrare (i) basta usare il Principio di Inclusione Esclusione. Abbiamo

$$|D| + |\Phi| = |D \cup \Phi| + |D \cap \Phi| = |D \cup \Phi| + 1 \le n + 1.$$

Per quanto riguarda (ii), osserviamo che l'uguaglianza richiesta è verificata se e solo se $|D \cup \Phi| = n - 1$, ossia se e solo se esiste *esattamente* un intero k con $1 \le k \le n$ che non è né un divisore di n né primo con n.

Se n è un numero primo, allora $d(n) = 2$ e $\phi(n) = n - 1$, da cui $d(n) + \phi(n) = n + 1$. Quindi è sufficiente considerare i numeri composti. Se $n = ab$ con $a > 1$ e $b > 4$, allora ci sono almeno due numeri, $a(b-1)$ e $a(b-2)$, che non sono né divisori di n né primi con n, quindi per tali numeri l'uguaglianza richiesta non è verificata.

Supponiamo che $n = p_1 \cdots p_k$ sia la scomposizione di n in fattori primi, eventualmente ripetuti, con $p_1 \le p_2 \le \cdots \le p_k$. Ponendo $a = p_1$ e $b = p_2 \cdots p_k$ e usando quanto sopra dimostrato, si ha che $p_2 \cdots p_k = 2, 3, 4$, da cui $n = 4, 6, 9, 8$. Per verifica diretta, il caso $n = 4$ va escluso, infatti $d(4) + \phi(4) = 3 + 2 = 5$, mentre gli altri casi danno soluzioni

$$d(6) + \phi(6) = 4 + 2 = 6, \quad d(9) + \phi(9) = 3 + 6 = 9, \quad d(8) + \phi(8) = 4 + 4 = 8.$$

23. Osserviamo che i numeri naturali che soddisfano la proprietà richiesta sono necessariamente multipli di 3, e quindi sono della forma $n = 3^a m$, dove $(m,3) = 1$. Inoltre si deve avere $a \le 2$, perché altrimenti sia n che $\phi(n) = 2 \cdot 3^{a-1}\phi(m)$ sarebbero multipli di 9. Ora, n deve essere dispari, perché da $3 \mid n$ si ha $2 \mid \phi(n)$ e quindi 2 dividerebbe $(n, \phi(n))$. Infine, tutti i primi $p > 3$ che dividono n devono comparire nella fattorizzazione di n con potenza 1, perché altrimenti si avrebbe $p \mid (n, \phi(n))$. Abbiamo dunque due casi.

(1) L'intero n è un multiplo di 9, cioè $n = 9m$ con $(m, 3) = 1$ ed m dispari e libero da quadrati. Allora da $n \leq 120$ segue che $m \leq 13$. Se $p \mid m$ allora $3 \nmid p - 1$, perché altrimenti $9 \mid (n, \phi(n))$. Le uniche possibilità sono dunque $m = 1, 5, 11$, che danno i valori accettabili $n = 9, 45, 99$.

(2) Supponiamo, invece, che l'intero m non sia un multiplo di 9, cioè $n = 3m$ con $(m, 3) = 1$ ed m dispari e libero da quadrati. Se $n = 3p$ con p primo, allora $\phi(n) = 2(p - 1)$ e quindi la condizione richiesta è rispettata se e solo se $3 \mid p - 1$. Poiché $n \leq 120$, si ha che $p \leq 40$: gli unici primi che rispettano la condizione data sono 7, 13, 19, 31, 37, che danno i valori accettabili $n = 21, 39, 57, 93, 111$.

Se, infine, $n = 3m$ dove m è il prodotto di almeno due primi distinti, necessariamente maggiori di 3, da $m \leq 40$ si ha che l'unica possibilità è $m = 5 \cdot 7$, che dà il valore accettabile $m = 105$.

24. Le possibili classi di resto modulo 2 delle terne (a, b, c) sono tre: $(1, 0, 0)$, $(0, 1, 0)$ e $(0, 0, 1)$. Le possibili classi di resto modulo 3 sono invece 12: $(0, x, y)$, $(x, 0, y)$ e $(x, y, 0)$, dove x e y sono diverse da zero.

In totale, ci sono dunque 36 classi di resto modulo 6 delle terne cercate. Fissata una classe di resto modulo 6, ci sono $10^3 = 1000$ terne che sono in quella classe, visto che $60/6 = 10$. Pertanto il numero delle terne cercate è $36 \cdot 1000 = 36000$.

25. Dimostriamo la tesi per induzione su $k = \omega(m)$. Si ha $k = 0$ se e solo se $m = 1$, per cui si ottiene

$$1 = \frac{\phi(1)}{1} \geq \frac{1}{0+1} = 1.$$

Supponiamo ora di avere dimostrato l'enunciato per $\omega(m) = k$, e dimostriamolo per $\omega(m) = k + 1$. Sia $m = p_1^{\alpha_1} \cdots p_{k+1}^{\alpha_{k+1}}$ con $p_1 < p_2 < \cdots < p_{k+1}$ e $\alpha_i > 0$ per ogni i. Sia poi $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

Per ipotesi induttiva, $\phi(n)/n \geq 1/(k+1)$; inoltre, evidentemente $p_i \geq i + 1$ per ogni i, da cui in particolare

$$1 - \frac{1}{p_{k+1}} \geq 1 - \frac{1}{k+2} = \frac{k+1}{k+2}.$$

Abbiamo dunque

$$\frac{\phi(m)}{m} = \frac{\phi(n)}{n} \cdot \left(1 - \frac{1}{p_{k+1}}\right) \geq \frac{1}{k+1} \cdot \frac{k+1}{k+2} = \frac{1}{k+2}.$$

26. I numeri che soddisfano le prime due proprietà sono $8 \cdot 9 \cdot 9 \cdot 9 - 1$: infatti, ci sono 8 possibilità per la prima cifra e 9 per tutte le altre, con l'eccezione del numero 1000. All'interno di essi, quelli che *non* soddisfano la terza proprietà sono tutti e soli quelli che hanno tutte le cifre distinte: ci sono 8 possibilità per la prima cifra; 8 possibilità per la seconda, 9 meno quella già usata per la prima cifra; 7 per la terza, 9 meno quelle già usate per le prime due cifre e 6 per la quarta cifra, 9 meno quelle già usate per le prime tre cifre.

Quindi i numeri di questo tipo sono $8 \cdot 8 \cdot 7 \cdot 6$. Ne segue che i numeri cercati sono $8 \cdot 9 \cdot 9 \cdot 9 - 1 - 8 \cdot 8 \cdot 7 \cdot 6 = 3143$.

27. (i) Ci sono due possibilità per $f(1)$: $f(1) = 1$ e $f(1) = 2$. Sia ora $2 \le i \le n$; supposto di aver scelto i valori $f(1), \dots, f(i-1)$, per ipotesi compresi in $\{1, \dots, i\}$ e distinti fra loro, $f(i)$ ha 2 possibilità, e cioè gli elementi di $\{1, \dots, i+1\} \setminus \{f(1), \dots, f(i-1)\}$. Infine, scelti $f(1), \dots, f(n-1)$, per $f(n)$ c'è solo una possibilità, l'unico elemento di $\{1, \dots, n\}$ distinto da $f(1), \dots, f(n-1)$. Pertanto la cardinalità dell'insieme cercato è 2^{n-1}.

(ii) Sia x_n la cardinalità dell'insieme dato, che chiamiamo X_n. Per $n = 1, 2$ tutte le permutazioni soddisfano la condizione data, pertanto $x_1 = 1 = F_2$ e $x_2 = 2 = F_3$.

Per ottenere la tesi è dunque sufficiente dimostrare che $x_{n+1} = x_n + x_{n-1}$ per $n \ge 2$. Poiché necessariamente $f(n+1) = n+1$ o $f(n+1) = n$, dividiamo l'insieme X_{n+1} in due sottoinsiemi: $Y_{n+1} = \{f \in X_{n+1} \mid f(n+1) = n+1\}$ e $Z_{n+1} = \{f \in X_{n+1} \mid f(n+1) = n\}$.

Gli elementi di Y_{n+1} sono in corrispondenza biunivoca con gli elementi di X_n e sono quindi x_n. Se invece $f \in Z_{n+1}$, allora, poiché $f(i) \le n$ per $i = 1, \dots, n-1$, necessariamente $f(n) = n+1$. Ne segue che Z_{n+1} è in corrispondenza biunivoca con X_{n-1} e quindi ha x_{n-1} elementi.

28. (i) Il numero dei sottoinsiemi richiesti può essere ottenuto sommando il numero N dei sottoinsiemi di X con 3 elementi tutti tra loro congrui modulo 5, con il numero M dei sottoinsiemi di X con 3 elementi, esattamente due dei quali congrui modulo 5. Poiché X contiene 20 elementi di ognuna delle classi modulo 5, abbiamo che N è dato dal numero di scelte di una classe modulo 5 per il numero di sottoinsiemi della classe scelta, cioè $N = 5 \cdot \binom{20}{3}$. Analogamente M è dato dal numero di scelte di una classe modulo 5 per il numero di sottoinsiemi di due elementi nella classe scelta per il numero di scelte di un elemento fuori dalla classe scelta, quindi $M = 5 \cdot \binom{20}{2} \cdot 80$. Svolgendo i calcoli otteniamo $N + M = 81700$.

⟦Lo stesso risultato poteva essere ottenuto sottraendo dal numero $\binom{100}{3}$ di tutti i sottoinsiemi di X con 3 elementi, il numero $\binom{5}{3}20^3$ dei sottoinsiemi con 3 elementi in classi distinte modulo 5.⟧

(ii) L'insieme X contiene 20 elementi di ognuna delle classi modulo 5. Le applicazioni da X in X che dobbiamo contare mandano ognuno dei 100 elementi $n \in X$ in uno dei 20 elementi della classe di $n+1$ modulo 5 che sono contenuti in X. Il numero cercato è quindi 20^{100}.

29. (i) La condizione $(xy, 6) = 1$ è equivalente a $(x, 6) = 1$ e $(y, 6) = 1$, cioè si chiede di contare le coppie ordinate di elementi di X con entrambe le coordinate coprime con 6. Ora, posto $X_i = \{x \in X \mid x \equiv i \pmod 6\}$ per $i \in \{1, 2, 3, 4, 5, 6\}$, abbiamo che $X = \bigsqcup_{i=1}^{6} X_i$ e per ogni $x \in X_i$ si ha $(x, 6) = (i, 6)$. Ne segue che $x \in X$ è coprimo con 6 se e solo se $x \in X_1$ o $x \in X_5$. Poiché $100 = 16 \cdot 6 + 4$, risulta $|X_1| = 17$ e $|X_5| = 16$. Quindi in X ci sono 33 elementi coprimi con 6.

Le coppie ordinate di elementi di X con entrambe le coordinate coprime con 6 sono 33^2.

(ii) Sia $A = \{(x, y) \in X^2 \,|\, x < y + 6\}$. Per ogni $y = 1, 2, \ldots, 95$ sia $X_y = \{1, \ldots, y + 5\}$, e, per $96 \le y \le 100$, poniamo $X_y = X$. È chiaro che

$$A = \bigsqcup_{y=1}^{100} X_y \times \{y\}$$

e quindi, trattandosi di un'unione disgiunta,

$$\begin{aligned} |A| &= \sum_{y=1}^{100} |X_y| \\ &= \sum_{y=1}^{95} (y + 5) + 5 \cdot 100 \\ &= 500 + \sum_{y=6}^{100} y \\ &= 500 + 100 \cdot 101/2 - (1 + 2 + 3 + 4 + 5) \\ &= 5535. \end{aligned}$$

30. (i) Le applicazioni dell'insieme A sono biettive, quindi per ogni $y \in X$, esiste $x \in X$ tale che $y = f(x)$. Dalla condizione $f^2(x) \equiv f(x) \pmod 2$ si ottiene $f(y) \equiv y \pmod 2$ per ogni $y \in X$, quindi le applicazioni cercate sono esattamente le applicazioni biettive da X in X che mandano i numeri pari nei numeri pari e i dispari nei dispari. Ne segue $|A| = 50!50!$.

(ii) Sia $f \in B$ e sia $Y = f^{-1}(1)$, allora Y è non vuoto perché $1 \in f(X)$. Inoltre $f(Y) = \{1\}$ e $1 \notin f(X \setminus Y)$. Si verifica facilmente che la condizione $f^2(X) = \{1\}$ è equivalente a $\{1\} = f(Y) \subseteq Y$ e $f(X \setminus Y) \subseteq Y$, allora per quanto detto sopra $f(X \setminus Y) \subseteq Y \setminus \{1\}$.

Le applicazioni dell'insieme B per le quali $Y = f^{-1}(1)$ è un sottoinsieme fissato di X con $1 \in Y$ e $|Y| = k + 1$ sono quindi tante quante le applicazioni da $X \setminus Y$ in $Y \setminus \{1\}$, cioè k^{99-k}. Per ogni $k \ge 0$ esistono $\binom{99}{k}$ sottoinsiemi Y di cardinalità $k + 1$ in X che contengono 1, quindi

$$|B| = \sum_{k=0}^{99} \binom{99}{k} k^{99-k}.$$

31. (i) È chiaro che $d \,|\, 144000 = 2^7 3^2 5^3$ se e solo se $d = 2^a 3^b 5^c$ con $0 \le a \le 7$, $0 \le b \le 2$ e $0 \le c \le 3$. Il numero dei divisori di un tale d è $(a + 1)(b + 1)(c + 1)$ ed è quindi pari se e solo se almeno uno tra a, b, c è dispari. Il numero dei d con un numero pari di divisori si ottiene sommando il numero dei d tali che: a è dispari e b, c sono qualsiasi, $4 \cdot 3 \cdot 4 = 48$ possibilità; a è pari, b dispari e c qualsiasi,

$4 \cdot 1 \cdot 4 = 16$ possibilità e, infine, a e b sono pari e c è dispari, con $4 \cdot 2 \cdot 2 = 16$ possibilità.

Quindi X ha 80 elementi.

⟦Questo risultato poteva essere ottenuto sottraendo dal numero $8 \cdot 3 \cdot 4 = 96$ di tutti i divisori di 144000, il numero di quelli con un numero dispari di divisori e quindi con a, b, c pari, cioè $4 \cdot 2 \cdot 2 = 16$.⟧

(ii) Per quanto riguarda l'insieme Y, osserviamo che un numero che è un quadrato è anche un cubo se e solo se è una sesta potenza. Ne segue che $d = 2^a 3^b 5^c \in Y$ se e solo se a, b, c sono pari, ma non tutti divisibili per 6. Si ha quindi $|Y| = 4 \cdot 2 \cdot 2 - 2 \cdot 1 \cdot 1 = 14$.

32. (i) Sia $X_0 = \{x \in X \mid x \equiv 0 \pmod 2\}$ e $X_1 = \{x \in X \mid x \equiv 1 \pmod 2\}$. Per ogni $A \subseteq X$, posto $A_i = A \cap X_i$ per $i = 0, 1$, si ha $A = A_0 \cup A_1$ e $\sum_{a \in A} a \equiv |A_1| \pmod 2$.

Quindi abbiamo $A \in \mathcal{A}$ se e solo se A_1 ha cardinalità pari. Allora i sottoinsiemi $A \in \mathcal{A}$ si ottengono scegliendo un qualsiasi sottoinsieme A_0 di X_0, per un totale di 2^{50} scelte, e un sottoinsieme A_1 di X_1 con un numero pari di elementi, per un totale di $\sum_{k=0}^{25} \binom{50}{2k} = 2^{49}$ scelte. Da questo segue che $|\mathcal{A}| = 2^{99}$.

(ii) Usando la notazione introdotta nel primo punto, osserviamo che in questo caso la condizione $A \in \mathcal{B}$ non pone vincoli su A_1 che può quindi essere un qualsiasi sottoinsieme di X_1; abbiamo 2^{50} scelte per A_1. Il sottoinsieme A_0 può invece essere di uno dei seguenti tipi.

Può avere almeno tre elementi: $|A_0| \geq 3$, e per questo tipo ci sono $2^{50} - \binom{50}{0} - \binom{50}{1} - \binom{50}{2}$ scelte. Oppure $|A_0| = 2$ e in tal caso almeno uno dei due elementi deve essere divisibile per 4 o, equivalentemente, i 2 elementi che scegliamo in X_0 non devono entrambi essere nel sottoinsieme dei 25 elementi divisibili per 2 ma non per 4, quindi abbiamo $\binom{50}{2} - \binom{25}{2}$ scelte. O può essere, infine, $|A_0| = 1$ e l'elemento scelto deve essere uno dei 12 elementi di X_0 divisibili per 8, quindi ci sono 12 scelte.

Concludiamo $|\mathcal{B}| = 2^{50}(2^{50} - \binom{50}{0} - \binom{50}{1} - \binom{25}{2} + 12) = 2^{50}(2^{50} - 339)$.

33. Sia $X = \{2, \ldots, 1000\}$ e sia $n \in X$. Scriviamo $n = 2^a p_1^{e_1} \cdots p_r^{e_r}$ con $p_1, \ldots, p_r$ primi dispari distinti, $e_i \geq 1$ e $a \geq 0$. Inoltre, poiché $\phi(n)$ è un numero pari per ogni $n > 2$, affinché valga la condizione di divisibilità richiesta n deve essere pari, cioè $a \geq 1$. Ne segue che

$$\phi(n) = 2^{a-1} \prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1) \mid n \iff \prod_{i=1}^{r} (p_i - 1) \mid 2 \prod_{i=1}^{r} p_i.$$

Poiché i p_i sono dispari, si ha $2^r \mid \prod_{i=1}^{r}(p_i - 1)$: deve quindi essere $r = 0, 1$ in quanto 4 non divide $2 \prod_{i=1}^{r} p_i$.

Se $r = 0$ allora $n = 2^a$ con $a \geq 1$: in X esistono esattamente 9 interi di questa forma e tutti verificano la condizione $\phi(n) \mid n$.

Se, invece, $r = 1$ si ha $n = 2^a p^e$ con p primo dispari e $a, e \geq 1$: la condizione $\phi(n) \mid n$ è equivalente a $p - 1 \mid 2p$ e quindi a $p - 1 \mid 2$, visto che $(p - 1, p) = 1$. L'unica possibilità è avere $p = 3$.

Gli interi $n = 2^a 3^e$, con $a, e \geq 1$, in X possono essere contati, ad esempio, nel modo seguente: $2^a 3^e \in X$ se e solo se $2^a \leq 1000/3^e$, da cui si ottiene immediatamente che per $e = 1$ ci sono 8 valori di a, per $e = 2$ ci sono 6 valori di a, per $e = 3$ ci sono 5 valori di a, per $e = 4$ ci sono 3 valori di a, per $e = 5$ ci sono 2 valori di a, mentre per $e \geq 6$ non c'è nessun valore di a.

Concludendo gli n cercati sono $9 + 8 + 6 + 5 + 3 + 2 = 33$.

34. Verifichiamo la formula per induzione su n. Per $n = 1$ si ha evidentemente $x_1 = 1/2$, cioè la probabilità che al primo lancio esca testa, ed effettivamente $1/2 = 2/3 + (-1)/(3 \cdot 2)$. Per $n = 2$ si ha $x_2 = 1/2 \cdot 1/2 + 1/2 = 3/4$, cioè la probabilità che nei primi due lanci esca testa sommata alla probabilità che al primo lancio esca croce, ed effettivamente $3/4 = 2/3 + 1/(3 \cdot 2^2)$.

Supponiamo ora di avere dimostrato la formula per tutti i numeri positivi $m < n$ e dimostriamola per n. Osserviamo che si può avere $x_k = n$ in due modi mutualmente esclusivi: o $x_{k-1} = n - 1$ e al k–esimo lancio esce testa o $x_{k-1} = n - 2$ e al k–esimo lancio esce croce.

Per ipotesi induttiva, la probabilità del primo caso è uguale a

$$\frac{1}{2}\left(\frac{2}{3} + \frac{(-1)^{n-1}}{3 \cdot 2^{n-1}}\right)$$

e la probabilità del secondo caso è uguale a

$$\frac{1}{2}\left(\frac{2}{3} + \frac{(-1)^{n-2}}{3 \cdot 2^{n-2}}\right).$$

Sommando, si ottiene che la probabilità di ottenere $x_k = n$ per un certo k è uguale a

$$\frac{2}{3} + \frac{1}{2} \cdot \frac{(-1)^n}{3 \cdot 2^{n-1}}(-1 + 2) = \frac{2}{3} + \frac{(-1)^n}{3 \cdot 2^n}$$

come richiesto.

35. Scriviamo $S(f) = S_+(f) + S_-(f)$, dove

$$S_+(f) = \sum_{i \mid f(i) > i} (f(i) - i), \qquad S_-(f) = -\sum_{i \mid f(i) < i} (f(i) - i).$$

Poiché chiaramente si ha $\sum_{i=1}^{10} (f(i) - i) = 0$, se ne deduce che $S_+(f) = S_-(f)$ e che quindi $S(f) = 2S_+(f)$ è sempre pari. Pertanto la risposta alla domanda del secondo punto è zero.

Per il primo punto dobbiamo avere $S_+(f) = S_-(f) = 1$, ossia c'è esattamente un indice i per cui $f(i) = i + 1$ ed esattamente un j per cui $f(j) = j - 1$, mentre per gli indici k diversi da i, j si ha $f(k) = k$. Dunque la funzione deve scambiare fra loro due interi consecutivi, lasciando fissi tutti gli altri. Ci sono esattamente 9 coppie di interi consecutivi e pertanto la risposta è 9.

Per l'ultimo punto abbiamo $S_+(f) = S_-(f) = 2$. Possiamo distinguere tre sottocasi.

(1) Esiste un solo i per cui $f(i) = i + 2$ ed un solo j per cui $f(j) = j - 2$. Questo caso si tratta come il punto (i), considerando che le coppie di interi la cui differenza è 2 sono 8.

(2) Esistono esattamente due indici i per cui $f(i) = i + 1$ ed esattamente due indici j per cui $f(j) = j - 1$. In questo caso la funzione scambia i numeri di due coppie di interi consecutivi. Per contare quante sono le possibilità di questo tipo, si osservi che se la coppia più piccola, cioè quella con interi più piccoli, è $\{1, 2\}$ allora per la seconda coppia ci sono 7 possibilità; se la coppia più piccola è $\{2, 3\}$ allora per la seconda coppia ci sono 6 possibilità, e così via. Abbiamo quindi un totale di $7 + 6 + \cdots + 1 = 28$ possibilità.

(3) Esistono due indici i per cui $f(i) = i + 1$ e un indice j per cui $f(j) = j - 2$, o viceversa. Analizziamo solo il primo caso, perché l'altro è simmetrico.

Necessariamente la permutazione deve essere del tipo $(i, i + 1, i + 2)$, cioè deve scambiare circolarmente 3 interi consecutivi. Le terne di interi consecutivi sono 8, e considerando anche il caso simmetrico, si hanno 16 possibilità.

Sommando i risultati precedenti si ottiene che la risposta al terzo punto è $8 + 28 + 16 = 52$.

36. La somma dei numeri da 1 a 100 è 5050.

(i) Scegliere un sottoinsieme A di 96 elementi è la stessa cosa di scegliere il suo complementare B di 4 elementi. Poiché 5050 è pari la somma degli elementi di A è pari se e solo se lo è la somma degli elementi di B. Si danno i casi seguenti.

(1) I 4 numeri sono tutti pari, ossia B è un sottoinsieme di 4 elementi dei 50 numeri pari compresi fra 1 e 100; in questo caso B può essere scelto in $\binom{50}{4}$ modi.

(2) I 4 numeri sono tutti dispari; analogamente a prima, ci sono $\binom{50}{4}$ possibilità.

(3) I 4 numeri sono due pari e due dispari; in questo caso B è formato da un sottoinsieme di 2 elementi dei 50 numeri pari e da un sottoinsieme di 2 elementi dei 50 numeri dispari; questo caso dà $\binom{50}{2} \cdot \binom{50}{2}$ possibilità.

In totale ci sono dunque $2\binom{50}{4} + \binom{50}{2}^2$ casi possibili.

(ii) Analogamente a prima, invece di scegliere A scegliamo il suo complementare C di 3 elementi. Poiché $5050 \equiv 1 \pmod 3$, La somma degli elementi di A è divisibile per 3 se e solo se la somma degli elementi di C è congrua a 1 modulo 3.

Osserviamo che nei numeri da 1 a 100 ci sono 33 elementi congrui a zero modulo 3, 34 elementi congrui a 1 e 33 elementi congrui a 2. Sia $C = \{a, b, c\}$. Si danno i seguenti casi a meno dell'ordine: (1) $a \equiv b \equiv 0, c \equiv 1 \pmod 3$, in questo caso $\{a, b\}$ può essere scelto in $\binom{33}{2}$ modi e c in 34 modi; (2) $a \equiv b \equiv 1, c \equiv 2 \pmod 3$, in questo caso $\{a, b\}$ può essere scelto in $\binom{34}{2}$ modi e c in 33 modi o, infine, (3) $a \equiv b \equiv 2, c \equiv 0 \pmod 3$, in questo caso $\{a, b\}$ può essere scelto in $\binom{33}{2}$ modi e c in 33 modi.

Il totale dà dunque $\binom{33}{2} \cdot 34 + \binom{34}{2} \cdot 33 + \binom{33}{2} \cdot 33$.

37. L'insieme A è in corrispondenza biunivoca con l'insieme dei sottoinsiemi di $\{1, \ldots, 100\}$ con 5 elementi: infatti basta far corrispondere ad $f \in A$ l'insieme dei

suoi valori $\{f(1), f(2), f(3), f(4), f(5)\}$. La cardinalità di A è quindi uguale al numero dei modi di scegliere un sottoinsieme di 5 elementi di un insieme di 100 elementi, e cioè $\binom{100}{5}$.

L'insieme B si ottiene dall'insieme A togliendo l'insieme delle applicazioni tali che $f(i+1) = f(i) + 1$ per ogni $i = 1, 2, 3, 4$. Ossia togliendo l'insieme delle applicazioni per cui $f(1) = a$, $f(2) = a + 1$, $f(3) = a + 2$, $f(4) = a + 3$, $f(5) = a + 4$ con $a \in \{1, \ldots, 96\}$. Pertanto $|B| = \binom{100}{5} - 96$.

Per contare gli elementi di C, osserviamo che la condizione data è equivalente alla seguente: l'applicazione $g(i) = f(i) - i$ è strettamente crescente ed a valori nell'insieme $\{0, \ldots, 95\}$. Infatti

$$f(i+1) > f(i) + 1 \Longleftrightarrow f(i+1) - (i+1) > f(i) + 1 - (i+1) = f(i) - i$$

e inoltre

$$f(1) \geq 1 \Longleftrightarrow g(1) \geq 0 \quad \text{e} \quad f(100) \leq 100 \Leftrightarrow g(100) \leq 95.$$

Pertanto per contare l'insieme dato basta contare l'insieme delle funzioni strettamente crescenti a valori in $\{0, \ldots, 95\}$. Ragionando come fatto per contare l'insieme A, si deduce che C ha $\binom{96}{5}$ elementi.

38. (i) Si consideri prima il problema di formare un insieme *ordinato* di n squadre di 4 persone. Per formare la prima squadra bisogna scegliere un sottoinsieme di 4 persone dall'insieme di $4n$ persone, e questo si può fare in $\binom{4n}{4}$ modi. La seconda squadra sarà scelta all'interno del restante insieme di $4n - 4$ persone, e quindi potrà essere formate in $\binom{4n-4}{4}$ modi. Procedendo in questo modo, l'insieme ordinato di n squadre può essere formato in

$$\binom{4n}{4}\binom{4n-4}{4}\cdots\binom{4}{4} = \frac{(4n)!}{(4!)^n}$$

modi. Poiché, infine, lo stesso insieme di n squadre si può ottenere ordinando le squadre in $n!$ modi diversi, la risposta è

$$\frac{(4n)!}{(4!)^n \cdot n!}.$$

(ii) Anche in questo caso scegliamo dapprima le n squadre in ordine. Per formare la prima squadra bisogna scegliere una coppia di uomini e una coppia di donne all'interno dei rispettivi insiemi di $2n$ elementi ciascuno: questo può essere fatto in $\binom{2n}{2}^2$ modi. Procedendo come nel caso precedente, un insieme ordinato di n squadre può essere scelto in

$$\binom{2n}{2}^2\binom{2n-2}{2}^2\cdots\binom{2}{2}^2 = \frac{(2n)!^2}{2^{2n}}$$

modi, e un insieme non ordinato di n squadre può essere scelto in

$$\frac{(2n)!^2}{2^{2n}n!}$$

modi.

39. Osserviamo che x e $f(x)$ devono avere lo stesso numero di divisori e lo stesso numero di multipli nell'intervallo considerato. Ne segue che 1, l'unico numero con un solo divisore, deve andare in 1, e un primo deve andare in un primo, infatti i primi sono caratterizzati dall'avere esattamente 2 divisori.

In generale, il numero dei divisori di un intero m può essere calcolato usando la scomposizione in primi $p_1^{a_1} \cdots p_k^{a_k}$ di m ed è dato dal prodotto $(a_1+1)\cdots(a_k+1)$; infatti in un divisore di m il primo p_i può comparire con qualsiasi esponente tra 0 e a_i, e vi sono a_i+1 scelte per ogni dato $i = 1, \ldots, k$.

Consideriamo in particolare il caso in cui tutti gli a_i siano uguali ad 1, ovvero $m = p_1 p_2 \cdots p_k$. In questo caso m ha esattamente 2^k divisori. Ora visto che p_i divide m, la sua immagine $q_i = f(p_i)$ deve essere un primo che divide $f(m)$. Inoltre i q_i devono essere distinti perché f è iniettiva. Quindi $f(m)$ deve essere un multiplo di $q_1 q_2 \cdots q_k$, e siccome deve avere lo stesso numero di divisori di m (che sono 2^k), deve coincidere con questo prodotto. Questo dimostra il punto (i).

Per il punto (ii) osserviamo che le potenze dei primi sono caratterizzate dal fatto che non vi sono due primi distinti che le dividono. Visto che abbiamo già dimostrato che i primi vanno in primi, e primi distinti vanno in primi distinti, ne segue che una potenza p^n di un primo p deve andare in una potenza del primo corrispondente $q = f(p)$. Possiamo in effetti dire di più: p^n deve andare in q^n, cioè con lo stesso esponente n, altrimenti p^n, che ha $n+1$ divisori, non avrebbe lo stesso numero di divisori della sua immagine. Questo finisce la dimostrazione del punto (ii).

Più in generale, per induzione su m, mostriamo che se il primo p_i va in $q_i = f(p_i)$, per $i = 1, \ldots, k$, allora $m = p_1^{a_1} \cdots p_k^{a_k}$ va necessariamente in $q_1^{a_1} \cdots q_k^{a_k}$.

Per $k = 1$ lo abbiamo appena dimostrato, sia quindi $k > 1$. Possiamo supporre che gli esponenti a_i siano positivi, per ipotesi induttiva $m/p_1^{a_1} = \prod_{j\neq 1} p_j^{a_j}$ va in $\prod_{j\neq 1} q_j^{a_j}$. Poiché $m/p_1^{a_1}$ divide m, $f(m/p_1^{a_1})$ deve dividere $f(m)$. Quindi in particolare $q_j^{a_j}$ divide $f(m)$ per ogni $j \neq 1$. Un ragionamento analogo, scambiando 1 con un altro indice, mostra che anche $q_1^{a_1}$ divide $f(m)$. Quindi $f(m)$ deve essere un multiplo di $q_1^{a_1} \cdots q_k^{a_k}$ e, dovendo avere lo stesso numero di divisori di m, deve coincidere con questo numero.

Abbiamo così dimostrato che f è determinata dalla sua restrizione all'insieme dei numeri primi, ovvero da come permuta i numeri primi. Mostriamo ora che per $n = 10$ l'unica possibile f è l'identità. A tal fine basta mostrare che ogni primo va in se stesso. I primi minori di 10 sono 2, 3, 5, 7. Se il primo 2 andasse in 3, 2^3 dovrebbe andare in 3^3, ma questo è assurdo perché $3^3 > 10$. Similmente si escludono gli altri casi, e quindi 2 va in 2. Analogamente 3 va in 3 altrimenti non sapremmo dove mandare 3^2. Le uniche possibilità rimaste per $f(5)$ sono 5 o 7, ma siccome 2 va in 2, $2 \cdot 5$ deve andare in $2 \cdot f(5)$, e questo esclude il caso $f(5) = 7$. Quindi in definitiva ogni primo va in se stesso ed f è l'identità.

Per $n = 13$, ragionando allo stesso modo, vediamo, invece, che f può permutare in qualsiasi modo i primi $7, 11, 13$ e fissare gli altri numeri, e vi sono quindi 6 possibilità.

40. (i) Basta considerare quali sono i 4 insiemi di 10 carte occupati da ciascun seme, perché all'interno dell'insieme l'ordine delle carte è fissato. Per scegliere l'insieme delle posizioni occupate dai denari ci sono $\binom{40}{10}$ possibilità; per l'insieme delle posizioni occupate dalle spade restano $\binom{30}{10}$ possibilità; per le posizioni occupate dai bastoni rimangono $\binom{20}{10}$ possibilità, ed infine le posizioni delle coppe sono le rimanenti. Il numero richiesto è dunque

$$\binom{40}{10} \cdot \binom{30}{10} \cdot \binom{20}{10} = \frac{40!}{(10!)^4}.$$

(ii) Scegliamo le 20 posizioni occupate dalle carte di denari e di spade complessivamente: questo si può fare in $\binom{40}{20}$ modi. A questo punto, i denari devono occupare le prime 10 di queste posizioni, mentre le spade le ultime 10. All'interno delle loro dieci posizioni, però, sia i denari che le spade possono essere ordinati in un modo qualsiasi, ossia in 10! modi ciascuno. Infine, le coppe e i bastoni possono essere disposti a caso nelle restanti 20 posizioni, quindi in 20! modi. La risposta è pertanto

$$\binom{40}{20} \cdot (10!)^2 \cdot 20! = \frac{40! \cdot (10!)^2}{20!}.$$

41. Supponiamo dapprima $n = 2m$ pari, con $m \geq 1$, e dividiamo gli n numeri nei due sottoinsiemi P e D, rispettivamente dei numeri pari e dei numeri dispari, con m elementi ciascuno. Se un sottoinsieme X *non* contiene almeno tre numeri della stessa parità, allora ha al più due elementi di P e al più due elementi di D. Sommando i tre casi in cui X possieda 0, 1 o 2 numeri pari, si ottiene che la scelta degli elementi pari di X può avvenire in

$$\binom{m}{0} + \binom{m}{1} + \binom{m}{2} = \frac{m^2 + m + 2}{2}$$

modi. La stessa cosa vale per la scelta degli elementi dispari, per cui il numero dei sottoinsiemi X che non contengono almeno 3 elementi della stessa parità è

$$\left(\frac{m^2 + m + 2}{2}\right)^2.$$

Nel caso in cui $n = 2m - 1$ è dispari, con $m \geq 1$, il sottoinsieme dei dispari contiene m elementi mentre quello dei pari contiene $m - 1$ elementi, pertanto la formula per il numero dei sottoinsiemi X che non contengono almeno 3 elementi della stessa parità diventa

$$\frac{m^2 + m + 2}{2} \cdot \frac{m^2 - m + 2}{2}.$$

La risposta al problema si ottiene togliendo dal numero di tutti i sottoinsiemi di $\{1, \ldots, n\}$ quelli appena contati, abbiamo cioè

$$\begin{cases} 2^{2m} - \left(\dfrac{m^2+m+2}{2}\right)^2 & \text{se } n = 2m, \\ 2^{2m-1} - \dfrac{m^2+m+2}{2} \cdot \dfrac{m^2-m+2}{2} & \text{se } n = 2m-1. \end{cases}$$

42. Per un elemento $\overline{x} \in \mathbb{Z}/40\mathbb{Z}$ chiamiamo $c(\overline{x}) \in \{0, 1, 2, 3\}$ il *colore* di x. Dividiamo l'insieme $\mathbb{Z}/40\mathbb{Z}$ in 10 sottoinsiemi $A_0, \ldots, A_9$ di 4 elementi ciascuno, dove A_i è l'insieme dei 4 elementi di $\mathbb{Z}/40\mathbb{Z}$ congrui ad i modulo 10.

L'enunciato del problema non pone condizioni per elementi appartenenti ad insiemi A_i diversi, quindi gli A_i possono essere colorati ciascuno indipendentemente dagli altri.

Vediamo quanti sono i modi di colorare ciascun $A_i = \{\overline{i}, \overline{i+10}, \overline{i+20}, \overline{i+30}\}$. Distinguiamo due casi: (1) $\overline{i}$ e $\overline{i+20}$ hanno lo stesso colore o (2) $\overline{i}$ e $\overline{i+20}$ hanno colori distinti.

(1) Nel primo caso, ci sono 4 scelte per il colore di $\overline{i}$ e $\overline{i+20}$; gli altri due elementi potranno essere colorati con un colore diverso, cioè ciascuno, indipendentemente l'uno dall'altro, con uno qualsiasi degli altri 3 colori restanti. Quindi le possibilità per questo caso sono $4 \cdot 3^2 = 36$.

(2) Nel secondo caso, ci sono 4 scelte per il colore di $\overline{i}$ e 3 scelte, cioè tutte meno quella del colore scelto per $\overline{i}$, per il colore di $\overline{i+20}$. Per quanto riguarda gli elementi rimanenti, essi potranno essere colorati ciascuno, indipendentemente l'uno dall'altro, con uno qualsiasi dei due colori restanti. Quindi le possibilità per questo caso sono $4 \cdot 3 \cdot 2^2 = 48$.

Il totale delle possibilità delle colorazioni per un insieme A_i è dunque $36 + 48 = 84$. Poiché ci sono 10 insiemi A_i, ed essi possono essere colorati in modo indipendente, il numero totale di possibilità è 84^{10}.

43. (i) Per ogni riga ci sono due colorazioni per cui una riga è interamente bianca o nera, e di conseguenza $2^n - 2$ colorazioni in cui ciò non vale. Inoltre, le scelte del colore delle righe sono indipendenti l'una dall'altra. Pertanto il numero delle colorazioni possibili è $(2^n - 2)^n$.

(ii) Si tratta di scegliere n caselle in modo che ce ne sia esattamente una in ogni riga ed una in ogni colonna. Equivalentemente, se nella riga i–esima si sceglie la colonna $\sigma(i)$–esima, l'applicazione $i \longmapsto \sigma(i)$ deve essere una *permutazione* dell'insieme $\{1, \ldots, n\}$. Pertanto si hanno $n!$ possibilità.

(iii) In ogni riga si deve scegliere il sottoinsieme di $n/2$ caselle da colorare di bianco, quelle da colorare di nero saranno le restanti e quindi saranno automaticamente determinate. Pertanto ci sono $\binom{n}{n/2}$ modi per colorare ogni riga. Le colorazioni delle righe sono indipendenti una dall'altra, pertanto il numero totale di colorazioni possibili è $\binom{n}{n/2}^n$.

44. Soluzione 1. In questa soluzione usiamo le proprietà dei coefficienti binomiali.

In entrambe le somme per $k = 0$ si ha l'addendo nullo, possiamo quindi ometterlo. Osserviamo anche che $k\binom{k}{n} = n\binom{n-1}{k-1}$, come segue subito dalla definizione dei coefficienti binomiali. Vale quindi:

$$\text{(i)} \quad \sum_{k=0}^{n} k\binom{n}{k} = \sum_{k=1}^{n} k\binom{n}{k} = n\sum_{k=1}^{n}\binom{n-1}{k-1} = n\sum_{h=0}^{n-1}\binom{n-1}{h} = n2^{n-1}.$$

$$\begin{aligned}\text{(ii)} \quad \sum_{k=0}^{n} k^2\binom{n}{k} &= \sum_{k=1}^{n} kn\binom{n-1}{k-1} = n\sum_{h=0}^{n-1}(h+1)\binom{n-1}{h} \\ &= n\sum_{h=0}^{n-1} h\binom{n-1}{h} + n\sum_{h=0}^{n-1}\binom{n-1}{h}.\end{aligned}$$

Usando ora il risultato del punto precedente se $n-1 \geq 1$, o per verifica diretta se $n-1 = 0$, si ottiene infine

$$\sum_{k=0}^{n} k^2\binom{n}{k} = n(n-1)2^{n-2} + n2^{n-1} = (n^2+n)2^{n-2}.$$

Soluzione 2. Ora una soluzione per induzione.

(i) Sia $p(n) : \sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}$ e proviamo che $p(n)$ è vera per ogni $n \geq 1$ per induzione su n. Per $n = 1$ si ha $\sum_{k=0}^{1} k\binom{n}{k} = \binom{1}{1} = 1$ e quindi la tesi è vera.

Supponiamo ora $n \geq 1$ e $p(n)$ vera e proviamo che anche $p(n+1)$ è vera. Si ha

$$\begin{aligned}\sum_{k=0}^{n+1} k\binom{n+1}{k} &= \sum_{k=1}^{n} k\left(\binom{n}{k} + \binom{n}{k-1}\right) + (n+1)\binom{n+1}{n+1} \\ &= \sum_{k=1}^{n} k\binom{n}{k} + \sum_{k=0}^{n}(k+1)\binom{n}{k} - (n+1)\binom{n}{n} + n + 1 \\ &= n2^{n-1} + \sum_{k=0}^{n} k\binom{n}{k} + \sum_{k=0}^{n}\binom{n}{k} \\ &= n2^{n-1} + n2^{n-1} + 2^n \\ &= (n+1)2^n\end{aligned}$$

dove abbiamo usato che $p(n)$ vera, cioè che $\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}$ e che $\sum_{k=0}^{n}\binom{n}{k} = 2^n$. Questo finisce la dimostrazione che $p(n+1)$ è vera.

(ii) Procediamo, come nel punto precedente, per induzione con la proposizione $q(n) : \sum_{k=0}^{n} k^2\binom{n}{k} = n(n+1)2^{n-2}$. Anche in questo caso è banale verificare che $q(1)$ è vera, supponiamo quindi $n \geq 1$ e $q(n)$ vera. Usando quanto provato nel punto

(i) abbiamo

$$\begin{aligned}\sum_{k=0}^{n+1} k^2\binom{n}{k} &= \sum_{k=1}^{n} k^2\left(\binom{n}{k}+\binom{n}{k-1}\right)+(n+1)^2\binom{n+1}{n+1}\\ &= \sum_{k=1}^{n} k^2\binom{n}{k}+\sum_{k=0}^{n}(k+1)^2\binom{n}{k}-(n+1)^2\binom{n}{n}+(n+1)^2\\ &= n(n+1)2^{n-2}+\sum_{k=0}^{n} k^2\binom{n}{k}+2\sum_{k=0}^{n} k\binom{n}{k}+\sum_{k=0}^{n}\binom{n}{k}\\ &= n(n+1)2^{n-1}+n2^n+2^n\\ &= (n+1)(n+2)2^{n-1}\end{aligned}$$

e quindi anche $q(n+1)$ è vera.

Soluzione 3. Vediamo una soluzione combinatoria.

(i) Sia X l'insieme $\{1,2,\ldots,n\}$ e sia $\mathcal{F} \doteq \{(A,a)\,|\,a \in A \subseteq X\}$, cioè l'insieme dei sottoinsiemi A di X con l'elemento a di A che pensiamo come evidenziato. Vogliamo contare la cardinalità di $\mathcal{F}$ in due modi diversi.

Per prima cosa scegliamo A di cardinalità k in X: questo si può fare in $\binom{n}{k}$ modi; poi scegliamo in k modi diversi l'elemento a di A. Quindi, visto che A può avere cardinalità $0,1,\ldots,n$ abbiamo che $\mathcal{F}$ ha cardinalità $\sum_{k=0}^{n} k\binom{n}{k}$.

Ma possiamo anche prima scegliere a in n modi in X e poi scegliere un sottoinsieme A di X che contiene a. Visto che X ha cardinalià n e a è un elemento di A, abbiamo 2^{n-1} modi di scegliere A. Quindi $\mathcal{F}$ ha cardinalità $n2^{n-1}$. Questo prova la formula.

(ii) Ragioniamo come nel punto precedente con l'insieme $\mathcal{G} = \{(A,a,b)\,|\,a,b \in A \subseteq X\}$ dei sottoinsiemi A di X con due elementi a e b di A, anche coincidenti, evidenziati.

Scegliamo A di cardinalità k in $\binom{n}{k}$ modi e poi scegliamo a e b in A in k^2 modi. Quindi $\mathcal{G}$ ha cardinalità $\sum_{k=0}^{n} k^2\binom{n}{k}$.

D'altra parte possiamo anche procedere nel seguente modo. Consideriamo prima il caso $a = b$: scegliamo questo elemento in n modi e poi scegliamo A in X in modo che contenga a in 2^{n-1} modi. Per il caso $a \neq b$ scegliamo a in n modi, b in $n-1$ modi e poi A in 2^{n-2} modi in quanto deve contenere sia a che b. Quindi in totale $\mathcal{G}$ ha cardinalità $n2^{n-1} + n(n-1)2^{n-2} = n(n+1)2^{n-2}$ e la formula è dimostrata.

Soluzione 4. Per questa ultima soluzione usiamo lo sviluppo del Binomio di Newton.

Sia $\mathbb{R}[x]$ l'anello dei polinomi nell'indeterminata x, indichiamo con $D : \mathbb{R}[x] \longrightarrow \mathbb{R}[x]$ l'operazione di derivazione e sia $\mathbb{R}[x] \ni f(x) \overset{\nu}{\longmapsto} f(1) \in \mathbb{R}$ la valutazione in 1.

(i) Consideriamo il polinomio $p(x) \doteq (1+x)^n$ e valutiamo in 1 la sua derivata: $\nu(D(p(x))) = \nu(n(1+x)^{n-1}) = n2^{n-1}$. Ma possiamo anche sviluppare con il Bi-

nomio di Newton $p(x) = \sum_{k=0}^{n} \binom{n}{k} x^k$ e quindi abbiamo

$$\nu(D(p(x))) = \nu\left(\sum_{k=1}^{n} k\binom{n}{k} x^{k-1}\right) = \sum_{k=1}^{n} k\binom{n}{k}$$

e la formula da provare segue.

(ii) Introduciamo anche la mappa $\mathbb{R}[x] \ni f(x) \overset{\mu}{\longmapsto} xf(x) \in \mathbb{R}[x]$ che moltiplica un polinomio per x. Valutiamo ora $\nu D\mu D$ sul polinomio $p(x) = (1+x)^n$. Abbiamo

$$\begin{aligned}
\nu D\mu D(1+x)^n &= \nu D(nx(1+x)^{n-1}) \\
&= n\nu((1+x)^{n-1} + (n-1)x(1+x)^{n-2}) \\
&= n(2^{n-1} + (n-1)2^{n-2}) \\
&= n(n+1)2^{n-2}.
\end{aligned}$$

Sviluppando invece con il binomio di Newton abbiamo

$$\begin{aligned}
\nu D\mu D(1+x)^n &= \nu D\mu D\left(\sum_{k=0}^{n} \binom{n}{k} x^k\right) \\
&= \sum_{k=0}^{n} \binom{n}{k} \nu D\mu D\left(x^k\right) \\
&= \sum_{k=0}^{n} \binom{n}{k} \nu D\left(kx^k\right) \\
&= \sum_{k=0}^{n} \binom{n}{k} \nu\left(k^2 x^{k-1}\right) \\
&= \sum_{k=0}^{n} k^2 \binom{n}{k}
\end{aligned}$$

e la formula è dimostrata.

45. Osserviamo che la condizione imposta è indipendente sulle cifre di posto pari e su quelle di posto dispari, quindi se le possibilità per le cifre di posto dispari sono N allora la cardinalità cercata è N^2 visto che le condizioni su posti pari e dispari sono anche simmetriche.

Ci basta quindi contare il numero di 15–uple $(a_1, a_3, \ldots, a_{29})$ di 0 e 1 per cui la somma delle cifre è al più 2. In particolare tale somma può quindi essere 0, 1 o 2. Essa è 0 per il solo caso $a_1 = a_3 = \cdots = a_{29} = 0$. Se invece è 1 abbiamo tutti zeri e un solo 1 e quindi 15 casi e, infine, se è 2 abbiamo tutti 0 e due 1 da sistemare in 15 posti, cioè $\binom{15}{2}$ casi. In totale $1 + 15 + 105 = 121 = 11^2$.

Concludiamo che la cardinalità richiesta è 11^4.

46. (i) Si tratta di contare gli insiemi $A = \{a, b, c\} \subseteq X$ tale che $a + b = 10$. L'equazione $a + b = 10$ in X è verificata solo quando l'insieme $\{a, b\}$ è uno dei seguenti insiemi di due elementi: $\{1, 9\}$, $\{2, 8\}$, $\{3, 7\}$ e $\{4, 6\}$; quindi il sottoinsieme $\{a, b\}$ si può scegliere in 4 modi. L'insieme A si costruisce aggiungendo ad ognuno dei sottoinsiemi costruiti un elemento c diverso dai due elementi già scelti. Questo può essere fatto in 98 modi per ognuno dei 4 sottoinsiemi sopra riportati. Poiché gli insiemi costruiti in questo modo risultano tutti distinti il loro numero è $4 \cdot 98 = 392$.

(ii) Sia X_5 il sottoinsieme di X dei multipli di 5; chiaramente $|X_5| = 20$. Gli insiemi $A = \{a, b, c\}$ che dobbiamo contare sono quelli che hanno tutti e tre gli elementi divisibili per 5 o esattamente 2 elementi divisibili per 5. I primi sono i sottoinsiemi di 3 elementi di X_5 e sono quindi $\binom{20}{3}$; i secondi si ottengono scegliendo due elementi in X_5 e uno fuori, quindi sono $\binom{20}{2} \cdot 80$. In totale gli insiemi cercati risultano essere in numero di $\binom{20}{3} + \binom{20}{2} \cdot 80$.

47. Scriviamo un elemento x di $\mathbb{Z}/2^{100}\mathbb{Z}$ come $x = 2^\alpha x_1$ con x_1 dispari e $0 \le \alpha \le 100$. Per $\alpha = 100$ si ha $x = \overline{0}$; fissato $\alpha < 100$ scegliere x equivale a scegliere x_1 come una classe modulo $2^{100-\alpha}$, dispari; queste classi sono $\phi(2^{100-\alpha}) = 2^{99-\alpha}$.

Sia ora $x = 2^\alpha x_1$, con x_1 dispari; l'equazione $xy = \overline{0}$ può essere scritta come $2^\alpha x_1 y \equiv 0 \pmod{2^{100}}$. Le soluzioni y sono le classi modulo 2^{100} tali che $y \equiv 0 \pmod{2^{100-\alpha}}$, e queste sono esattamente 2^α.

Concludendo, per $0 \le \alpha \le 99$ le coppie $(2^\alpha x_1, y)$ cercate sono $2^{99-\alpha} \cdot 2^\alpha = 2^{99}$; per $\alpha = 100$, sia ha $x = 0$ e tutti i valori di y vanno bene. In totale le soluzioni cercate sono quindi

$$\sum_{\alpha=0}^{99} 2^{99} + 2^{100} = 100 \cdot 2^{99} + 2^{100} = 51 \cdot 2^{100}.$$

48. (i) Il numero di squadre di 4 persone che si possono formare scegliendole da un insieme di 13 persone è ovviamente $\binom{13}{4}$. Tra queste quelle che comprendono due persone fissate p e q sono $\binom{11}{2}$ in quanto 2 delle 4 persone sono p e q e le altre 2 possono essere scelte liberamente tra le restanti 11. La probabilità che p e q siano nella stessa squadra è quindi $\binom{11}{2}/\binom{13}{4} = 1/13$. La probabilità che p e q non siano nella stessa squadra è quindi $12/13$.

(ii) Sia n il numero cercato. Poiché in ogni squadra ci sono esattamente $\binom{4}{2} = 6$ coppie e il numero totale di coppie è $\binom{13}{2} = 78$, si ha $78 = 6n$ da cui $n = 13$.

49. Sia $X = \{0, 1, \ldots, 100\}$. Sappiamo che i divisori d di $2^{100}3^{100}$ sono tutti e soli i numeri della forma $2^x 3^y$ con $x, y \in X$; dobbiamo vedere quali di questi risolvono la congruenza

$$2^x 3^y \equiv 4 \pmod 5.$$

Osserviamo che $3 \equiv 2^{-1} \pmod 5$, quindi la congruenza diventa $2^{x-y} \equiv 2^2 \pmod 5$. Essa ha soluzione $x - y \equiv 2 \pmod 4$ in quanto 2 ha ordine moltiplicativo 4 modulo 5.

Tenendo conto che l'insieme X contiene 26 elementi della classe di 0 modulo 4 e 25 elementi di ognuna delle altre classi modulo 4, si calcola che le coppie di interi $(x, y) \in X \times X$ tali che $x \equiv y+2 \pmod 4$ sono $26 \cdot 25 + 25 \cdot 25 + 25 \cdot 26 + 25 \cdot 25 = 2550$.

50. (i) Sia $A = \{x, y\}$ un sottoinsieme di due elementi di X. Affinché $x + y$ sia divisibile per 4 si possono dare le seguenti possibilità: x e y sono entrambi divisibili per 4; x e y sono entrambi congrui a 2 modulo 4 o, infine, uno fra x e y è congruo a 1 modulo 4 e l'altro è congruo a 3 modulo 4.

Nel primo caso A deve essere contenuto nel sottoinsieme di X costituito dai multipli di 4, che ha 25 elementi; quindi questo caso dà luogo a $\binom{25}{2}$ possibilità. Analogamente, anche il secondo caso dà luogo a $\binom{25}{2}$ possibilità.

Nell'ultimo caso l'insieme A può essere formato da uno qualsiasi dei 25 elementi congrui a 1 ed uno qualsiasi dei 25 elementi congrui a 3 modulo 4, quindi in 25^2 modi.

Sommando i risultati ottenuti si ha il numero cercato: $2 \cdot \binom{25}{2} + 25^2$.

(ii) Sia $A = \{a, b, c\}$ un sottoinsieme di 3 elementi di X. Possiamo supporre di aver scritto l'insieme in modo che $a < b < c$. I numeri di X minori di a sono $x = a - 1$; quelli fra a e b sono $y = b - a - 1$, quelli fra b e c sono $z = c - b - 1$; quelli maggiori di c sono $t = 100 - c$.

È chiaro che il sottoinsieme A è completamente determinato dalla scelta dei numeri x, y, z, t. Abbiamo inoltre che $x + y + z + t = 97$. Per ipotesi, y e z sono positivi. Ponendo $x' = x + 1$ e $t' = t + 1$ anche x' e t' sono positivi. Pertanto la condizione da soddisfare è $x' + y + z + t' = 99$. Le soluzioni di questa equazione in interi positivi sono $\binom{98}{3}$.

51. (i) Per la coppia (m_f, M_f) ci sono 9 possibilità: $(1, 2)$, $(2, 3)$, $\ldots$, $(9, 10)$. Per ciascuna di queste possibilità, le applicazioni cercate sono quelle con valori in un insieme di due elementi, con l'unica restrizione che entrambi questi elementi compaiano come valori della funzione. In definitiva, avendo fissato l'immagine, bisogna solo escludere le applicazioni costanti, ossia abbiamo $2^{10} - 2$ possibilità. Considerando i 9 casi possibili di (m_f, M_f), il numero delle applicazioni cercate è $9 \cdot (2^{10} - 2)$.

(ii) L'insieme di tutte le applicazioni da $\{1, 2, \ldots, 10\}$ in sé ha 10^{10} elementi. Da questo insieme bisogna togliere le applicazioni per cui $M_f \neq 10$ oppure $m_f \neq 1$. Siano $A = \{f \in X \mid M_f \neq 10\}$, $B = \{f \in X \mid m_f \neq 1\}$. Sia A che B sono insiemi di tutte le applicazioni da un insieme di 10 elementi in un insieme di 9 elementi, mentre $A \cap B$ è l'insieme di tutte le applicazioni da un insieme di 10 elementi in un insieme di 8 elementi. Ne segue che

$$|A \cup B| = 9^{10} + 9^{10} - 8^{10},$$

da cui l'insieme cercato ha cardinalità $10^{10} - 2 \cdot 9^{10} + 8^{10}$.

52. Riscriviamo l'equazione come $n - \phi(n) = 8$. Evidentemente n non può essere uguale a 1, quindi esistono dei fattori primi che dividono n.

Supponiamo dapprima che nella fattorizzazione di n compaia un solo fattore primo, e quindi $n = p^a$ per qualche numero primo p e qualche esponente $a \geq 1$. Allora $n - \phi(n) = p^a - (p^a - p^{a-1}) = p^{a-1}$, da cui $p^{a-1} = 8$, ossia $p = 2$, $a - 1 = 3$ e questo dà la soluzione $n = 2^4 = 16$.

In secondo luogo, supponiamo che $n = p^a q^b$ abbia esattamente due fattori primi distinti p e q, con $p < q$. Allora $n - \phi(n) = p^a q^b - (p^a - p^{a-1})(q^b - q^{b-1}) = p^{a-1} q^{b-1}(p + q - 1)$. Ne segue che $p^{a-1} q^{b-1} \mid 8$.

Se $p^{a-1} q^{b-1} = 1$, allora $p + q - 1 = 8$ e quindi, poiché $p + q = 9$ è un numero dispari, uno dei due addendi deve essere pari, ossia $p = 2$ e $q = 7$. Questo dà la soluzione $n = 14$.

Se $p^{a-1} q^{b-1} = 2$, allora $p + q - 1 = 4$, che ha per unica soluzione $p = 2$, $q = 3$. Questo dà la soluzione $n = 2^2 \cdot 3 = 12$.

Se $p^{a-1} q^{b-1} \geq 4$, allora $p + q - 1 \leq 2$, che è chiaramente impossibile.

Supponiamo, infine, che nella fattorizzazione di n compaiano almeno tre fattori primi distinti p, q, r, con $p < q < r$. Allora l'insieme degli interi $\{1 \leq x \leq n \mid p \text{ divide } x\}$ comprende almeno $qr \geq 3 \cdot 5 = 15$ numeri che non sono primi con n, quindi $n - \phi(n) \geq 15$.

Concludendo, le soluzioni dell'equazione data sono $n = 12, 14, 16$.

53. (i) L'insieme dei punti fissi è un sottoinsieme di 10 elementi di un insieme di 100 elementi, e quindi può essere scelto in $\binom{100}{10}$ modi. Gli altri 90 elementi non devono essere fissi e quindi ciascuno di essi può essere mandato in 99 elementi, quelli diversi da sé stesso. Il numero di applicazioni cercato è dunque

$$\binom{100}{10} \cdot 99^{90}.$$

(ii) Ci sono due possibilità per ottenere $\sum_{x \in X} |f(x) - x| = 2$: o c'è un solo elemento x non lasciato fisso da f per cui $|f(x) - x| = 2$ o ci sono esattamente due elementi x, y non lasciati fissi da f per cui $|f(x) - x| = |f(y) - y| = 1$.

Nel primo caso, ci sono 2 possibilità per $f(x)$ se $x \neq 1, 2, 99, 100$ ed una possibilità altrimenti. Nel secondo caso, ci sono due possibilità per ogni elemento della coppia x, y a meno che uno o entrambi gli elementi della coppia appartengano all'insieme $A = \{1, 100\}$.

Se uno solo degli elementi appartiene ad A, allora c'è un'unica scelta possibile per l'immagine di questo elemento e ci sono due scelte possibili per l'immagine dell'altro elemento. Se la coppia è A c'è una sola scelta possibile.

Concludendo, il numero di applicazioni cercato è

$$2 \cdot 100 - 4 + \binom{98}{2} \cdot 4 + 2 \cdot 98 \cdot 2 + 1 = 19601.$$

54. (i) Il numero dei sottoinsiemi di X con 5 elementi è $\binom{20}{5}$. Per ogni sottoinsieme A con 5 elementi, il sottoinsieme B deve avere esattamente 7 elementi al di fuori di A ed un numero qualsiasi di elementi in comune con A. Pertanto, fissato A, il

numero di scelte per B è $\binom{15}{7} \cdot 2^5$. La risposta è dunque

$$\binom{20}{5} \cdot \binom{15}{7} \cdot 2^5.$$

(ii) Scegliamo l'insieme $Y = (A \cup B) \cap C$ in $\binom{20}{8}$ modi. Ogni fissato elemento di Y può essere in $A \setminus B$, $B \setminus A$ o $A \cap B$; abbiamo quindi 3^8 modi per distribuire gli elementi di Y in A e B.

Ragionando allo stesso modo, ogni fissato elemento di $X \setminus Y$ può essere in cinque insiemi diversi: $X \setminus (A \cup B \cup C)$, $A \setminus (B \cup C)$, $B \setminus (A \cup C)$, $C \setminus (A \cup B)$ o, infine, $(A \cap B) \setminus C$. Ciò corrisponde quindi a 12^5 modi di disporre gli elementi di $X \setminus Y$.

In totale le scelte risultano essere

$$\binom{20}{8} \cdot 3^8 \cdot 5^{12}.$$

55. (i) Le stringhe che hanno k coordinate pari sono $\binom{10}{k} \cdot 3^k \cdot 2^{10-k}$. Infatti esse si possono costruire scegliendo k posti sui 10 possibili e mettendo in questi posti valori pari, cioè 0, 2 o 4, e nei rimanenti $10 - k$ posti andranno valori dispari, cioè 1 o 3. Le stringhe cercate sono quelle in cui ci sono 6, 7, 8, 9 oppure 10 coordinate pari e sono quindi

$$\sum_{k=6}^{10} \binom{10}{k} \cdot 3^k \cdot 2^{10-k} = 3^7 \cdot 2827.$$

(ii) Possiamo interpretare le stringhe come le cifre in base 5 di un numero naturale: $(a_0, \dots, a_9) \longmapsto a_0 + a_1 5 + \cdots + a_9 5^9$. Osservando che $5 \equiv -1 \pmod 6$, abbiamo che le stringhe da contare sono quelle per cui

$$a_0 + a_1 5 + \cdots + a_9 5^9 \equiv \sum_{i=0}^{9} (-1)^i a_1 \equiv 0 \pmod 6$$

cioè quelle che corrispondono ad un multiplo di 6. Le stringhe con 10 coordinate corrispondono ai numeri naturali tra 0 e $5^{10} - 1$ e tra questi i multipli di 6 sono $\lceil 5^{10}/6 \rceil$.

⟦Visto che $5^2 \equiv 1 \pmod 6$, di conseguenza $5^{10} \equiv 1 \pmod 6$. Ne segue che $\lceil 5^{10}/6 \rceil = 1 + (5^{10} - 1)/6 = 1 + (5^5 - 1)(5^5 + 1)/6 = 1 + (5^5 - 1)(5 + 1)(5^4 - 5^3 + 5^2 - 5 + 1)/6 = 1 + (5^5 - 1)(5^4 - 5^3 + 5^2 - 5 + 1) = 5^9 - 5^8 + 5^7 - 5^6 + 5^5 - 5^4 + 5^3 - 5^2 + 5$.⟧

56. (i) Siano $A \in X$, $a = \min A$ e $b = \max A$. Allora $b = 60 + a$, e, poiché $b \leq 100$, per a abbiamo 40 scelte, cioè gli interi tra 1 e 40. Gli insiemi $A \in X$ con $\min A = a$ e $\max A = b$ si costruiscono scegliendo $A \setminus \{a, b\}$ come un qualsiasi sottoinsieme di $\{a + 1, \dots, a + 59\}$, e per questa scelta ci sono quindi 2^{59} possibilità. Abbiamo quindi $|X| = 40 \cdot 2^{59} = 2^{62} \cdot 5$.

(ii) Siano N_2 e N_5 i sottoinsiemi di N formati rispettivamente degli interi che non sono multipli di 2 e di 5. Poniamo $Y_i = \{f \in Y \mid f(N) \subseteq N_i\}$ per $i = 2, 5$. Si

ha $Y = Y_2 \cup Y_5$ e $Y_2 \cap Y_5 = \{f \in Y \mid f(N) \subseteq N_2 \cap N_5\}$, quindi $|Y| = |Y_2 \cup Y_5| = |Y_2| + |Y_5| - |Y_2 \cap Y_5| = |N_2|^{100} + |N_5|^{100} - |N_2 \cap N_5|^{100}$. Ora $|N_2| = 50$, $|N_5| = 80$ e $|N_2 \cap N_5| = 40$ perché i non multipli di 5 sono metà pari e metà dispari. Abbiamo quindi $|Y| = 50^{100} + 80^{100} - 40^{100}$.

57. Per contare le coppie (α, β) che verificano le condizioni richieste distinguiamo 3 casi.

(1) La parola α si scrive con una sola lettera: le parole α di questo tipo sono 26, una per ogni lettera dell'alfabeto, e in questo caso β sarà una qualsiasi parola di lunghezza 3 che si può scrivere con le 25 lettere rimanenti, quindi per β ci sono 25^3 possibili scelte.

(2) La parola α si scrive con due lettere: le parole α di questo tipo sono $\binom{26}{2} \cdot 3$, cioè i modi per scegliere 2 lettere dell'alfabeto moltiplicati per il numero di parole di lunghezza 3 che si possono scrivere con 2 lettere. In questo caso β sarà una qualsiasi parola di lunghezza 3 che si può scrivere con le 24 lettere rimanenti, quindi per β ci sono 24^3 possibili scelte.

(3) Supponiamo, infine, che la parola α si scriva con 3 lettere distinte: le parole α di questo tipo sono $\binom{26}{3} \cdot 3!$, cioè i modi per scegliere 3 lettere dell'alfabeto moltiplicati per il numero di permutazioni di 3 lettere. In questo ultimo caso β sarà una qualsiasi parola di lunghezza 3 che si può scrivere con le 23 lettere rimanenti, quindi per β ci sono 23^3 possibili scelte.

In totale il numero di coppie che verificano la condizione richiesta è

$$26 \cdot 25^3 + \binom{26}{2} \cdot 2 \cdot \frac{3!}{2!} \cdot 24^3 + \binom{26}{3} \cdot 3! \cdot 23^3.$$

58. (i) Possiamo costruire le coppie (A, B) cercate scegliendo i 40 elementi di $A \cup B$, $\binom{100}{40}$ scelte, scegliendo poi tra questi i 10 elementi che formano A, e questo si può fare in $\binom{40}{10}$ modi, e infine, scegliendo il sottoinsieme di A che rappresenta l'intersezione con B, per questo abbiamo 2^{10} scelte. Ne segue che la cardinalità cercata è $\binom{100}{40}\binom{40}{10}2^{10}$.

(ii) Chiamiamo Γ l'insieme dei sottoinsiemi cercati e sia Σ l'insieme dei sottoinsiemi A di X con 5 elementi per cui $\prod_{x \in A} x \not\equiv 0 \pmod 9$. Allora $|\Gamma| = \binom{100}{5} - |\Sigma|$.

Per calcolare la cardinalità di Σ consideriamone la partizione data da:

$$\Sigma_3 = \left\{ A \subseteq X \;\middle|\; |A| = 5,\ \prod_{x \in A} x \not\equiv 0 \pmod 3 \right\}$$

$$\Sigma_9 = \left\{ A \subseteq X \;\middle|\; |A| = 5,\ \prod_{x \in A} x \equiv 0 \pmod 3,\ \prod_{x \in A} x \not\equiv 0 \pmod 9 \right\}.$$

Ora $|\Sigma_3| = \binom{100-33}{5}$ in quanto possiamo scegliere i 5 elementi di A tra i $100 - 33$ elementi non divisibili per 3. Inoltre $|\Sigma_9| = \binom{100-33}{4} \cdot 22$ in quanto si tratta di scegliere 4 elementi non divisibili per 3 e il quinto divisibile per 3 e non per 9 e

per quest'ultimo le scelte sono tra i 33 elementi multipli di 3 meno gli 11 che sono multipli di 9.

Otteniamo quindi che

$$|\Gamma| = \binom{100}{5} - \binom{100-33}{5} - \binom{100-33}{4} \cdot 22.$$

59. Indichiamo con T_k il punteggio totalizzato con i primi k lanci, e con P_k la probabilità che T_k sia divisibile per 7; vogliamo calcolare P_n. Ovviamente $T_n = T_{n-1} + i$, dove $i \in \{1, \dots, 6\}$ è il punteggio ottenuto con l'n–esimo lancio, quindi $T_n \equiv 0 \pmod 7$ se e solo se $i \equiv -T_{n-1} \pmod 7$. Ne segue che se $T_{n-1} \equiv 0 \pmod 7$ non è possibile ottenere un multiplo di 7, mentre se $T_{n-1} \not\equiv 0 \pmod 7$ c'è un unico valore di i che permette di totalizzare un multiplo di 7.

Abbiamo quindi dimostrato che P_n verifica la relazione di ricorrenza $P_n = (1 - P_{n-1})/6$.

Tenendo conto che $P_1 = 0$ è ora facile dimostrare per induzione che vale la seguente formula esplicita

$$P_n = \frac{1}{6^{n-1}} \sum_{i=0}^{n-2} 6^i (-1)^{n+i}.$$

60. (i) Poiché $(2, 3) = 1$ l'equazione data è risolubile con interi. Una soluzione particolare dell'equazione $2x + 3y = 1$ è $x = -1$, $y = 1$, quindi una soluzione particolare dell'equazione $2x + 3y = 100$ è $x = -100$, $y = 100$ e la soluzione generale con x, y interi è $x = -100 + 3k$, $y = 100 - 2k$, dove $k \in \mathbb{Z}$.

Si ha $x > 0$ se e solo se $-100 + 3k > 0$, ossia $3k > 100$, cioè $k \geq 34$. Si ha $y > 0$ se e solo se $100 - 2k > 0$, ossia $2k < 100$, cioè $k < 50$.

Pertanto vi è una soluzione in interi positivi per ogni k con $34 \leq k < 50$, e quindi ci sono 16 soluzioni di questo tipo.

(ii) L'equazione $x + y + z = 100$ con x, y, z interi positivi ha $\binom{99}{2}$ soluzioni; esse sono in corrispondenza biunivoca con i sottoinsiemi $\{x, x + y\}$ di $\{1, 2, \dots, 99\}$. Ovviamente tutte queste soluzioni sono con terne ordinate (x, y, z) con $x, y, z \in \{1, 2, \dots, 100\}$, ma solo quelle per cui gli elementi x, y, z sono tutti distinti corrispondono a sottoinsiemi di 3 elementi di $\{1, 2, \dots, 100\}$. Più precisamente, la corrispondenza è tra 6 soluzioni di questo tipo ed un sottoinsieme in quanto un insieme di 3 elementi può essere ordinato in $3! = 6$ modi.

Le terne di soluzioni che hanno due valori delle incognite uguali e il terzo diverso sono di una delle tre forme (x, x, y), (x, y, x), (y, x, x), con $2x + y = 100$. Poiché si deve avere $y = 100 - 2x$, il valore di y è determinato da x, e le disuguaglianze $x > 0$, $y > 0$ danno $0 < x < 50$, cioè 49 valori di x. Considerate le 3 forme possibili delle soluzioni, ci sono $3 \cdot 49$ soluzioni di questo tipo.

Non ci sono soluzioni con tutte e 3 le incognite uguali visto che l'equazione $3x = 100$ non ha soluzioni intere.

Pertanto le soluzioni con tutte le incognite distinte sono $\binom{99}{2} - 3 \cdot 49 = 96 \cdot 49$ e gli insiemi cercati sono $96 \cdot 49/6 = 784$.

61. Per $n = 1$ si ha $\phi(n) = 1$, quindi per $a = 43$ l'equazione proposta è risolubile. Supponiamo d'ora in poi $n > 1$, e quindi $\phi(n) < n$, ossia $a < 43$. Riscrivendo opportunamente la formula per la funzione ϕ di Eulero, si ottiene

$$\frac{\phi(n)}{n} = \prod_{p \mid n} \frac{p-1}{p} = \frac{a}{43}$$

dove il prodotto è esteso ai numeri primi che dividono n. Il più grande numero primo q che divide n compare certamente nel denominatore di $\phi(n)/n$, quindi $q = 43$. Se 43 è l'unico primo che divide n allora $n = 43^k$ per qualche intero positivo k e $\phi(n)/n = 42/43$, dunque $a = 42$.

Supponiamo ora che esista almeno un altro primo che divide n, e supponiamo che q_1 sia il più grande di questi numeri primi. Se $q_1 \nmid 42$, allora q_1 compare nel denominatore di $\phi(n)/n$, e ciò è assurdo. Quindi $q_1 = 2, 3$ o 7. Osserviamo anche che $5 \nmid n$, perché, anche se fosse $q_1 = 7$, se 5 dividesse n il denominatore di $\phi(n)/n$ sarebbe divisibile per 5, e questo è impossibile.

Pertanto n può essere solo della forma $n = 2^x 3^y 7^z 43^t$, con $x, y, z \geq 0$ e $t > 0$. Analizzando le otto possibilità in base all'essere x, y e z uguali o maggiori di zero, si ottengono gli otto possibili valori di a che sono minori di 43 e cioè: 42, 36, 28, 24, 21, 18, 14, 12.

62. (i) Possiamo riscrivere la congruenza del testo come $(a-1)(b-1) = ab - a - b + 1 \equiv 1 \pmod 3$. Si tratta quindi di considerare sottoinsiemi $\{a, b\}$ di X con $a - 1 \equiv b - 1 \equiv 1 \pmod 3$ oppure $a - 1 \equiv b - 1 \equiv -1 \pmod 3$. Nel primo caso $a \equiv b \equiv 2 \pmod 3$ e nel secondo caso $a \equiv b \equiv 0 \pmod 3$. Il numero degli elementi di X congrui a 2 modulo 3 è 33, così come il numero degli elementi di X congrui a zero modulo 3. Pertanto ci sono $\binom{33}{2}$ sottoinsiemi sia del primo che del secondo tipo, e il numero cercato è $2 \cdot \binom{33}{2} = 33 \cdot 32 = 1056$.

(ii) Siano S la famiglia dei sottoinsiemi $\{a, b\}$ di X tali che $ab \equiv 0 \pmod 3$ e T la famiglia dei sottoinsiemi $\{a, b\}$ di X tali che $a + b \equiv 0 \pmod 3$. Il numero cercato è $|S \cup T|$; per il Principio di Inclusione Esclusione, abbiamo $|S \cup T| = |S| + |T| - |S \cap T|$.

I sottoinsiemi della famiglia S sono quelli che hanno almeno un elemento divisibile per 3, quindi il complementare di S nei sottoinsiemi di due elementi di X è costituito dai sottoinsiemi che non hanno nessun elemento divisibile per 3. Ne segue che $|S| = \binom{100}{2} - \binom{67}{2} = 50 \cdot 99 - 67 \cdot 33 = 33 \cdot 83$.

I sottoinsiemi della famiglia T sono quelli per cui $b \equiv -a \pmod 3$. Quindi abbiamo o $a \equiv b \equiv 0 \pmod 3$, e ci sono $\binom{33}{2}$ sottoinsiemi di questo tipo, oppure un elemento congruo ad 1 ed un altro congruo a -1 modulo 3, per $34 \cdot 33$ sottoinsiemi di questo secondo tipo. In totale, $|T| = 33 \cdot 16 + 33 \cdot 34 = 33 \cdot 50$.

I sottoinsiemi della famiglia $S \cap T$ sono quelli che hanno entrambi gli elementi divisibili per 3: almeno un elemento per il fatto di appartenere alla famiglia S e di conseguenza entrambi per il fatto di appartenere alla famiglia T. Quindi $|S \cap T| = \binom{33}{2} = 33 \cdot 16$.

In conclusione, $|S \cup T| = 33 \cdot (83 + 50 - 16) = 33 \cdot 97 = 3201$.

63. (i) Per ogni $\sigma \in \mathsf{S}(X)$ si ha evidentemente

$$\sum_{i=1}^{100}(\sigma(i)-i)=\sum_{i=1}^{100}\sigma(i)-\sum_{i=1}^{100}i=0$$

da cui

$$\sum_{i=1}^{100}(\sigma(i)-i)\equiv 0\cdot|X_{0,\sigma}|+1\cdot|X_{1,\sigma}|+2\cdot|X_{2,\sigma}|\equiv 0 \pmod 3$$

cioè $|X_{1,\sigma}|\equiv -2\cdot|X_{2,\sigma}|\equiv|X_{2,\sigma}| \pmod 3$.

(ii) Dividiamo l'insieme X in $X_0 \sqcup X_1$ con X_0 sottoinsieme dei numeri pari e X_1 sottoinsieme dei numeri dispari. Per ogni permutazione σ, dividiamo X_0 e X_1 nel modo seguente $X_0 = X^\sigma_{0,0} \sqcup X^\sigma_{0,1}$ e $X_1 = X^\sigma_{1,0} \sqcup X^\sigma_{1,1}$ dove $X^\sigma_{i,j} = \{x \in X_i \mid \sigma(x) \in X_j\}$ per $i, j = 0, 1$.

È evidente che $|X^\sigma_{0,1}|$ può essere un qualsiasi numero intero k con $0 \le k \le 50$. Altrettanto evidentemente, se $|X^\sigma_{0,1}| = k$, allora $|X^\sigma_{1,0}| = k$ e $|X^\sigma_{0,0}| = |X^\sigma_{1,1}| = 50 - k$. Ci sono quindi $\binom{50}{k}$ scelte indipendenti sia per $X^\sigma_{0,1}$ che per $X^\sigma_{1,0}$, mentre i due insiemi $X^\sigma_{0,0}$ e $X^\sigma_{1,1}$ risultano fissati dalla scelta dei primi due, in quanto ne sono i complementari.

Inoltre, la condizione del problema è soddisfatta se e solo se valgono le condizioni seguenti: $\sigma(X^\sigma_{0,1}) = X^\sigma_{1,0}$, e questo corrisponde a $k!$ scelte; $\sigma(X^\sigma_{1,0}) = X^\sigma_{0,1}$, con $k!$ scelte; $\sigma(X^\sigma_{0,0}) = X^\sigma_{0,0}$, con $(50-k)!$ scelte, e, infine, $\sigma(X^\sigma_{1,1}) = X^\sigma_{1,1}$, con $(50-k)!$. Ne segue che il numero di permutazioni cercate è

$$\sum_{k=0}^{50}\binom{50}{k}^2 (k!)^2\cdot((50-k)!)^2=\sum_{k=0}^{50}(50!)^2=50!^2\cdot 51!.$$

64. (i) Scriviamo $x = 2^{\alpha_1}5^{\beta_1}$, $y = 2^{\alpha_2}5^{\beta_2}$, $z = 2^{\alpha_3}5^{\beta_3}$ con $\alpha_1, \alpha_2, \alpha_3$ e $\beta_1, \beta_2, \beta_3$ interi non negativi. La condizione su x, y, z è equivalente al sistema

$$\begin{cases}\alpha_1+\alpha_2+\alpha_3=100\\ \beta_1+\beta_2+\beta_3=100.\end{cases}$$

Le due equazioni sono indipendenti una dall'altra, e ciascuna ha un numero di soluzioni uguale al numero di soluzioni in interi non negativi dell'equazione $t_1 + t_2 + t_3 = 100$, ossia $\binom{102}{2}$.

Pertanto il numero di terne cercate è $\binom{102}{2}^2$.

(ii) La condizione è equivalente al sistema

$$\begin{cases}2\alpha_1+\alpha_2+\alpha_3=100\\ 2\beta_1+\beta_2+\beta_3=100\end{cases}$$

e anche in questo caso le due equazioni sono indipendenti una dall'altra. Per simmetria, possiamo limitarci a contare le soluzioni della prima. La prima equazione è

equivalente alla disequazione

$$2\alpha_1 + \alpha_2 \leq 100$$

poiché, evidentemente, essa è necessaria e d'altra parte se è soddisfatta, si può determinare in modo unico α_3 per avere $2\alpha_1 + \alpha_2 + \alpha_3 = 100$.

Questa disuguaglianza ha $101 - 2\alpha_1$ soluzioni per ogni possibile valore di α_2 tra 0 e 50 compresi. In tutto abbiamo

$$\sum_{\alpha_2=0}^{50} (101 - 2\alpha_1) = 51^2$$

soluzioni e, quindi, il numero totale di terne è $51^2 \cdot 51^2 = 51^4$.

65. Contiamo separatamente le due classi di applicazioni: (1) quelle per cui $1 \notin \mathrm{Im}(f)$ e (2) quelle per cui invece $1 \in \mathrm{Im}(f)$.

(1) Se $1 \notin \mathrm{Im}(f)$, allora $f(a) \neq 1$ e $f(b) \neq 1$ e quindi siamo sicuri che $f(a) \cdot f(b)$ non è un numero primo per ogni scelta di a e b in $X \setminus \{1\}$. Di conseguenza, visto che $|X \setminus \{1\}| = 9$, abbiamo in tutto 9^{10} applicazioni.

(2) Se $1 \in \mathrm{Im}(f)$, vuol dire che esiste $c \in X$ tale che $f(c) = 1$. Di conseguenza, affinché l'applicazione f rispetti la condizione richiesta, $f(a)$ non può essere un numero primo per nessun a in X; infatti, se così non fosse, avremmo $f(a) \cdot f(c) = f(a)$ uguale a un numero primo. D'altra parte se $f(a)$ è un numero composto per ogni $a \neq c$ in X allora sicuramente l'applicazione f rispetta la condizione.

Pertanto, dobbiamo contare le applicazioni la cui immagine è contenuta in $X \setminus \{2, 3, 5, 7\}$ e tali che $1 \in \mathrm{Im}(f)$. Per contare queste applicazioni, possiamo contare tutte le applicazioni $X \longrightarrow X \setminus \{2, 3, 5, 7\}$ e togliere da queste quelle per cui $1 \notin \mathrm{Im}(f)$, ovvero le applicazioni $X \longrightarrow X \setminus \{1, 2, 3, 5, 7\}$. Ma le applicazioni $X \to X \setminus \{2, 3, 5, 7\}$ sono 6^{10} e quelle $X \longrightarrow X \setminus \{1, 2, 3, 5, 7\}$ sono 5^{10}. Otteniamo quindi $6^{10} - 5^{10}$ applicazioni per questa seconda classe.

Sommando i due casi (1) e (2) abbiamo in tutto $9^{10} + 6^{10} - 5^{10}$ applicazioni.

⟦ Per contare le applicazioni delle seconda classe, cioè quelle da $X \longrightarrow X \setminus \{2, 3, 5, 7\}$ tali che $1 \in \mathrm{Im}(f)$, si possono anche contare le applicazioni con $|f^{-1}(1)| = k$ con $k \geq 1$ e poi sommare su tutte le cardinalità possibili. La cardinalità cercata è cioè uguale a

$$\begin{aligned}\sum_{k=1}^{10} \left|\left\{f : X \longrightarrow X \setminus \{2, 3, 5, 7\} \mid \left|f^{-1}(1)\right| = k\right\}\right| &= \sum_{k=1}^{10} \binom{10}{k} 5^{10-k} \\ &= \sum_{k=0}^{10} \binom{10}{k} 5^{10-k} - \binom{10}{0} 5^{10} \\ &= 6^{10} - 5^{10}. \qquad ⟧\end{aligned}$$

66. (i) Ogni squadra che soddisfi i vincoli richiesti può essere costruita scegliendo 2 coppie di gemelli tra le n presenti, questo si può fare in $\binom{n}{2}$ modi, quindi completandola con due persone non gemelle appartenenti alle rimanenti $n - 2$ coppie

di gemelli. Per fare quest'ultima scelta possiamo prima scegliere due coppie di gemelli tra le $n-2$ rimaste, per ciò ci sono $\binom{n-2}{2}$ modi, e poi, fissate queste, resta da scegliere in ognuna uno dei due gemelli, 2^2 scelte in totale. Concludendo, vi sono

$$\binom{n}{2}\binom{n-2}{2}2^2 = n(n-1)(n-2)(n-3)$$

squadre che soddisfano i vincoli.

(ii) Per contare il numero delle squadre possibili si contano tutte le possibili suddivisioni in 4 squadre da 6 e da queste si tolgono quelle in cui tutte le coppie di gemelli sono nella stessa squadra. Suddividere le 24 persone in 4 squadre da 6 vuol dire ripartire 24 elementi in 4 sottoinsiemi di cardinalità 6. Il numero di partizioni possibili è

$$\frac{1}{4!}\binom{24}{6}\binom{18}{6}\binom{12}{6}\binom{6}{6} = \frac{24!}{4!720^4}.$$

Da questi dobbiamo togliere le squadre in cui ogni coppia di gemelli è nella stessa squadra e queste sono

$$\frac{1}{4!}\binom{12}{3}\binom{9}{3}\binom{6}{3}\binom{3}{3} = \frac{12!}{4!6^4}.$$

La risposta alla questione posta è quindi $\frac{24!}{4!720^4} - \frac{12!}{4!6^4}$.

67. (i) Per ogni $x \in \mathbb{N}$ gli interi x^{100} e x hanno la stessa parità, dobbiamo dunque contare quei sottoinsiemi A di $X = \{1, \dots, 100\}$ per cui $\sum_{a\in A} a$ è un numero pari. Un sottoinsieme A soddisfa tale condizione se e solo se contiene una quantità pari di elementi dispari.

Consideriamo la partizione di X data dagli insiemi $X_0 = \{2, 4, \dots, 100\}$ e $X_1 = \{1, 3, \dots, 99\}$; essi hanno entrambi 50 elementi. Come per tutti gli insiemi non vuoti, i sottoinsiemi di cardinalità pari di X_1 sono tanti quanti quelli di cardinalità dispari; ci sono quindi 2^{49} sottoinsiemi di X_1 con un numero dispari di elementi. Da ciò segue che la cardinalità cercata è $2^{50} \cdot 2^{49} = 2^{99}$.

(ii) Sia (A, B) una coppia di sottoinsiemi di X che soddisfa le richieste e consideriamo la partizione di $A \cup B$ data da $A' = A \setminus (A \cap B)$, $B' = B \setminus (A \cap B)$ e $C = A \cap B$. Le condizioni imposte ci dicono che gli insiemi A' e B' possono essere scelti liberamente purché disgiunti, mentre l'insieme C, anch'esso disgiunto da A' e B', può ricadere soltanto in uno dei seguenti casi: (1) C contiene solo elementi dispari tranne esattamente un elemento multiplo di 4 ma non di 8, (2) C contiene esattamente 2 elementi pari ma non multipli di 4.

Osserviamo che in X vi sono $25 = 50 - 25$ multipli di 2 ma non di 4, $13 = 25 - 12$ multipli di 4 ma non di 8. Costruire la coppia (A, B) è equivalente a costruire la tripla (A', B', C) e, per contare queste triple, consideriamo separatamente i due casi.

Nel caso (1) abbiamo 13 scelte per l'unico multiplo di 4 che figura in C. Abbiamo poi 3 scelte per ognuno dei rimanenti 49 elementi pari di X in quanto ognuno può

essere scelto come membro di A', di B' o di nessuno dei due. Infine i 50 elementi dispari di X possono essere scelti come membri di A', B', C o di nessuno dei tre, quindi per ognuno abbiamo 4 scelte possibili. In tutto quindi $13 \cdot 3^{49} \cdot 4^{50}$ possibilità.

Analogamente, nel caso (2) abbiamo $\binom{25}{2}$ scelte per la coppia di elementi pari da mettere in C. I rimanenti 48 elementi pari di X possono essere scelti come membri di A', di B' o di nessuno dei due e, infine, i 50 elementi dispari di X possono essere scelti come membri di A', B', C o di nessuno dei tre. In tutto quindi $\binom{25}{2} \cdot 3^{48} \cdot 4^{50}$ possibilità.

Sommando quanto ottenuto nei due casi si ha la risposta

$$13 \cdot 3^{49} \cdot 4^{50} + \binom{25}{2} \cdot 3^{48} \cdot 4^{50} = 113 \cdot 3^{49} \cdot 2^{100}.$$

3.3 Congruenze

68. Osserviamo che $13 \equiv 64 \equiv 2^6 \pmod{17}$ e quindi la prima equazione diventa $2^{ax} \equiv 2^6 \pmod{17}$. Visto che l'ordine di 2 in $(\mathbb{Z}/17\mathbb{Z})^*$ è 8, abbiamo $ax \equiv 6 \pmod 8$. Quest'equazione impone che a e x non possono essere entrambi pari; infatti se così fosse si avrebbe $ax \equiv 0 \pmod 4$ contro $ax \equiv 2 \pmod 4$. Distinguiamo i casi a pari e a dispari.

(1) Se a è pari, allora, per quanto appena visto, x è dispari e quindi $x-2$ è invertibile modulo 4. Dalla seconda equazione abbiamo $x \equiv a \pmod 4$ che è impossibile perché avremmo x pari.

(2) Se invece a è dispari, allora x è pari, diciamo $x = 2y$ che nella prima equazione diventa $2ay \equiv 6 \pmod 8$ e quindi $ay \equiv 3 \pmod 4$. Ora, da a dispari ricaviamo $a^2 \equiv 1 \pmod 4$ e, quindi, la prima equazione diventa $y \equiv -a \pmod 4$; allora y è dispari. Sostituendo $x = 2y$ nella seconda abbiamo $(2y-a)(2y-2) \equiv 0 \pmod 4$ cioè $y - 1 \equiv 0 \pmod 2$ che è verificata visto che y è dispari.

Possiamo quindi concludere che, per a dispari, la soluzione è $x \equiv -2a \pmod 8$.

69. Essendo $2 \in (\mathbb{Z}/9\mathbb{Z})^*$ anche $a \equiv 2^x \in (\mathbb{Z}/9\mathbb{Z})^*$. Quindi $a \not\equiv 0 \pmod 3$, da cui $x \equiv a^2 \equiv 1 \pmod 3$.

L'ordine di $(\mathbb{Z}/9\mathbb{Z})^*$ è 6 e 2 è un suo generatore. Inoltre da $x \equiv 1 \pmod 3$ abbiamo che x può essere congruo a 1 o a 4 modulo 6. Nel primo caso $a \equiv 2^x \equiv 2 \pmod 9$, mentre nel secondo caso $a \equiv 2^x \equiv -2 \pmod 9$. Quindi $a \equiv \pm 2 \pmod 9$ è una condizione necessaria.

D'altra parte se $a \equiv 2 \pmod 9$ allora $x \equiv 1 \pmod 3$ è soluzione del sistema, mentre se $a \equiv -2 \pmod 9$ allora $x \equiv 4 \pmod 6$ è soluzione del sistema.

70. Dalla seconda congruenza abbiamo che $4 = (4, 24)$ divide a^2 e quindi a è pari, diciamo $a = 2b$. La seconda congruenza diventa $x^2 \equiv b^2 \pmod 6$.

La prima congruenza è ora $2^x \equiv 3^{2b} \equiv (3^2)^b \equiv 2^b \pmod 7$. Essa è equivalente a $x \equiv b \pmod 3$ visto che 3 è l'ordine di 2 in $(\mathbb{Z}/7\mathbb{Z})^*$. Il sistema, per $a = 2b$ pari,

è quindi equivalente a

$$\begin{cases} x^2 \equiv b^2 & (\text{mod } 6) \\ x \equiv b & (\text{mod } 3). \end{cases}$$

Dalla prima equazione abbiamo $x \equiv x^2 \equiv b^2 \equiv b \pmod 2$; è quindi necessario $x \equiv b \pmod 6$. Ma questa condizione è anche, ovviamente, sufficiente. Concludiamo che la soluzione esiste per ogni a pari.

71. Osserviamo che l'ordine di 2 in $(\mathbb{Z}/13\mathbb{Z})^*$ è 12, cioè 2 è un generatore di tale gruppo, e $3 \equiv 2^4 \pmod{13}$. Dalla seconda congruenza abbiamo $x - 1 = 3y$ per qualche y intero. Allora la prima congruenza diventa

$$(2^4)^{3y(3y+2)} = 2^{12y(3y+2)} \equiv 1 \equiv 2^a \pmod{13}.$$

Tale congruenza è quindi risolubile se e solo se $a \equiv 0 \pmod{12}$ e in tal caso $x \equiv 1 \pmod 3$ è la soluzione cercata.

72. Per prima cosa osserviamo che 2 ha ordine 3 in $(\mathbb{Z}/7\mathbb{Z})^*$, quindi 2^x dipende solo dalla classe di resto modulo 3 di x. Inoltre, la seconda equazione è equivalente al sistema $x \equiv \pm 1 \pmod 3$, $x \equiv \pm 1 \pmod 5$, con scelte indipendenti dei segni. In particolare x non è congruo a 0 modulo 3. Quindi se $x \equiv 1 \pmod 3$ allora $x \equiv 2^x \equiv 2 \pmod 7$, mentre se invece $x \equiv -1 \pmod 3$ allora $x \equiv 2^x \equiv -3 \pmod 7$.

Il sistema è quindi equivalente all'unione dei quattro sistemi

$$\begin{cases} x \equiv 1 & (\text{mod } 3) \\ x \equiv 2 & (\text{mod } 7) \\ x \equiv \pm 1 & (\text{mod } 5), \end{cases} \qquad \begin{cases} x \equiv -1 & (\text{mod } 3) \\ x \equiv -3 & (\text{mod } 7) \\ x \equiv \pm 1 & (\text{mod } 5). \end{cases}$$

Con facili calcoli si giunge alla conclusione che il sistema ha per soluzioni le classi 16, -26, 11 e -31 modulo 105.

73. Usando la definizione dei binomiali abbiamo

$$\begin{cases} \dfrac{n(n-1)(n-2)}{6} \equiv 0 & (\text{mod } 2) \\ \dfrac{n(n-1)(n-2)(n-3)}{24} \equiv 0 & (\text{mod } 2) \end{cases}$$

e quindi, eliminando gli elementi invertibili modulo 2, abbiamo

$$\begin{cases} n(n-1)(n-2) \equiv 0 & (\text{mod } 4) \\ n(n-1)(n-2)(n-3) \equiv 0 & (\text{mod } 16). \end{cases}$$

La prima equazione è chiaramente risolta per n congruo a 0, 1 e 2 modulo 4 e non risolta per n congruo a -1 modulo 4.

Per risolvere la seconda equazione, osserviamo che esattamente due fra i numeri $n, n-1, n-2, n-3$ sono pari, e che questi due numeri sono due numeri pari consecutivi. Tra due numeri pari consecutivi, solo uno dei due può essere divisibile

per 4, mentre l'altro è divisibile per 2 ma non per 4. Pertanto, se il prodotto deve essere divisibile per 16, il numero divisibile per 4 deve essere, in realtà, divisibile per 8. Ne segue che la seconda congruenza è risolubile per n congruo a 0, 1, 2, 3 modulo 8.

Poiché n congruo ad a modulo 8 implica n congruo ad a modulo 4, le soluzioni del sistema sono n congruo a 0, 1, 2 modulo 8.

74. La congruenza $x^2 \equiv 4 \pmod{14}$ è equivalente al sistema delle due congruenze $x^2 \equiv 0 \pmod 2$ e $x^2 \equiv 4 \pmod 7$. Inoltre la prima di questa due può essere riscritta come $x \equiv 0 \pmod 2$ visto che x^2 è sempre congruo a x modulo 2.

La seconda, a sua volta, diventa $(x-2)(x+2) \equiv 0 \pmod 7$ e, visto che 7 è primo, le soluzioni sono $x \equiv 2 \pmod 7$ o $x \equiv -2 \pmod 7$.

Quindi le soluzioni del sistema originario sono date dall'unione delle soluzioni dei due sistemi

$$\begin{cases} x \equiv 0 & \pmod 2 \\ x \equiv 2 & \pmod 7 \\ x \equiv 3 & \pmod 5, \end{cases} \qquad \begin{cases} x \equiv 0 & \pmod 2 \\ x \equiv -2 & \pmod 7 \\ x \equiv 3 & \pmod 5. \end{cases}$$

Con facili calcoli abbiamo che le soluzioni del sistema sono date dalle classi di resto -12 e -2 modulo 70.

75. Fattorizziamo in primi 847 come $7 \cdot 11^2$. Quindi la prima congruenza diventa il sistema delle due congruenze $x^{660} \equiv 1 \pmod 7$ e $x^{660} \equiv 1 \pmod{11^2}$.

Occupiamoci della prima di esse. È chiaro che se 7 dividesse x allora 7 dividerebbe anche x^{660} contro $x^{660} \equiv 1 \pmod 7$. D'altra parte se 7 non divide x allora $x^6 \equiv 1 \pmod 7$ per il Piccolo Teorema di Fermat. Quindi $x^{660} = (x^6)^{110} \equiv 1^{110} \equiv 1 \pmod 7$. Abbiamo quindi visto che la prima congruenza è risolta da ogni x non divisibile per 7.

Analogamente ragioniamo per la seconda congruenza. Se 11 dividesse x allora 11 dividerebbe anche x^{660}, cosa impossibile. Allora $x^{\phi(11^2)} = x^{110} \equiv 1 \pmod{11}$ e quindi $x^{660} = (x^{110})^6 \equiv 1^6 = 1 \pmod{11^2}$. Quindi la seconda congruenza è risolta da ogni x non divisibile per 11.

Possiamo quindi riscrivere in sistema originario come

$$\begin{cases} x \not\equiv 0 & \pmod 7 \\ x \not\equiv 0 & \pmod{11} \\ x \equiv 11 & \pmod{13}. \end{cases}$$

Le soluzioni della terza sono ovviamente tutti gli interi $x = 11 + 13k$ con k intero. Imponendo che x non sia divisibile per 7 e non sia divisibile per 11 troviamo che k non può essere congruo a 4 modulo 7 e non può essere congruo a 0 modulo 11.

76. Scomponendo in fattori $85 = 5 \cdot 17$ la congruenza considerata è equivalente al sistema

$$\begin{cases} x^3 - a^3 \equiv 0 & \pmod 5 \\ x^3 - a^3 \equiv 0 & \pmod{17}. \end{cases}$$

Sia ora p uno dei due primi 5 o 17. Se $a \equiv 0 \pmod{p}$ allora abbiamo $x^3 \equiv 0 \pmod{p}$ e quindi $x \equiv 0 \equiv a \pmod{p}$ visto che p è primo. Se invece $a \not\equiv 0 \pmod{p}$, allora a è invertibile modulo p e, quindi, possiamo riscrivere la congruenza come $(x/a)^3 \equiv 1 \pmod{p}$.

Visto che sicuramente 0 non è soluzione e 3 non divide $p-1$ l'unica possibile soluzione è $x/a \equiv 1 \pmod{p}$, cioè $x \equiv a \pmod{p}$.

Allora il sistema è in ogni caso equivalente a

$$\begin{cases} x \equiv a & (\text{mod } 5) \\ x \equiv a & (\text{mod } 17) \end{cases}$$

e, visto che $x \equiv a \pmod{85}$ è una soluzione, essa è l'unica soluzione possibile per il Teorema Cinese dei Resti.

Quindi possiamo concludere che, per ogni a, la congruenze $x^3 - a^3 \equiv 0 \pmod{85}$ ha solo la soluzione $x \equiv a \pmod{85}$.

77. Osserviamo che 2 è primo con 3^3 e quindi $2^{\phi(3^3)} = 2^{18} \equiv 1 \pmod{3^3}$. Visto che 9 e 6 sono gli unici divisori massimali propri di 18, calcoliamo 2^9 e 2^6 modulo 3^3. Troviamo che $2^9 \equiv -1 \pmod{3^3}$ e $2^6 \equiv 10 \pmod{3^3}$. Questo ci permette di concludere che 2 ha ordine moltiplicativo 18 modulo 3^3. Inoltre $2^5 = 32 \equiv 5 \pmod{3^3}$.

Possiamo allora riscrivere la congruenza iniziale come $2^x \equiv 2^5 \pmod{3^3}$ e concludere che essa è equivalente a $x \equiv 5 \pmod{18}$.

Il primo dei due sistemi da risolvere può essere, quindi, riscritto in modo equivalente come

$$\begin{cases} x \equiv 5 & (\text{mod } 18) \\ x \equiv 2 & (\text{mod } 15). \end{cases}$$

E per il Teorema Cinese dei Resti, fattorizzando in primi, abbiamo il sistema

$$\begin{cases} x \equiv 5 & (\text{mod } 9) \\ x \equiv 1 & (\text{mod } 2) \\ x \equiv 2 & (\text{mod } 3) \\ x \equiv 2 & (\text{mod } 5). \end{cases}$$

Osserviamo ora che la prima congruenza implica la terza e quindi quest'ultima può essere rimossa dal sistema. Con semplici calcoli troviamo che le soluzioni sono $-13 + 90k$ con k intero.

Mostriamo invece che il secondo sistema del testo non ha alcuna soluzione. Se $2^x \equiv 5 \pmod{3^4}$ allora, in particolare, $2^x \equiv 5 \pmod{3^3}$ e quindi $x \equiv 5 \pmod{18}$ per quanto visto sopra. Quindi $x \equiv -1 \pmod{3}$ e il sistema è incompatibile in quanto dall'ultima congruenza abbiamo $x \equiv 0 \pmod{3}$.

78. (i) Se $81^x \equiv b \pmod{125}$ allora sicuramente $81^x \equiv b \pmod{5}$, cioè $b \equiv 1 \pmod{5}$. Quindi per avere soluzione la classe di b modulo 125 può essere solo una delle 25 classi congrue a 1 modulo 5. Vediamo come questo sia anche sufficiente.

Osserviamo che 81 è primo con 125 e calcoliamone l'ordine moltiplicativo. Visto che $\phi(125) = 100$ tale ordine deve essere un divisore di 100. Cominciamo con calcolare 81^5 modulo 125.

Si ha $81 = 1 + 16 \cdot 5$ e quindi $81^5 = (1 + 16 \cdot 5)^5 \equiv 1 + 5 \cdot 16 \cdot 5 + 10 \cdot 16^2 \cdot 5^2 + \cdots \equiv 1 + 16 \cdot 5^2 \equiv 1 + 5^2 \pmod{125}$ dove abbiamo tralasciato di scrivere altri termini sicuramente congrui a 0 modulo 125 in quanto contengono potenze ancora maggiori di 5. Quanto visto finora ci permette di dire che 81 non ha ordine moltiplicativo un divisore di 5 modulo 125.

Continuando in modo analogo abbiamo $81^{25} = (81^5)^5 \equiv (1+5^2)^5 \equiv 1+5 \cdot 5^2 + \cdots \equiv 1 \pmod{125}$. Questo prova che l'ordine cercato deve essere un divisore di 25 e, non essendo 1 o 5 per quanto visto sopra, esso è 25.

Ma questo dice che le potenze di 81 modulo 125 sono 25 classi distinte. Visto che la congruenza data ha soluzione se e solo se b è una potenza di 81 modulo 125 abbiamo provato che la condizione trovata all'inizio è anche sufficiente.

(ii) Visto che x_0 è una soluzione allora $81^{x_0} \equiv b_0 \pmod{125}$. La congruenza diventa quindi $81^x \equiv 81^{x_0} \pmod{125}$ e, visto che 81 ha ordine moltiplicativo 25 modulo 125, tutte le soluzioni sono date da $x_0 + 25 \cdot k$ con k intero qualsiasi.

79. Calcoliamo, per prima cosa, l'ordine moltiplicativo di 2 modulo 125; esso è un divisore di $\phi(125) = 100$.

Osserviamo che se $2^n \equiv 1 \pmod{125}$ allora $2^n \equiv 1 \pmod 5$. Ne segue che, poiché l'ordine moltiplicativo di 2 modulo 5 è 4, l'ordine moltiplicativo di 2 modulo 125 è un multiplo di 4, ossia uno tra i numeri 4, 20, 100.

Abbiamo $2^4 = 16 = 1 + 3 \cdot 5$, da cui, usando lo sviluppo delle potenze di un binomio, $2^{20} = (2^4)^5 = (1 + 3 \cdot 5)^5 \equiv 1 + 3 \cdot 5^2 \pmod{5^3}$. L'ordine di 2 modulo 5^3 non può quindi essere un divisore di 20, e pertanto esso è uguale a 100.

Visto che $2^7 = 128 \equiv 3 \pmod{125}$, 7 è una soluzione della congruenza. In particolare la congruenza si può riscrivere come $2^x \equiv 2^7 \pmod{125}$ e, per quando provato sopra, tutte le soluzioni sono date da $7 + 100k$ con k intero qualsiasi.

Vediamo ora la soluzione della congruenza modulo $625 = 5^4$. Abbiamo già osservato che $2^{4 \cdot 5} \equiv 1 + 3 \cdot 5^2 \pmod{5^3}$, cioè $2^{4 \cdot 5} = 1 + 3 \cdot 5^2 + h \cdot 5^3$ per qualche intero h. Usando ancora lo sviluppo delle potenze di un binomio, abbiamo $2^{4 \cdot 5^2} = (1 + 3 \cdot 5^2 + h \cdot 5^3)^5 = (1 + (3 + 5h)5^2)^5 \equiv 1 + 5(3 + 5h)5^2 \equiv 1 + 3 \cdot 5^3 \pmod{5^4}$. Una soluzione di $2^x \equiv 3 \pmod{5^4}$ è anche una soluzione di $2^x \equiv 3 \pmod{5^3}$ e quindi $x = 7 + 100k$ per quanto già visto.

Mettendo insieme $2^7 = 3 + 5^3$ e $2^{100k} \equiv (1 + 3 \cdot 5^3)^k \equiv 1 + 3k5^3 \pmod{5^4}$, otteniamo $2^x = 2^{7+100k} \equiv (3 + 5^3)(1 + 3k5^3) \equiv 3 + (1 + 9k)5^3 \pmod{5^4}$; quindi x è soluzione se e solo se $k \equiv 1 \pmod 5$. Concludiamo $x \equiv 107 \pmod{500}$.

80. Calcolando le potenze di 5 modulo 11 vediamo che 5 ha ordine moltiplicativo 5 modulo 11 e che $3 \equiv 5^2 \pmod{11}$. Quindi la prima congruenza può essere riscritta come $5^x \equiv 5^2 \pmod{11}$ e essa è quindi equivalente a $x \equiv 2 \pmod 5$.

Per il Teorema Cinese dei Resti, la seconda congruenza è equivalente al sistema

$$\begin{cases} x^2 \equiv 0 & \pmod 3 \\ x^2 \equiv -3 & \pmod 7. \end{cases}$$

La prima di queste congruenze è equivalente a $x \equiv 0 \pmod 3$ in quanto 3 è un numero primo. La seconda è equivalente a $x \equiv \pm 2 \pmod 7$ visto che 7 è primo e $(\pm 2)^2 \equiv 3 \pmod 7$.

Possiamo quindi riscrivere il sistema del testo come

$$\begin{cases} x \equiv 0 & \pmod 3 \\ x \equiv 2 & \pmod 5 \\ x \equiv \pm 2 & \pmod 7. \end{cases}$$

Con semplici calcoli vediamo che le classi di resto 12 e 72 modulo 105 sono le soluzioni del sistema.

81. La condizione data è equivalente alla congruenza

$$7x^3 - 8ax^2 + 9x + 3a \equiv 0 \pmod{21}$$

e questa a sua volta è equivalente al sistema

$$\begin{cases} 7x^3 - 8ax^2 + 9x + 3a \equiv 0 & \pmod 3 \\ 7x^3 - 8ax^2 + 9x + 3a \equiv 0 & \pmod 7. \end{cases}$$

Riducendo i coefficienti delle equazioni, si ottiene infine

$$\begin{cases} x^3 + ax^2 \equiv 0 & \pmod 3 \\ -ax^2 + 2x + 3a \equiv 0 & \pmod 7. \end{cases}$$

Poiché $x^3 + ax^2 = x^2(x + a)$ e 3 è un numero primo, la prima equazione ha le soluzioni $x \equiv 0 \pmod 3$ e $x \equiv -a \pmod 3$.

Per la risolubilità della seconda equazione, si ha

$x \equiv 0 \pmod 7$ è soluzione $\Longrightarrow a \equiv 0 \pmod 7$;
$x \equiv 1 \pmod 7$ è soluzione $\Longrightarrow a \equiv -1 \pmod 7$;
$x \equiv 2 \pmod 7$ è soluzione $\Longrightarrow a \equiv -3 \pmod 7$;
$x \equiv 3 \pmod 7$ è soluzione $\Longrightarrow a \equiv 1 \pmod 7$;
$x \equiv -3 \pmod 7$ è soluzione $\Longrightarrow a \equiv -1 \pmod 7$;
$x \equiv -2 \pmod 7$ è soluzione $\Longrightarrow a \equiv 3 \pmod 7$;
$x \equiv -1 \pmod 7$ è soluzione $\Longrightarrow a \equiv 1 \pmod 7$.

In funzione di a, la tabella precedente si può riassumere nel seguente modo

se $a \equiv 0 \pmod 7$ allora $x \equiv 0 \pmod 7$;
se $a \equiv 1, -1, 3 \pmod 7$ allora c'è la soluzione $x \equiv a + 2 \pmod 7$;
se $a \equiv 1, -1, -3 \pmod 7$ allora c'è la soluzione $x \equiv a - 2 \pmod 7$;
se $a \equiv \pm 2 \pmod 7$ non ci sono soluzioni.

Se entrambe le equazioni del sistema sono risolubili, allora il sistema è risolubile, perché $(3, 7) = 1$. Risolvendo i vari sistemi in cui le equazioni sono risolubili, si ottiene

se $a \equiv 0 \pmod 7$, allora $x \equiv 0, -a \pmod{21}$;
se $a \equiv 1, -1, 3 \pmod 7$, allora ci sono le soluzioni $x \equiv 15a + 9, 8a + 9 \pmod{21}$;

se $a \equiv 1, -1, -3 \pmod 7$, allora ci sono le soluzioni $x \equiv 15a + 12, 8a + 12 \pmod{21}$.

82. Per il Teorema Cinese dei Resti, la congruenza è equivalente al sistema

$$\begin{cases} x^{15} \equiv x^{27} & \pmod 7 \\ x^{15} \equiv x^{27} & \pmod{11} \end{cases}$$

che può essere riscritto nella forma

$$\begin{cases} x^{15}(x^{12} - 1) \equiv 0 & \pmod 7 \\ x^{15}(x^{12} - 1) \equiv 0 & \pmod{11}. \end{cases}$$

Evidentemente $x \equiv 0 \pmod 7$ e $x \equiv 0 \pmod{11}$ sono soluzioni, rispettivamente, della prima e della seconda equazione. Se $(x, 7) = 1$, allora, per il Piccolo Teorema di Fermat, si ha $x^6 \equiv 1 \pmod 7$ e quindi anche $x^{12} \equiv 1 \pmod 7$. Pertanto la prima equazione è verificata per ogni intero x, cioè 7 soluzioni modulo 7.

Per quando riguarda la seconda equazione, il Piccolo Teorema di Fermat dice che, se $(x, 11) = 1$, allora $x^{10} \equiv 1 \pmod{11}$; pertanto per questi valori si ha soluzione se e solo se $x^2 \equiv 1 \pmod{11}$, ossia $(x + 1)(x - 1) \equiv 0 \pmod{11}$. Poiché 11 è un numero primo, le uniche soluzioni sono $x \equiv \pm 1 \pmod{11}$. Insieme alla soluzione $x \equiv 0 \pmod{11}$ si hanno in totale 3 soluzioni modulo 11.

Il numero delle soluzioni modulo 77 è dato dalle combinazioni delle soluzioni modulo 7 con le soluzioni modulo 11 ed è dunque uguale a $7 \cdot 3 = 21$.

83. Per la seconda condizione, i numeri interi x tali che $x^3 \equiv x \pmod 7$ non sono mai soluzioni del sistema. Ora $x^3 \equiv x \pmod 7$ è equivalente a $x(x - 1)(x + 1) \equiv 0 \pmod 7$ e, poiché 7 è un numero primo, le soluzioni di questa equazione sono $x \equiv 0, 1, -1 \pmod 7$.

In particolare, visto che la classe $\overline{0}$ modulo 7 non è mai una soluzione, la prima equazione si può scrivere equivalentemente nella forma $x^{k-1} \equiv 1 \pmod 7$. Una classe a è soluzione di quest'ultima equazione se e solo se $k - 1$ è multiplo dell'ordine moltiplicativo di a modulo 7. Per verifica diretta, l'ordine moltiplicativo delle classi $\overline{2}$ e $\overline{4}$ è 3, mentre quello delle classi $\overline{3}$ e $\overline{5}$ è 6. Pertanto, se $k \equiv 1 \pmod 6$, le soluzioni sono $x \equiv 2, 3, 4, 5 \pmod 7$; se $k \equiv 1 \pmod 3$ ma $k \not\equiv 1 \pmod 6$, ossia se $k \equiv 4 \pmod 6$, le soluzioni sono $x \equiv 2, 4 \pmod 7$ e se, infine, $k \not\equiv 1 \pmod 3$, non ci sono soluzioni.

84. Perché la prima equazione sia risolubile è necessario e sufficiente che $(a, 25) \mid 4$, ossia che $(a, 25) = 1$. La seconda equazione è equivalente al sistema

$$\begin{cases} x^2 + a \equiv 0 & \pmod 5 \\ x^2 + a \equiv 0 & \pmod 3 \end{cases}$$

e, per verifica diretta, si vede che questo è risolubile se e solo se $a \equiv 0, \pm 1 \pmod 5$ e $a \equiv 0, -1 \pmod 3$. Dunque le due equazioni sono entrambe risolubili per $a \equiv \pm 1 \pmod 5$ e $a \equiv 0, -1 \pmod 3$.

Poiché però il massimo comune divisore dei moduli delle due equazioni è $(25, 15) = 5$, il sistema è risolubile se e solo se ci sono soluzioni delle due equazioni che hanno la stessa classe di congruenza modulo 5.

Se $a \equiv 1 \pmod 5$ le soluzioni della prima equazione sono congrue a $-1 \pmod 5$, mentre quelle della seconda equazione sono congrue a $\pm 2 \pmod 5$. Se $a \equiv -1 \pmod 5$, le soluzioni della prima equazione sono congrue a $1 \pmod 5$, e quelle della seconda sono congrue a $\pm 1 \pmod 5$. Dunque il sistema è risolubile se e solo se $a \equiv -1 \pmod 5$ e $a \equiv 0, -1 \pmod 3$, cioè se e solo se $a \equiv -1, 9 \pmod{15}$.

Consideriamo ora il caso $a = -1$. La prima equazione dà $x \equiv -4 \pmod{25}$; dunque la classe delle soluzioni modulo 25 è univocamente determinata ed è $x \equiv 1 \pmod 5$. Inoltre, per la discussione precedente, esistono soluzioni della seconda equazione che rispettano questa condizione. Restano dunque da trovare le soluzioni che soddisfano anche $x^2 - 1 \equiv 0 \pmod 3$, ossia $x \equiv \pm 1 \pmod 3$. Mettendo insieme le soluzioni modulo 25 e modulo 3, concludiamo che le soluzioni del sistema sono $x \equiv -4, -29 \pmod{75}$.

85. Entrambe le equazioni sono risolubili solo se $(a, 9) = 1$. La soluzione della prima equazione sarà allora $x \equiv a^{-1} \pmod 9$, e quindi sarà coprima con 9, mentre la soluzione della seconda equazione sarà $x \equiv 0 \pmod{\operatorname{ord}(a)}$, dove $\operatorname{ord}(a)$ indica l'ordine di a nel gruppo moltiplicativo $(\mathbb{Z}/9\mathbb{Z})^*$, in particolare $\operatorname{ord}(a)$ è un divisore di $\phi(9) = 6$. Perché il sistema sia risolubile occorre quindi che $\operatorname{ord}(a)$ non sia multiplo di 3, ossia $\operatorname{ord}(a) = 1, 2$.

Se $\operatorname{ord}(a) = 1$ allora $a \equiv 1 \pmod 9$, la soluzione della prima equazione è $x \equiv 1 \pmod 9$ mentre la seconda equazione è vera per ogni intero x. Pertanto la soluzione del sistema è $x \equiv 1 \pmod 9$.

Se $\operatorname{ord}(a) = 2$, allora $a \not\equiv 1 \pmod 9$ e $a^2 \equiv 1 \pmod 9$, ossia $9 \mid a^2 - 1 = (a + 1)(a - 1)$. In particolare 3 divide uno dei fattori $a + 1$, $a - 1$, ma non può dividerli entrambi perché la loro differenza è 2. Ne segue che 9 deve dividere uno dei fattori; avendo escluso $a \equiv 1 \pmod 9$, si ha necessariamente $a \equiv -1 \pmod 9$.

Allora la prima equazione ha per soluzione $x \equiv -1 \pmod 9$ mentre la seconda $x \equiv 0 \pmod 2$. La soluzione del sistema è quindi $x \equiv 8 \pmod{18}$.

86. La prima equazione è risolubile se e solo se $(6a - 1, 21) = 1$, ossia se e solo se $3 \nmid 6a - 1$ e $7 \nmid 6a - 1$. Poiché $3 \mid 6a$ per ogni a, si ha che $3 \nmid 6a - 1$ per ogni a; invece $7 \mid 6a - 1$ se e solo se $a \equiv -1 \pmod 7$. Pertanto la prima equazione è risolubile se e solo se $a \not\equiv -1 \pmod 7$.

La seconda equazione è sempre risolubile, esprimendo già la soluzione.

Il massimo comune divisore dei moduli delle due equazioni è 7, quindi, supposto che la prima equazione sia risolubile, il sistema è risolubile se e solo se le soluzioni delle due equazioni coincidono modulo 7. Sostituendo il valore di x dato dalla seconda equazione nella prima si ottiene la condizione $(6a - 1)a \equiv 1 \pmod 7$, che ha per soluzioni $a \equiv 2, 4 \pmod 7$.

Osserviamo ora che, se $a \equiv 2, 4 \pmod 7$, la soluzione del sistema è una classe di congruenza modulo il minimo comune multiplo dei moduli, cioè 105. Poiché dalla

seconda equazione si ha la classe della soluzione modulo 35, è sufficiente determinare dalla prima equazione la classe della soluzione modulo 3, che è evidentemente $x \equiv -1 \pmod 3$. Abbiamo così il sistema

$$\begin{cases} x \equiv -1 & \pmod 3 \\ x \equiv a & \pmod{35} \end{cases}$$

e, con facili calcoli, ricaviamo la soluzione $x \equiv 36a + 35 \pmod{105}$.

87. Per il Teorema Cinese dei Resti, la prima equazione è equivalente ad un sistema di due congruenze, una modulo 2 ed una modulo 17. Poiché $9 \equiv 1 \pmod 2$, la congruenza modulo 2 è soddisfatta per tutti i valori di a e di x e quindi può essere eliminata dal sistema. Per la congruenza modulo 17, si vede per verifica diretta che l'ordine moltiplicativo di 9 modulo 17 è 8, quindi la congruenza è risolta se e solo se $ax \equiv 0 \pmod 8$. In particolare, la congruenza è risolubile per tutti i valori di a e la soluzione è $x \equiv 0 \pmod{8/(a, 8)}$.

Analogamente, sostituiamo la seconda equazione con due congruenze, una modulo 3 ed una modulo 5. La congruenza modulo 3 si riduce a $x^2 \equiv 0 \pmod 3$, che non dipende da a ed ha per soluzione $x \equiv 0 \pmod 3$. La congruenza modulo 5 si riduce a $x^2 + ax - 1 \equiv 0 \pmod 5$ che ha soluzione se e solo se $a^2 + 4$ è un quadrato modulo 5, e cioè se e solo se $a \equiv 0, 1, -1 \pmod 5$. Le soluzioni sono, rispettivamente, $x \equiv \pm 1, 2, -2 \pmod 5$.

Il sistema è dunque risolubile se e solo se $a \equiv 0, 1, -1 \pmod 5$.

In particolare per $a = 4$, usando quanto visto sopra, la soluzione si determina mediante il sistema

$$\begin{cases} x \equiv 0 & \pmod 2 \\ x \equiv 0 & \pmod 3 \\ x \equiv -2 & \pmod 5. \end{cases}$$

Con semplici calcoli si ottiene $x \equiv 18 \pmod{30}$.

88. La prima equazione è risolubile se e solo se $(3, 42) = 3 \mid a$, ossia se e solo se $a = 3b$ con $b \in \mathbb{Z}$, e in tal caso l'equazione diventa $x \equiv b \pmod{14}$. Poiché 6 è l'inverso di 6 modulo 35 la seconda equazione è equivalente a $x \equiv 6 \pmod{35}$. Usando il Teorema Cinese dei Resti il sistema diventa

$$\begin{cases} x \equiv b & \pmod 2 \\ x \equiv b & \pmod 7 \\ x \equiv 6 & \pmod 7 \\ x \equiv 1 & \pmod 5 \end{cases}$$

e quest'ultimo è quindi risolubile se e solo se $b \equiv 6 \pmod 7$, cioè se e solo se $a \equiv 18 \pmod{21}$.

Sotto questa condizione su a il sistema è quindi equivalente a

$$\begin{cases} x \equiv b & \pmod 2 \\ x \equiv 6 & \pmod{35} \end{cases}$$

ed ha soluzione $x \equiv 6 + 35b \pmod{70}$.

Concludendo, il sistema è risolubile se e solo se $a \equiv 18 \pmod{21}$ e in tal caso la soluzione è $x \equiv 6 \pmod{70}$ se $a \equiv 18 \pmod{42}$, e $x \equiv 41 \pmod{70}$ se $a \equiv 39 \pmod{42}$.

89. L'ordine della classe di 5 modulo 2^4 è 4 e $5^2 \equiv 9 \pmod{2^4}$, quindi la prima equazione è equivalente a $x \equiv 2 \pmod{4}$.

Usando il Teorema Cinese dei Resti, spezziamo la seconda equazione in una congruenza modulo 11 e in una congruenza modulo 16. Poiché 11 è un primo dispari, l'equazione $x^2 + 2x + 8 \equiv 0 \pmod{11}$ può essere risolta con la formula per le equazioni di secondo grado, ottenendo come soluzioni $x \equiv 1, -3 \pmod{11}$.

Consideriamo ora il sottosistema

$$\begin{cases} x \equiv 2 & \pmod{4} \\ x^2 + 2x + 8 \equiv 0 & \pmod{16} \end{cases}$$

sostituendo il valore di x ottenuto dalla prima congruenza, $x = 2 + 4t$, nella seconda congruenza, otteniamo

$$(2 + 4t)^2 + 2(2 + 4t) + 8 \equiv 8t \equiv 0 \pmod{16}$$

e questa equazione è verificata se e solo se $t \equiv 0 \pmod{2}$, cioè il sottosistema ha soluzione $x \equiv 2 \pmod{8}$.

Il sistema assegnato è quindi equivalente all'unione dei due sistemi

$$\begin{cases} x \equiv 1 & \pmod{11} \\ x \equiv 2 & \pmod{8}, \end{cases} \qquad \begin{cases} x \equiv -3 & \pmod{11} \\ x \equiv 2 & \pmod{8} \end{cases}$$

che hanno rispettivamente soluzione $x \equiv 34 \pmod{88}$ e $x \equiv -14 \pmod{88}$, come si trova subito con facili calcoli.

90. La seconda equazione è risolubile se e solo se $3 \mid a$, sia quindi $a = 3b$. La congruenza $6x \equiv 3b \pmod{21}$ è equivalente a $x \equiv 4b \pmod{7}$.

La prima congruenza diventa $x^2 \equiv 15b \pmod{120}$ ed essa può essere spezzata, per il Teorema Cinese dei Resti, in due congruenze modulo 8 e modulo 15. Tenendo inoltre presente che $x^2 \equiv 0 \pmod{15}$ se e solo se $x \equiv 0 \pmod{15}$, otteniamo il sistema

$$\begin{cases} x^2 \equiv -b & \pmod{8} \\ x \equiv 0 & \pmod{15} \\ x \equiv 4b & \pmod{7}. \end{cases}$$

I moduli delle congruenze di questo sistema sono due a due coprimi, quindi il sistema è risolubile se e solo se le singole equazioni sono risolubili. In questo caso, poiché la seconda e la terza equazione sono già risolte, l'unica condizione da imporre è la risolubilità della prima equazione, ovvero che $-b$ sia un quadrato modulo 8, cioè $b \equiv 0, -1, 4 \pmod{8}$.

Concludendo, il sistema è risolubile se e solo se $a = 3b \equiv 0, -3, 12 \pmod{24}$.

Per $a = 45 \equiv -3 \pmod{24}$, e quindi con la notazione precedente $b = 15$, il sistema è risolubile e diventa

$$\begin{cases} x^2 \equiv 1 & (\text{mod } 8) \\ x \equiv 0 & (\text{mod } 15) \\ x \equiv 4 & (\text{mod } 7). \end{cases}$$

Si verifica facilmente che il sottosistema formato dalla seconda e dalla terza congruenza ha soluzione $x \equiv 60 \pmod{105}$ e che la prima equazione ha soluzione $x \equiv 1, 3, 5, 7 \pmod 8$, cioè $x \equiv 1 \pmod 2$. Il sistema è quindi equivalente a

$$\begin{cases} x \equiv 1 & (\text{mod } 2) \\ x \equiv 60 & (\text{mod } 105) \end{cases}$$

che ha soluzione $x \equiv 165 \pmod{210}$.

91. Per il Teorema Cinese dei Resti, l'equazione assegnata è equivalente al sistema

$$\begin{cases} x^{100} \equiv a & (\text{mod } 7) \\ x^{100} \equiv a & (\text{mod } 11). \end{cases}$$

Contiamo le soluzioni di ognuna delle due equazioni.

La congruenza $x^{100} \equiv a \pmod 7$ ha, per $a \equiv 0 \pmod 7$, l'unica soluzione $x \equiv 0 \pmod 7$.

Sia quindi $a \not\equiv 0 \pmod 7$, allora $x \equiv 0 \pmod 7$ non è soluzione dell'equazione e le eventuali soluzioni verificano $x^6 \equiv 1 \pmod 7$. Poiché $100 = 16 \cdot 6 + 4$, l'equazione da risolvere è equivalente a $x^4 \equiv a \pmod 7$. Le quarte potenze in $(\mathbb{Z}/7\mathbb{Z})^*$ sono $\overline{1}, \overline{2}, \overline{4}$, quindi se $a \equiv 3, 5, 6 \pmod 7$ l'equazione non ha soluzioni, mentre se $a \equiv 1, 2, 4 \pmod 7$ l'equazione ha due soluzioni.

Per $a \equiv 0 \pmod{11}$, la congruenza $x^{100} \equiv a \pmod{11}$ ha l'unica soluzione $x \equiv 0 \pmod{11}$.

Sia quindi $a \not\equiv 0 \pmod{11}$, allora $x \equiv 0 \pmod{11}$ non è soluzione dell'equazione e le eventuali soluzioni verificano $x^{10} \equiv 1 \pmod{11}$, quindi anche $x^{100} \equiv 1 \pmod{11}$. Ne segue che l'equazione ha 10 soluzioni se $a \equiv 1 \pmod{11}$, mentre non ha soluzioni per $a \not\equiv 0, 1 \pmod{11}$.

Mettiamo ora insieme quanto ottenuto per le singole equazioni.

Per $a \equiv 0 \pmod 7$ e $a \equiv 0 \pmod{11}$, cioè per $a \equiv 0 \pmod{77}$, il sistema ha l'unica soluzione $x \equiv 0 \pmod{77}$.

Per $a \equiv 0 \pmod 7$ e $a \equiv 1 \pmod{11}$, cioè per $a \equiv -21 \pmod{77}$, la prima equazione ha un'unica soluzione e la seconda ne ha 10, quindi ci sono 10 soluzioni modulo 77.

Per $a \equiv 1, 2, 4 \pmod 7$ e $a \equiv 0 \pmod{11}$, cioè per $a \equiv 22, 44, 11 \pmod{77}$, la prima equazione ha 2 soluzioni e la seconda ne ha 1, quindi ci sono 2 soluzioni modulo 77.

Infine, per $a \equiv 1, 2, 4 \pmod 7$ e $a \equiv 1 \pmod{11}$, cioè per $a \equiv 1, 23, 67 \pmod{77}$, la prima equazione ha 2 soluzioni e la seconda ne ha 10, quindi ci sono 20 soluzioni modulo 77.

Se, invece, a non è in una di queste classi modulo 77 l'equazione non ha soluzione.

92. (i) Per il Teorema Cinese dei Resti $x^a \equiv 1 \pmod{92}$ può essere spezzata in una congruenza modulo 4 e una modulo 23.

La congruenza $x^a \equiv 1 \pmod{23}$ ha come soluzione gli elementi di $(\mathbb{Z}/23\mathbb{Z})^*$ il cui ordine divide a, ed è quindi equivalente a $x^d \equiv 1 \pmod{23}$ dove $d = (a, \phi(23))$. Poiché 23 è un numero primo, il gruppo $(\mathbb{Z}/23\mathbb{Z})^*$ è ciclico di ordine $\phi(23) = 22$. Possiamo concludere che $x^a \equiv 1 \pmod{23}$ ha $d = (a, 22)$ soluzioni modulo 23.

Con gli stessi argomenti si ottiene che $x^a \equiv 1 \pmod{4}$ ha $(a, 2)$ soluzioni modulo 4.

Concludendo, l'equazione assegnata ha $(a, 2) \cdot (a, 22)$ soluzioni modulo 92.

Osserviamo che il numero di soluzioni può anche essere espresso in termini della classe di a modulo 22.

Se $a \equiv 1, 3, 5, 7, 9, 13, 15, 17, 19, 21 \pmod{22}$, cioè $(a, 2) = 1$ e $(a, 22) = 1$, l'equazione ha una sola soluzioni modulo 92.

Se $a \equiv 2, 4, 6, 8, 10, 12, 14, 16, 18, 20 \pmod{22}$, cioè $(a, 2) = 2$ e $(a, 22) = 2$, l'equazione ha 4 soluzioni modulo 92.

Se $a \equiv 11 \pmod{22}$, cioè $(a, 2) = 1$ e $(a, 22) = 11$, l'equazione ha 11 soluzioni modulo 92.

Se infine $a \equiv 0 \pmod{22}$, cioè $(a, 2) = 2$ e $(a, 22) = 22$, l'equazione ha 44 soluzioni modulo 92.

(ii) Risolvendo la seconda equazione e spezzando la prima in una congruenza modulo 4 e una modulo 23 otteniamo

$$\begin{cases} x^a \equiv 1 & \pmod{4} \\ x^a \equiv 1 & \pmod{23} \\ x \equiv 9 & \pmod{23}. \end{cases}$$

Osserviamo che l'insieme dei quadrati in $(\mathbb{Z}/23\mathbb{Z})^*$ coincide con il sottogruppo di ordine 11. Essendo 11 primo, tale sottogruppo ha tutti gli elementi, tranne $\overline{1}$, di ordine 11. Ora, 9 è un quadrato e quindi il suo ordine in $(\mathbb{Z}/23\mathbb{Z})^*$ è 11. Allora se $a \not\equiv 0 \pmod{11}$ il sistema non è risolubile; se invece $a \equiv 0 \pmod{11}$ il sistema è equivalente a

$$\begin{cases} x^a \equiv 1 & \pmod{4} \\ x \equiv 9 & \pmod{23}. \end{cases}$$

L'equazione $x^a \equiv 1 \pmod{4}$ ha come unica soluzione $x \equiv 1 \pmod{4}$ se $a \equiv 1 \pmod{2}$ e ha soluzione $x \equiv \pm 1 \pmod{4}$ se $a \equiv 0 \pmod{2}$. Risolvendo i sistemi corrispondenti si ottiene: se $a \equiv 11 \pmod{22}$ il sistema ha soluzione $x \equiv 9 \pmod{92}$; se, invece, $a \equiv 0 \pmod{22}$ il sistema ha soluzione $x \equiv 9, 55 \pmod{92}$.

93. La prima congruenza ha soluzione se e solo se $a \equiv 0 \pmod{2}$ e in tal caso ha un'unica soluzione modulo 11. Per il Teorema Cinese dei Resti la seconda con-

gruenza è equivalente al sistema

$$\begin{cases} x^2 \equiv a & (\text{mod } 3) \\ x^2 \equiv -a & (\text{mod } 4) \\ x^2 \equiv 0 & (\text{mod } 7). \end{cases}$$

La congruenza $x^2 \equiv 0 \pmod 7$ ha l'unica soluzione $x \equiv 0 \pmod 7$ per ogni valore di a.

La congruenza $x^2 \equiv -a \pmod 4$ ha le due soluzioni $x \equiv 0, 2 \pmod 4$ se $a \equiv 0 \pmod 4$ e non ha invece soluzioni se $a \equiv 2 \pmod 4$, infatti le classi di 1 e 3 sono escluse in quanto possiamo assumere a pari per quanto visto sopra.

Infine $x^2 \equiv a \pmod 3$ ha l'unica soluzione $x \equiv 0 \pmod 3$ se $a \equiv 0 \pmod 3$, le due soluzioni $x \equiv \pm 1 \pmod 3$ se $a \equiv 1 \pmod 3$ e nessuna soluzione se $a \equiv 2 \pmod 3$.

Concludendo abbiamo i seguenti casi.

(1) Se $a \equiv 1 \pmod 2$ la prima equazione, e quindi il sistema, non ha soluzione.

(2) Se $a \equiv 0 \pmod 4$ e $a \equiv 0 \pmod 3$, cioè $a \equiv 0 \pmod{12}$, l'equazione $x^2 \equiv 7a \pmod{84}$ ha due soluzioni modulo 84 e $2x \equiv a \pmod{22}$ ha un'unica soluzione modulo 11, quindi il sistema ha due soluzioni modulo $84 \cdot 11 = 924$.

(3) Se, infine, $a \equiv 0 \pmod 4$ e $a \equiv 1 \pmod 3$, cioè $a \equiv 4 \pmod{12}$, l'equazione $x^2 \equiv 7a \pmod{84}$ ha 4 soluzioni modulo 84 e $2x \equiv a \pmod{22}$ ha un'unica soluzione modulo 11, quindi il sistema ha 4 soluzioni modulo $84 \cdot 11 = 924$.

Nei rimanenti casi il sistema non ha soluzione perché non ha soluzione la seconda congruenza.

94. Analizziamo la prima congruenza: osserviamo che non ha soluzione se a è pari, quindi necessariamente $a \equiv 1 \pmod 2$. In tal caso $a^x \equiv 1 \pmod 8$ se x è pari e $a^x \equiv a \pmod 8$ se x è dispari, quindi la congruenza è risolubile se e solo se $a \equiv 3 \pmod 8$ e in tal caso la soluzione è $x \equiv 1 \pmod 2$.

Sia quindi $a = 3 + 8b$. La seconda congruenza diventa $x^{6+16b} \equiv 4 \pmod 9$. Osserviamo che le soluzioni di questa congruenza vanno cercate in $(\mathbb{Z}/9\mathbb{Z})^*$, infatti una soluzione ha come potenza la classe di 4 che è invertibile in $\mathbb{Z}/9\mathbb{Z}$. In particolare $x^6 \equiv 1 \pmod 9$, e l'equazione diventa $x^{4b} \equiv 4 \pmod 9$.

Usando di nuovo il fatto che le seste potenze sono 1 in $(\mathbb{Z}/9\mathbb{Z})^*$, si ha che se $b \equiv 0 \pmod 3$ l'equazione non ha soluzioni, se $b \equiv 1 \pmod 3$ l'equazione è equivalente a $x^4 \equiv 4 \pmod 9$ e ha come soluzione $x \equiv \pm 4 \pmod 9$ e se, infine, $b \equiv 2 \pmod 3$ l'equazione è equivalente a $x^2 \equiv 4 \pmod 9$ e ha come soluzione $x \equiv \pm 2 \pmod 9$.

Concludendo abbiamo i seguenti casi.

(1) Se $a \equiv 11 \pmod{24}$ la prima equazione ha soluzione $x \equiv 1 \pmod 2$ e la seconda $x \equiv \pm 4 \pmod 9$, e quindi il sistema ha soluzione $x \equiv 5, 13 \pmod{18}$.

(2) Se $a \equiv 19 \pmod{24}$ la prima equazione ha soluzione $x \equiv 1 \pmod 2$ e la seconda $x \equiv \pm 2 \pmod 9$, e quindi il sistema ha soluzione $x \equiv 7, 11 \pmod{18}$.

Infine, se $a \not\equiv 11, 19 \pmod{24}$ una delle due equazioni, e quindi il sistema, non ha soluzione.

95. Il problema è equivalente a contare il numero di soluzioni modulo 100 dell'equazione $xy \equiv 0 \pmod{100}$. Quest'ultima equazione, per il Teorema Cinese

dei Resti, è equivalente al sistema

$$\begin{cases} xy \equiv 0 \pmod 4 \\ xy \equiv 0 \pmod{25}. \end{cases}$$

Consideriamo, in generale, l'equazione $xy \equiv 0 \pmod{p^2}$, dove p è un numero primo, ossia $p^2 \mid xy$. Essa ha soluzione quando uno dei due fattori è divisibile per p^2, cioè congruo a zero modulo p^2, e l'altro è qualsiasi, oppure quando entrambi sono divisibili per p.

Le coppie $(x, \overline{0})$ sono p^2, così come le coppie $(\overline{0}, y)$. Poiché però $(\overline{0}, \overline{0})$ è rappresentabile in entrambe le forme, il numero totale di coppie di questo tipo è $2p^2 - 1$.

Le coppie di numeri divisibili per p ma non per p^2 sono rappresentate da classi di resto della forma (pa, pb) con $1 \leq a, b \leq p-1$, e quindi sono $(p-1)^2$. In totale, le coppie cercate sono quindi $2p^2 - 1 + (p-1)^2 = 3p^2 - 2p$.

Sostituendo i valori $p = 2$ e $p = 5$, si ottengono rispettivamente i valori 8 e 65. Ancora per il Teorema Cinese dei Resti, il numero di soluzioni dell'equazione $xy \equiv 0 \pmod{100}$ è quindi uguale a $8 \cdot 65 = 520$.

96. La prima congruenza del sistema è risolubile se e solo se $6 = (6, 72) \mid 4a$, ossia se e solo se $3 \mid a$. In tal caso, ponendo $a = 3b$, si può semplificare la congruenza per 6 ottenendo $x \equiv 2b \pmod{12}$.

La seconda congruenza è risolubile, poiché $1 = (5, 39) \mid 2$, e la soluzione è $x \equiv 16 \pmod{39}$.

Poiché però $(12, 39) = 3$, il sistema ha soluzione se e solo se le soluzioni delle due congruenze sono le stesse modulo 3, ossia $2b \equiv 16 \pmod 3$ e dunque $b \equiv 2 \pmod 3$. In questo caso, esiste una ed una sola soluzione modulo il minimo comune multiplo dei moduli delle due equazioni, cioè modulo 156.

In conclusione, esiste una soluzione modulo 156 se $a \equiv 6 \pmod 9$ e nessuna soluzione altrimenti.

97. Per risolvere la prima equazione bisogna cercare l'ordine di 8 nel gruppo moltiplicativo $(\mathbb{Z}/27\mathbb{Z})^*$. Esso è un divisore di $\phi(27) = 18$. Si ha $8^2 \equiv 10$, $8^3 \equiv -1$, $8^6 \equiv 1 \pmod{27}$, per cui l'ordine cercato è 6. Poiché $8^3 \equiv -1 \pmod{27}$, le soluzioni della prima equazione sono le stesse di $x^2 - 1 \equiv 3 \pmod 6$. Risolvendo separatamente modulo 2 e modulo 3 si ottiene

$$\begin{cases} x \equiv 0 \pmod 2 \\ x \equiv \pm 1 \pmod 3. \end{cases}$$

Similmente, la seconda equazione è equivalente al sistema

$$\begin{cases} x^{22} + 2x \equiv 8 \pmod 4 \\ x^{22} + 2x \equiv 8 \pmod{11}. \end{cases}$$

La prima equazione di quest'ultimo sistema si può riscrivere come $x^{22} + 2x \equiv 0 \pmod 4$. Poiché $x^{22} \equiv x \pmod 2$, ne segue che x deve essere pari. D'altra parte,

se x è pari, allora sia x^{22} che $2x$ sono divisibili per 4, quindi si ha una soluzione. Dunque la soluzione della prima equazione è $x \equiv 0 \pmod 2$.

Per verifica diretta, si vede che $x \equiv 0 \pmod{11}$ non è soluzione della seconda equazione. D'altra parte, se $x \not\equiv 0 \pmod{11}$ è una soluzione, allora, per il Piccolo Teorema di Fermat, $x^{10} \equiv x^{20} \equiv 1 \pmod{11}$, e dunque le soluzioni della seconda equazione sono le stesse di quelle dell'equazione $x^2 + 2x \equiv 8 \pmod{11}$.

Visto che questa equazione di secondo grado ha le soluzioni $2, -4$ in $\mathbb{Z}$, essa avrà le loro classi come soluzioni modulo 11 e non altre essendo 11 primo.

Infine, poiché le soluzioni delle due equazioni del sistema originario sono le stesse modulo 2, esso diventa

$$\begin{cases} x \equiv 0 & \pmod 2 \\ x \equiv \pm 1 & \pmod 3 \\ x \equiv 2, -4 & \pmod{11}. \end{cases}$$

Questo dà origine a 4 soluzioni modulo $2 \cdot 3 \cdot 11 = 66$. Con semplici calcoli si trova che le soluzioni sono $x \equiv 2, 40, 46, 62 \pmod{66}$.

98. Calcolando le prime potenze di 3 modulo 5, si osserva che $3^3 \equiv 2 \pmod 5$ e che l'ordine moltiplicativo di 3 modulo 5 è 4. Pertanto la prima equazione si può riscrivere come $3^x \equiv 3^{3a} \pmod 5$ ed ha per soluzione $x \equiv 3a \equiv -a \pmod 4$.

La seconda equazione si può scindere in due equazioni, una modulo 3 ed una modulo 8. L'equazione modulo 3 ha sempre una e una sola soluzione modulo 3, dal momento che $x^3 \equiv x \pmod 3$ per ogni x. Per l'equazione modulo 8, distinguiamo due casi.

(1) Se a è pari, allora anche x deve essere pari; ma per ogni x pari si ha $x^3 \equiv 0 \pmod 8$; quindi si ha una soluzione modulo 2, cioè 4 soluzioni modulo 8, se $a \equiv 6 \pmod 8$, e nessuna soluzione altrimenti.

(2) Se a è dispari, allora anche x deve essere dispari; in questo caso, osservando che $x^2 \equiv 1$ e $x^3 \equiv x \pmod 8$ si ha sempre una e una sola soluzione modulo 8.

Il sistema quindi non ha nessuna soluzione per $a \equiv 0, 2, 4 \pmod 8$. Negli altri casi, per verificare la risolubilità del sistema bisogna ora controllare che la soluzione dell'equazione modulo 4 e quella modulo 2 od 8 siano coerenti.

Se a è pari, e dunque $a \equiv 6 \pmod 8$, l'equazione modulo 4 ha per soluzione $x \equiv 2 \pmod 4$, coerente con la soluzione $x \equiv 0 \pmod 2$. In questo caso quindi c'è una sola soluzione modulo 12.

Se a è dispari, le equazioni sono ancora coerenti, infatti abbiamo osservato che la soluzione dell'equazione modulo 8 è $x \equiv a + 2$ e $a + 2 \equiv -a \pmod 4$ per a dispari. Pertanto c'è una sola soluzione modulo 24.

99. La prima congruenza ha soluzione se e solo se $\overline{3}$ appartiene al sottogruppo generato da $\overline{a}$ in $(\mathbb{Z}/7\mathbb{Z})^*$, ossia se e solo se il sottogruppo generato da $\overline{3}$ è contenuto nel sottogruppo generato da $\overline{a}$. Poiché $\overline{3}$ è un generatore del gruppo $(\mathbb{Z}/7\mathbb{Z})^*$, in quanto si verifica che il suo ordine è 6, questo significa che la prima congruenza ha soluzione se e solo se anche $\overline{a}$ è un generatore del gruppo.

Dato che $\overline{3}$ è un generatore, tutti gli altri generatori sono della forma $\overline{3}^i$ con $0 \le i < 6$ e $(i, 6) = 1$, ossia essi sono $\overline{3}$ e $\overline{3}^5 = \overline{3}^{-1} = \overline{5}$. Poiché un generatore

ha ordine 6 e $3^1 \equiv 3, 5^5 \equiv 3 \pmod 7$, le soluzioni della prima congruenza sono: per $a \equiv 3 \pmod 7$, si ha $x \equiv 1 \pmod 6$; mentre per $a \equiv 5 \pmod 7$, si ha $x \equiv 5 \pmod 6$.

Per quanto riguarda la seconda congruenza del sistema, si osservi che il quadrato di un numero pari è divisibile per 4, mentre il quadrato di un numero dispari è sempre congruo a 1 modulo 8. Pur avendo la seconda congruenza soluzioni anche per $a \equiv 0, 4 \pmod 8$, queste soluzioni si possono trascurare, in quanto danno necessariamente $x \equiv 0 \pmod 2$, che è incompatibile con le soluzioni della prima congruenza.

Basta quindi considerare il caso $a \equiv 1 \pmod 8$, che ha per soluzione $x \equiv 1 \pmod 2$ ed è quindi già garantito dalla soluzione della prima congruenza. Concludendo, se $a \equiv 3 \pmod 7$, $a \equiv 1 \pmod 8$, cioè $a \equiv 17 \pmod{56}$, la soluzione è $x \equiv 1 \pmod 6$; se, invece, $a \equiv 5 \pmod 7$, $a \equiv 1 \pmod 8$, cioè $a \equiv 33 \pmod{56}$, la soluzione è $x \equiv 5 \pmod 6$.

Per altri valori di a non ci sono soluzioni.

100. La prima equazione ha soluzione se e solo se $a \not\equiv 0 \pmod 5$. Se $a \equiv 1 \pmod 5$, le soluzioni sono tutti i numeri interi; se $a \equiv -1 \pmod 5$, cioè se l'ordine di a in $(\mathbb{Z}/5\mathbb{Z})^*$ è 2, la soluzione è $x \equiv 0 \pmod 2$; se $a \equiv 2, 3 \pmod 5$, e quindi se e solo se l'ordine di a in $(\mathbb{Z}/5\mathbb{Z})^*$ è 4, la soluzione è $x \equiv 0 \pmod 4$.

La seconda equazione ha soluzione se e solo se $(a, 8) \mid 2$, cioè se e solo se $a \not\equiv 0 \pmod 4$. Se a è dispari, allora $a^{-1} \equiv a \pmod 8$, e dunque la soluzione è $x \equiv 2a \pmod 8$, inoltre si osservi che in questo caso $2a \equiv \pm 2 \pmod 8$. Se $a \equiv 2 \pmod 4$, cioè $a = 2b$ con b dispari, la soluzione è $x \equiv b \pmod 4$.

Confrontando le soluzioni delle due equazioni, concludiamo quanto segue.

Nel caso a dispari: per $a \equiv 2, 3 \pmod 5$ non ci sono soluzioni comuni, mentre per $a \equiv \pm 1 \pmod 5$, cioè $a \equiv \pm 1 \pmod{10}$, le soluzioni della seconda equazione sono anche soluzioni della prima equazione e quindi il sistema ha per soluzioni esattamente quelle della seconda equazione.

Se, invece, $a \equiv 2 \pmod 4$: non ci sono soluzioni comuni alle due equazioni eccetto quando $a \equiv 1 \pmod 5$; in questo caso, e cioè $a \equiv 6 \pmod{20}$, le soluzioni della seconda equazione sono anche soluzioni della prima equazione e quindi sono le soluzioni del sistema.

101. Per verifica diretta si vede che l'ordine di 2 nel gruppo moltiplicativo $(\mathbb{Z}/13\mathbb{Z})^*$ è 12 e che $5 \equiv 2^9 \pmod{13}$. La prima equazione diventa quindi $2^{9(x^2-1)} \equiv 2^a \pmod{13}$ che, per quanto appena visto, è equivalente a $9(x^2 - 1) \equiv a \pmod{12}$. Da quest'ultima equazione ricaviamo che necessariamente $3 \mid a$ per avere soluzioni.

Poniamo dunque $a = 3b$; dividendo per i fattori comuni si ottiene $3(x^2 - 1) \equiv b \pmod 4$, ossia $x^2 \equiv 1 - b \pmod 4$. I quadrati dei numeri interi modulo 4 possono essere soltanto 0, nel caso x pari, e 1, nel caso x dispari. Pertanto l'ultima equazione ha soluzione se e solo se $b \equiv 0, 1 \pmod 4$, con soluzione rispettivamente $x \equiv 1, 0 \pmod 2$.

La seconda equazione equivale a $64 = 2^6 \mid x^3$ e quindi a $2^2 | x$, ossia $x \equiv 0 \pmod 4$, e quindi in particolare, $x \equiv 0 \pmod 2$. Affinché il sistema sia risolubile

è pertanto necessario e sufficiente che $b \equiv 1 \pmod 4$, ossia $a \equiv 3 \pmod{12}$, e in questo caso la soluzione è $x \equiv 0 \pmod 4$.

102. Per il Teorema Cinese dei Resti, la prima equazione è equivalente al sistema

$$\begin{cases} a^x \equiv 1 & (\text{mod } 2) \\ a^x \equiv 4 & (\text{mod } 7). \end{cases}$$

La prima di queste due equazioni è risolubile se e solo se $a \equiv 1 \pmod 2$; in questo caso, le soluzioni sono tutti gli x interi.

Per quanto riguarda la seconda equazione del sistema ora ottenuto, osserviamo che essa non è risolubile nei seguenti casi. Se $a \equiv 0 \pmod 7$, in quanto $a^x \equiv 0 \pmod 7$ per ogni x. Se $a \equiv 1 \pmod 7$, in quanto $a^x \equiv 1 \pmod 7$ per ogni x. Se $a \equiv -1 \pmod 7$, in quanto $a^x \equiv \pm 1 \pmod 7$ per ogni x.

Invece, l'equazione è risolubile negli altri casi e, in particolare, le soluzioni sono come di seguito indicato.

Se $a \equiv 2 \pmod 7$: visto che $2^2 \equiv 4 \pmod 7$ e che l'ordine di 2 modulo 7 è uguale a 3, la soluzione è $x \equiv 2 \pmod 3$.

Se $a \equiv 3 \pmod 7$: visto che $3^4 \equiv 4 \pmod 7$ e l'ordine di 3 modulo 7 è 6, la soluzione è $x \equiv 4 \pmod 6$; equivalentemente, $x \equiv 0 \pmod 2$ e $x \equiv 1 \pmod 3$.

Se $a \equiv 4 \pmod 7$: visto che $4^1 \equiv 4 \pmod 7$ e l'ordine di 4 modulo 7 è 3, la soluzione è $x \equiv 1 \pmod 3$.

Se $a \equiv 5 \pmod 7$: visto che $5^2 \equiv 4 \pmod 7$ e l'ordine di 5 modulo 7 è 6, la soluzione è $x \equiv 2 \pmod 6$; equivalentemente, $x \equiv 0 \pmod 2$ e $x \equiv 2 \pmod 3$.

Consideriamo ora l'equazione $x^a \equiv 1 \pmod 9$. Essa è soddisfatta per le coppie di interi (x, a) tali che $(x, 9) = 1$, ossia $(x, 3) = 1$ e a è multiplo dell'ordine moltiplicativo di x modulo 9.

Come abbiamo visto, la prima equazione del sistema originario è risolubile solo se a è dispari, quindi le soluzioni possono essere solo gli x che hanno un ordine moltiplicativo modulo 9 dispari e cioè $x \equiv 1, 4, 7 \pmod 9$. Più precisamente, poiché $\overline{1}$ ha ordine 1 mentre $\overline{4}$ e $\overline{7}$ hanno ordine 3, $x \equiv 1 \pmod 9$ è soluzione per ogni a, mentre $x \equiv 4, 7 \pmod 9$ sono soluzioni solo se $3 \mid a$.

In ogni caso le soluzioni possono essere solo numeri congrui a 1 modulo 3, quindi, per avere la compatibilità con la congruenza modulo 7, è necessario che $a \equiv 3, 4 \pmod 7$.

Questa condizione è anche sufficiente, perché per ogni a di questo tipo la congruenza modulo 9 ha per soluzione almeno $x \equiv 1 \pmod 9$, che è compatibile con le possibili soluzioni della congruenza modulo 7.

Riassumendo, il sistema è risolubile se e solo se $a \equiv 1 \pmod 2$ e $a \equiv 3, 4 \pmod 7$, ossia se e solo se $a \equiv 3, 11 \pmod{14}$.

103. (i) Consideriamo la successione periodica delle classi di congruenza delle potenze di 3 modulo 10:

$$3^1 = 3 \equiv 3, \quad 3^2 = 9 \equiv 9, \quad 3^3 = 27 \equiv 7, \quad 3^4 = 81 \equiv 1.$$

Quindi la successione è periodica di periodo 4, e la soluzione dell'equazione è $x \equiv 3 \pmod 4$.

(ii) Poiché le potenze di 3 sono tutte dispari e 10 è pari, ci può essere soluzione solo se $4+x$ è dispari, ossia solo se x è dispari. D'altra parte, per quanto visto sopra, le potenze di 3 dipendono solo dalla classe di congruenza dell'esponente modulo 4. Distinguiamo quindi due casi.

(1) Se $x \equiv 1 \pmod 4$ allora $3^x \equiv 3 \pmod{10}$ e l'equazione si riduce a $3 \equiv 4+x \pmod{10}$, ossia $x \equiv 9 \pmod{10}$. Combinando con la congruenza modulo 4 si ottiene $x \equiv 9 \pmod{20}$.

(2) Se, invece, $x \equiv 3 \pmod 4$ allora $3^x \equiv 7 \pmod{10}$ e l'equazione da risolvere si riduce a $7 \equiv 4+x \pmod{10}$, ossia $x \equiv 3 \pmod{10}$. Combinando con la congruenza modulo 4 si ottiene $x \equiv 3 \pmod{20}$.

104. La prima equazione non può, evidentemente, avere una soluzione con $x \equiv 0 \pmod 7$. Se $x \not\equiv 0 \pmod 7$, gli esponenti n tali che $x^n \equiv 1 \pmod 7$ sono tutti e soli i multipli dell'ordine della classe di x in $(\mathbb{Z}/7\mathbb{Z})^*$. Questo ordine è sempre un divisore dell'ordine del gruppo $(\mathbb{Z}/7\mathbb{Z})^*$, cioè 6. Notando però che l'esponente $2x+1$ è dispari, l'ordine di x deve essere dispari, e quindi le uniche possibilità sono 1, e in tal caso $x \equiv 1 \pmod 7$, o 3 e allora $x \equiv 2$ o $x \equiv 4 \pmod 7$.

Ogni $x \equiv 1 \pmod 7$ risolve la prima equazione, poiché $1^{2x+1} \equiv 1 \pmod 7$. Se $x \equiv 2, 4 \pmod 7$, allora l'esponente deve essere multiplo di 3, quindi si deve avere $2x+1 \equiv 0 \pmod 3$, ossia $x \equiv 1 \pmod 3$.

La seconda equazione è risolubile perché $(4, 15) \mid 7$ e ha come soluzione $x \equiv 13 \pmod{15}$, che è equivalente al sistema delle due equazioni $x \equiv 1 \pmod 3$, $x \equiv 3 \pmod 5$.

Notiamo che la congruenza modulo 3 della seconda equazione è, in ogni caso, compatibile con le soluzione della prima equazione; il sistema è quindi risolubile. Le soluzioni del sistema originario corrispondono alle soluzioni del sistema

$$\begin{cases} x \equiv 1, 2, 4 & \pmod 7 \\ x \equiv 1 & \pmod 3 \\ x \equiv 3 & \pmod 5. \end{cases}$$

Con facili calcoli, si ottengono le soluzioni $x \equiv 43, 58, 88 \pmod{105}$.

105. (i) Il sistema di equazioni

$$\begin{cases} x \equiv 1 & \pmod 1 \\ x \equiv 1 & \pmod 2 \\ \quad \vdots & \\ x \equiv 1 & \pmod{10} \end{cases}$$

è certamente risolubile, visto che ha la soluzione $x = 1$. Ora, se un sistema di equazioni lineari è risolubile, la soluzione è una classe di congruenza modulo il minimo comune multiplo dei moduli delle singole equazioni. Detto M il minimo comune multiplo dei numeri fra 1 e 10, cioè $M = 2^3 \cdot 3^2 \cdot 5 \cdot 7$, la soluzione è $x \equiv 1 \pmod M$. All'interno dei numeri tra 0 e k, il numero di interi che soddisfano questa congruenza è $\lceil k/M \rceil$.

(ii) Se $x \equiv -1 \pmod{n}$ allora $n \mid x+1$, per ogni intero positivo n. Ma l'unico numero intero che è divisibile per tutti i numeri è 0, quindi c'è l'unica soluzione $x+1=0$, cioè $x=-1$.

(iii) Se $x \equiv n \pmod{2n}$ allora $x = n+2hn = n(2h+1)$ per qualche intero h; in particolare, x è divisibile per ogni n. Come nel punto precedente, questo implica che $x=0$; ma nemmeno 0 è una soluzione, in quanto, prendendo, ad esempio, $n=1$, si ha $0 \not\equiv 1 \pmod{2}$. Quindi non c'è alcuna soluzione.

106. La coppia (x,n) è soluzione della congruenza se e solo se esiste un intero t tale che $x^n = 39 + 10xt$. In quest'ultima equazione x divide sia x^n che $10xt$, quindi una condizione necessaria è che x divida 39. Esaminiamo i vari divisori di 39.

Se $x=1$, $1^n \equiv 39 \pmod{10}$ ovviamente non ha soluzione.

Se $x=3$, l'equazione $3^n \equiv 39 \pmod{30}$ equivale al sistema

$$\begin{cases} 3^n \equiv 0 \pmod{3} \\ 3^n \equiv 9 \pmod{10}. \end{cases}$$

La prima equazione è verificata per ogni $n \geq 1$ mentre la seconda è verificata per $n \equiv 2 \pmod{4}$ in quanto 3 ha ordine 4 in $(\mathbb{Z}/10\mathbb{Z})^*$.

Se $x=13$, analogamente otteniamo il sistema

$$\begin{cases} 13^n \equiv 0 \pmod{13} \\ 3^n \equiv 9 \pmod{10} \end{cases}$$

che ha ancora come soluzione $n \equiv 2 \pmod{4}$.

Se $x=39$, il sistema diventa

$$\begin{cases} 39^n \equiv 0 \pmod{39} \\ 9^n \equiv 9 \pmod{10} \end{cases}$$

che questa volta ha per soluzione $n \equiv 1 \pmod{2}$.

107. Per il Teorema Cinese dei Resti, la congruenza è equivalente al sistema

$$\begin{cases} x^{5n} \equiv 1 \pmod{5} \\ x^{5n} \equiv 1 \pmod{11}. \end{cases}$$

Consideriamo la prima equazione. Per il Piccolo Teorema di Fermat, essa è equivalente a $x^n \equiv 1 \pmod{5}$. Gli elementi x che soddisfano questa equazione sono gli elementi di $(\mathbb{Z}/5\mathbb{Z})^*$ il cui ordine moltiplicativo è un divisore di n. Gli ordini degli elementi x di $(\mathbb{Z}/5\mathbb{Z})^*$ sono

$$1, \text{ se } x = \overline{1}; \quad 2, \text{ se } x = \overline{-1}; \quad 4, \text{ se } x = \overline{\pm 2}.$$

Quindi, per $n \equiv 0 \pmod{4}$ ci sono 4 soluzioni in quanto n è multiplo dell'ordine di tutti gli elementi. Per $n \equiv 2 \pmod{4}$ ci sono due soluzioni visto che n è multiplo dell'ordine dei soli elementi $\overline{\pm 1}$. Infine, per n dispari c'è una sola soluzione perché n è multiplo solo dell'ordine di $\overline{1}$.

Consideriamo ora la seconda equazione. Analogamente a quanto appena visto, gli elementi che soddisfano quest'equazione sono gli elementi di $(\mathbb{Z}/11\mathbb{Z})^*$ il cui ordine è un divisore di $5n$. Poiché il gruppo $(\mathbb{Z}/11\mathbb{Z})^*$ è ciclico, gli ordini dei suoi elementi sono 1, 2, 5 e 10 e il numero di elementi di ordine d è uguale a $\phi(d)$. Quindi c'è un elemento di ordine 1, un elemento di ordine 2, e ci sono 4 elementi di ordine 5 e 4 elementi di ordine 10.

⟦Si può facilmente verificare che $\overline{1}$ è l'unico elemento di ordine 1, $\overline{-1}$ è l'unico elemento di ordine 2, che $\overline{3}, \overline{4}, \overline{5}, \overline{9}$ sono gli elementi di ordine 5 e che $\overline{2}, \overline{6}, \overline{7}, \overline{8}$ sono gli elementi di ordine 10.⟧

Come prima, un elemento soddisfa l'equazione se e solo se il suo ordine è un divisore di $5n$. Se n è pari, allora $5n$ è un multiplo di 10, e quindi tutti i 10 elementi di $(\mathbb{Z}/11\mathbb{Z})^*$ sono soluzioni; se, invece, n è dispari, allora le soluzioni sono solo gli elementi il cui ordine è divisore di 5: l'elemento $\overline{1}$ ed i quattro elementi di ordine 5, in tutto 5 soluzioni.

Possiamo riassumere quanto visto come segue.

Se $n \equiv 0 \pmod 4$ ci sono 4 soluzioni modulo 5 e 10 soluzioni modulo 11, per un totale di 40 soluzioni.

Se $n \equiv 2 \pmod 4$ ci sono 2 soluzioni modulo 5 e 10 soluzioni modulo 11, per un totale di 20 soluzioni

Se, infine, n è dispari c'è una soluzione modulo 5 e ci sono 5 soluzioni modulo 11, per un totale di 5 soluzioni.

108. (i) Sia $f(x)$ il polinomio quadratico $x^2 - x + 43$, la congruenza da risolvere è equivalente al sistema $f(x) \equiv 0 \pmod 5$ e $f(x) \equiv 0 \pmod{11}$ per il Teorema Cinese dei Resti. Visto che 5 e 11 sono primi dispari possiamo usare la formula risolutiva delle equazioni di secondo grado in entrambi i casi.

Per 5, $f(x)$ ha discriminante 3^2 e quindi $f(x)$ ha le due soluzioni 2 e -1 modulo 5. Per il modulo 11 il discriminante è 4^2 e le soluzioni sono -3 e 4.

Osserviamo ora che $x_1 = 11$ e $x_2 = -10$ risolvono rispettivamente i sistemi $x_1 \equiv 1 \pmod 5$, $x_1 \equiv 0 \pmod{11}$ e $x_2 \equiv 0 \pmod 5$, $x_2 \equiv 1 \pmod{11}$. Allora l'equazione originale ha le 4 soluzioni

$$\begin{aligned} -3 &\equiv 2x_1 - 3x_2 \pmod{55} \\ 19 &\equiv -x_1 - 3x_2 \pmod{55} \\ -18 &\equiv 2x_1 + 4x_2 \pmod{55} \\ 4 &\equiv -x_1 + 4x_2 \pmod{55}. \end{aligned}$$

(ii) Per risolvere il sistema dobbiamo confrontare il valore modulo 5 delle classi soluzione della prima equazione, con la seconda. I valori modulo 5 delle soluzioni della prima equazione sono 2 e -1. Nel primo caso deve quindi essere $2^{11^4} \equiv 2^a \pmod 5$. Poiché 2 ha ordine moltiplicativo 4 in $(\mathbb{Z}/5\mathbb{Z})^*$ e $11^4 \equiv (-1)^4 = 1 \pmod 4$, l'equazione diventa $2 \equiv 2^a \pmod 5$ ed è risolubile se e solo $a \equiv 1 \pmod 4$. Quindi le classi -3 e -18 modulo 55 risolvono il sistema se e solo se $a \equiv 1 \pmod 4$.

Nel secondo caso abbiamo invece $(-1)^{11^4} = -1 \equiv (-1)^a \pmod 5$ e questa equazione è risolubile se e solo se $a \equiv 1 \pmod 2$. Quindi le classi 19 e 4 modulo 55 risolvono il sistema se e solo se $a \equiv 1 \pmod 2$.

Concludiamo allora che, se $a \equiv 0 \pmod 2$ il sistema non ha soluzione. Se $a \equiv 1 \pmod 2$ il sistema è risolubile. Più precisamente, dividendo la classe $a \equiv 1 \pmod 2$ nelle classi $a \equiv -1 \pmod 4$ e $a \equiv +1 \pmod 4$ abbiamo: se $a \equiv -1 \pmod 4$ le soluzioni sono le classi di 19 e 4 modulo 55, se invece $a \equiv 1 \pmod 4$ tutte le classi che risolvono la prima equazione risolvono anche la seconda, quindi le soluzioni sono le classi di $-3, -18, 19, 4$ modulo 55.

109. (i) L'equazione è equivalente al sistema di $x^2 + 2x + 5 \equiv 0 \pmod 5$ e $x^2 + 2x + 5 \equiv 0 \pmod{13}$. Poiché entrambi i moduli sono primi, ognuna delle due equazioni ha al più due radici. La prima ha chiaramente soluzioni 0 e -2 modulo 5. Per la seconda, usando la formula risolutiva delle equazioni di secondo grado, otteniamo che il discriminante è $-4 = 3^2 \pmod{13}$ e quindi le soluzioni sono 2 e -4 modulo 13. Le soluzioni dell'equazione assegnata sono quindi le soluzioni dei 4 sistemi

$$\begin{cases} x \equiv 0 \pmod 5 \\ x \equiv 2 \pmod{13}, \end{cases} \qquad \begin{cases} x \equiv -2 \pmod 5 \\ x \equiv 2 \pmod{13}, \end{cases}$$
$$\begin{cases} x \equiv 0 \pmod 5 \\ x \equiv -4 \pmod{13}, \end{cases} \qquad \begin{cases} x \equiv -2 \pmod 5 \\ x \equiv -4 \pmod{13}. \end{cases}$$

È semplice verificare che i due sistemi

$$\begin{cases} x \equiv 1 \pmod 5 \\ x \equiv 0 \pmod{13}, \end{cases} \qquad \begin{cases} x \equiv 0 \pmod 5 \\ x \equiv 1 \pmod{13} \end{cases}$$

hanno soluzioni rispettivamente $x_1 \equiv 26 \pmod{65}$ e $x_2 \equiv -25 \pmod{65}$; ne segue che le soluzioni dei 4 sistemi sopra, e quindi dell'equazione assegnata, sono: $0 \cdot x_1 + 2 \cdot x_2 \equiv 15$, $-2 \cdot x_1 + 2 \cdot x_2 \equiv -37$, $0 \cdot x_1 - 4 \cdot x_2 \equiv -30$ e $-2 \cdot x_1 - 4 \cdot x_2 \equiv -17 \pmod{65}$.

(ii) Ponendo $y = 3^x$ vediamo che y è soluzione dell'equazione del punto precedente. In particolare, visto che $3^x \neq 0$ modulo 5 e che le potenze di 3 modulo 13 sono 1, 3 e -4 abbiamo che deve necessariamente essere $3^x = y \equiv -2 \equiv 3 \pmod 5$ e $3^x = y \equiv -4 \pmod{13}$. La prima è equivalente a $x \equiv 1 \pmod 4$ e la seconda a $x \equiv 2 \pmod 3$. In conclusione le soluzioni richieste sono date dalla classe di resto di 5 modulo 12.

110. La prima congruenza del sistema è equivalente al sistema delle due equazioni $x^2 + 2x + 2 \equiv 0 \pmod 2$ e $x^2 + 2x + 2 \equiv 0 \pmod 5$ per il Teorema Cinese dei Resti. La prima di queste è chiaramente equivalente a $x \equiv 0 \pmod 2$, mentre la seconda ha discriminante $\Delta = 1 - 2 = -1 \equiv 2^2 \pmod 5$ e quindi soluzioni $-1 \pm \sqrt{\Delta} = -1 \pm 2$, cioè 1 e 2.

Per la seconda equazione: 7 è primo con 22 e quindi è invertibile, inoltre, il suo inverso è la classe di -3. L'equazione diventa quindi $x \equiv -60 \equiv 6 \pmod{22}$. Da questa si deduce, in particolare, $x \equiv 0 \pmod 2$ che è una delle due equazioni del sistema precedente, per cui ci basta considerare solo quella modulo 5. Dobbiamo

quindi risolvere i due sistemi

$$\begin{cases} x \equiv 1, 2 & (\text{mod } 5) \\ x \equiv 6 & (\text{mod } 22). \end{cases}$$

Il primo ha soluzione 6 e il secondo -38 modulo 110.

111. Spezziamo la prima congruenza in una congruenza modulo 4 e una modulo 3 e otteniamo

$$\begin{cases} ax \equiv 2 & (\text{mod } 4) \\ ax \equiv 2 & (\text{mod } 3) \\ 9x \equiv a^2 + 2a - 3 & (\text{mod } 81). \end{cases}$$

Analizziamo il sottosistema formato dalle ultime due equazioni che hanno entrambe modulo una potenza di 3. La congruenza $ax \equiv 2 \pmod 3$ ha soluzione se e solo se $a \equiv 1, 2 \pmod 3$ e, in tal caso, la soluzione è $x \equiv 2a^{-1} \equiv 2a \pmod 3$.

La congruenza $9x \equiv a^2 + 2a - 3 \pmod{81}$ ha soluzione se e solo se $a^2 + 2a - 3 \equiv 0 \pmod 9$. Ora $a^2 + 2a - 3 = (a-1)(a+3) \equiv 0 \pmod 9$ se e solo se $a \equiv 1 \pmod 9$, oppure $a \equiv 3 \pmod 9$, oppure $a \equiv 1 \pmod 3$ e $a \equiv 0 \pmod 3$, ma chiaramente quest'ultima condizione non si verifica mai.

Imponendo entrambe le condizioni di risolubilità di queste due equazioni otteniamo che condizione necessaria per la risolubilità del sistema è $a \equiv 1 \pmod 9$.

Poniamo quindi $a = 1 + 9k$ con $k \in \mathbb{Z}$. Si ha $a^2 + 2a - 3 = 9k(4 + 9k)$ e il sottosistema diventa

$$\begin{cases} x \equiv 2 & (\text{mod } 3) \\ x \equiv 4k & (\text{mod } 9). \end{cases}$$

Questo sistema è risolubile se e solo se le due equazioni sono compatibili, cioè se $4k \equiv 2 \pmod 3$. Abbiamo, quindi, risolubilità se e solo se $k \equiv 2 \pmod 3$, cioè per $a \equiv 19 \pmod{27}$ e, in tal caso, la soluzione è unica modulo 9.

La congruenza $ax \equiv 2 \pmod 4$ non ha soluzione per $a \equiv 0 \pmod 4$, ha una soluzione modulo 4 per $a \equiv 1, 3 \pmod 4$ e ha una soluzione modulo 2 per $a \equiv 2 \pmod 4$.

Poiché $(4, 9) = 1$, grazie al Teorema Cinese dei Resti possiamo concludere come segue.

Per $a \equiv 1, 3 \pmod 4$ e $a \equiv 19 \pmod{27}$, cioè per $a \equiv 73, 19 \pmod{108}$, il sistema ha un'unica soluzione modulo 36, e quindi $180/36 = 5$ soluzioni modulo 180.

Per $a \equiv 2 \pmod 4$ e $a \equiv 19 \pmod{27}$, cioè per $a \equiv 46 \pmod{108}$ il sistema ha una soluzione modulo 18 e quindi ha $180/18 = 10$ soluzioni modulo 180.

Infine, per gli altri valori dell'intero a il sistema non ha soluzione.

112. La prima equazione del sistema può essere spezzata, per il Teorema Cinese dei Resti, in

$$\begin{cases} x^{131} \equiv x & (\text{mod } 11) \\ x^{131} \equiv x & (\text{mod } 5). \end{cases}$$

La prima equazione si può scrivere come $x(x^{130}-1) \equiv 0 \pmod{11}$ da cui, essendo 11 primo, si ha $x \equiv 0 \pmod{11}$ oppure $x^{130} \equiv 1 \pmod{11}$. Ricordiamo che per il Piccolo Teorema di Fermat si ha $a^{10} \equiv 1 \pmod{11}$ per ogni $a \in \mathbb{Z}$ tale che $(a, 11) = 1$. Quindi $x^{130} \equiv 1 \pmod{11}$ ha come soluzioni tutti le classi di $(\mathbb{Z}/11\mathbb{Z})^*$. Ne segue che la congruenza $x^{131} \equiv x \pmod{11}$ è verificata per ogni x intero.

Analogamente $x^{131} \equiv x \pmod{5}$ se e solo se $x(x^{130}-1) \equiv 0 \pmod{5}$ e cioè se e solo se $x \equiv 0 \pmod{5}$ oppure $x^{130} \equiv 1 \pmod{5}$. Le soluzioni di $x^{130} \equiv 1 \pmod{5}$ sono da ricercarsi tra le classi di $(\mathbb{Z}/5\mathbb{Z})^*$ che quindi verificano $x^4 \equiv 1 \pmod{5}$. Abbiamo pertanto $x^{130} \equiv (x^4)^{32}x^2 \equiv x^2 \equiv 1 \pmod{5}$ e le soluzioni sono quindi $x \equiv \pm 1 \pmod{5}$. Concludiamo che $x^{131} \equiv x \pmod{5}$ ha per soluzioni $x \equiv 0, \pm 1 \pmod{5}$ e il sistema assegnato è equivalente ai tre sistemi

$$\begin{cases} x \equiv 0 & \pmod{5} \\ x(x^5+1) \equiv 0 & \pmod{125}, \end{cases}$$

$$\begin{cases} x \equiv 1 & \pmod{5} \\ x(x^5+1) \equiv 0 & \pmod{125}, \end{cases}$$

$$\begin{cases} x \equiv -1 & \pmod{5} \\ x(x^5+1) \equiv 0 & \pmod{125}. \end{cases}$$

Se $x \equiv 0 \pmod{5}$ allora $x^5 + 1 \in (\mathbb{Z}/125\mathbb{Z})^*$, quindi il primo sistema ha soluzione $x \equiv 0 \pmod{125}$.

Per $x \equiv 1 \pmod{5}$ sia x che $x^5 + 1$ sono coprimi con 5 e quindi invertibili in $\mathbb{Z}/125\mathbb{Z}$. Ne segue che il loro prodotto non può essere 0 modulo 125, il secondo sistema non ha allora soluzione.

Sia $x \equiv -1 \pmod{5}$, cioè $x = -1+5y$ con $y \in \mathbb{Z}$. Un tale x è invertibile modulo 125 e la seconda equazione è perciò equivalente a $(-1+5y)^5 + 1 \equiv 0 \pmod{125}$. Svolgendo i calcoli otteniamo

$$(-1+5y)^5 + 1 \equiv 5^2 y \equiv 0 \pmod{125}$$

che ha soluzione $y \equiv 0 \pmod{5}$. Abbiamo ricavato che le soluzioni del terzo sistema sono gli interi della forma $x = -1 + 25t$ con $t \in \mathbb{Z}$, cioè la classe $x \equiv -1 \pmod{25}$

Concludiamo, quindi, che le soluzioni del sistema assegnato sono $x \equiv 0 \pmod{125}$ e $x \equiv -1 \pmod{25}$.

113. Usando il Teorema Cinese dei Resti e invertendo 13 modulo 7 e modulo 19 possiamo riscrivere il sistema come

$$\begin{cases} ax \equiv 1 & \pmod{11} \\ ax \equiv 5 & \pmod{7} \\ x \equiv 3 & \pmod{7} \\ x \equiv -1 & \pmod{19}. \end{cases}$$

La prima equazione è risolubile se e solo se $(a, 11) = 1$, cioè $a \not\equiv 0 \pmod{11}$, e in tal caso la soluzione è $x \equiv a^{-1} \pmod{11}$. L' altra condizione per la risolubilità del

sistema è la compatibilità delle due equazioni modulo 7, che in questo caso dà la condizione $3a \equiv 5 \pmod 7$, quindi $a \equiv 4 \pmod 7$. Il sistema è quindi risolubile se e solo se

$$\begin{cases} a \not\equiv 0 & (\text{mod } 11) \\ a \equiv 4 & (\text{mod } 7) \end{cases}$$

che ha soluzione $a \equiv 4, 18, 25, 32, 39, 46, 53, 60, 67, 74 \pmod{77}$. In questo caso, chiamando b un rappresentante della classe di a^{-1} modulo 11, il sistema diventa

$$\begin{cases} x \equiv b & (\text{mod } 11) \\ x \equiv 3 & (\text{mod } 7) \\ x \equiv -1 & (\text{mod } 19) \end{cases}$$

da cui si ricava

$$\begin{cases} x \equiv b & (\text{mod } 11) \\ x \equiv -39 & (\text{mod } 133). \end{cases}$$

L'equazione risolvente di questo sistema è $133t - 11s = b + 39$.

Usando l'Algoritmo di Euclide, è facile trovare che $133(1) - 11(12) = 1$, quindi, moltiplicando per $b + 39$, otteniamo che $t = b + 39$, $s = 12b + 468$ è una soluzione particolare dell'equazione risolvente. La soluzione del nostro sistema è quindi $x \equiv -39 + 133(b + 39) \pmod{133 \cdot 11}$, ossia $x \equiv 759 + 133b \pmod{1463}$ dove $b \equiv a^{-1} \pmod{77}$ e a verifica le condizioni di risolubilità sopra elencate.

114. Studiamo innanzitutto la risolubilità delle singole equazioni.

Nella prima equazione si può ovviamente escludere il caso $x \equiv 0 \pmod 7$. Se $x \not\equiv 0 \pmod 7$, il Piccolo Teorema di Fermat dice che $x^6 \equiv 1 \pmod 7$. Poiché $80 = 13 \cdot 6 + 2$, l'equazione è quindi equivalente a $x^2 \equiv 2 \pmod 7$. Per verifica diretta, questa equazione è risolubile ed ha le soluzioni $x \equiv \pm 3 \pmod 7$.

Dall'uguaglianza $80 = 11 \cdot 7 + 3$ si ha che la seconda equazione si può riscrivere come $3^x \equiv 2 \pmod 7$. Esaminando le potenze di 3 modulo 7, si ottiene che $3^2 \equiv 2 \pmod 7$ e che il loro periodo è uguale a 6. Pertanto la seconda equazione è risolubile e le soluzioni sono $x \equiv 2 \pmod 6$.

La terza equazione è risolubile per ogni a perché $(7, 10) = 1 \mid a$. L'inverso di 7 modulo 10 è 3, quindi la soluzione è $x \equiv 3a \pmod{10}$.

Esaminiamo ora la risolubilità del sistema. Il massimo comun divisore dei moduli delle soluzioni delle ultime due equazioni è 2, quindi bisogna verificare che le soluzioni modulo 2 siano compatibili. La soluzione della seconda equazione implica che $x \equiv 0 \pmod 2$, mentre quella della terza implica $x \equiv a \pmod 2$. La condizione di risolubilità del sistema è quindi $a \equiv 0 \pmod 2$.

Poniamo quindi $a = 2b$ e risolviamo il sistema. La terza equazione si può riscrivere come $x \equiv 6b \pmod{10}$ o più semplicemente, visto che la congruenza modulo 2 è già stata stabilita dalla seconda equazione, come $x \equiv b \pmod 5$. Abbiamo ora tutte equazioni con moduli relativamente primi e, per il Teorema Cinese dei Resti, le soluzioni avranno come modulo il prodotto dei moduli.

Con facili calcoli si trova che le soluzioni sono $10 - 42a$ e $80 - 42a$ modulo 210.

115. Poiché $700 = 2^2 \cdot 5^2 \cdot 7$, la prima equazione, grazie al Teorema Cinese dei Resti, può essere riscritta come il seguente sistema

$$\begin{cases} x^{41} \equiv x & (\text{mod } 4) \\ x^{41} \equiv x & (\text{mod } 25) \\ x^{41} \equiv x & (\text{mod } 7). \end{cases}$$

Osserviamo ora che $x^{41} - x = x \cdot (x^{40} - 1)$ e che $(x, x^{40} - 1) = 1$. Pertanto, per ogni modulo m, le equazioni del sistema possono essere suddivise in due casi: $x \equiv 0 \pmod{m}$ oppure $x^{40} - 1 \equiv 0 \pmod{m}$.

Per $m = 4$ si hanno le soluzioni $x \equiv 0 \pmod 4$ e $(x, 2) = 1$. Infatti se $(x, 2) = 1$ allora $x^{\phi(4)} = x^2 \equiv 1 \pmod 4$, da cui $x^{40} = (x^2)^{20} \equiv 1 \pmod 4$.

Analogamente, per $m = 25$ si hanno le soluzioni $x \equiv 0 \pmod{25}$ e $(x, 5) = 1$. Infatti, se $(x, 5) = 1$ allora $x^{\phi(25)} = x^{20} \equiv 1 \pmod{25}$ e di conseguenza $x^{40} \equiv 1 \pmod{25}$.

Consideriamo infine il caso $m = 7$, come prima si ha la soluzione $x \equiv 0 \pmod 7$. Se invece $(x, 7) = 1$ allora, per il Piccolo Teorema di Fermat $x^6 \equiv 1 \pmod 7$, da cui $x^{36} \equiv 1 \pmod 7$ e quindi l'equazione si semplifica in $x^4 \equiv 1 \pmod 7$. Questa equazione ha per soluzioni tutti gli elementi di $(\mathbb{Z}/7\mathbb{Z})^*$ il cui ordine divide 4; ma siccome tutti gli elementi di questo gruppo hanno ordine che divide 6, si tratta di cercare gli elementi il cui ordine divide $(4, 6) = 2$ ossia le soluzioni di $x^2 \equiv 1 \pmod 7$, che sono $x \equiv \pm 1 \pmod 7$.

Veniamo alla seconda equazione del sistema originario. Modulo 4 si riduce a $x \equiv 1 \pmod 4$. Mentre modulo 25 si riduce a $-5x \equiv 0 \pmod{25}$, che ha per soluzione $x \equiv 0 \pmod 5$. E, infine, modulo 7 si riduce a $3x \equiv -3 \pmod 7$, che ha per soluzione $x \equiv -1 \pmod 7$.

Mettendo insieme i risultati della prima e seconda equazione, abbiamo trasformato il sistema dato nel seguente

$$\begin{cases} x \equiv 1 & (\text{mod } 4) \\ x \equiv 0 & (\text{mod } 25) \\ x \equiv -1 & (\text{mod } 7). \end{cases}$$

Con qualche calcolo, si trova che la soluzione di questo sistema è $x \equiv 125 \pmod{700}$.

116. L'equazione può essere risolubile solo se $(x, 27) = 1$, visto che x deve essere invertibile in $\mathbb{Z}/27\mathbb{Z}$, e, in tal caso, si deve avere che l'esponente $x + 1$ è congruo a 0 modulo k, dove k è l'ordine di x in $(\mathbb{Z}/27\mathbb{Z})^*$.

Poiché $\phi(27) = 18$, l'ordine di ogni elemento di $(\mathbb{Z}/27\mathbb{Z})^*$ è un divisore di 18.

Se $x + 1 \equiv 0 \pmod{18}$, ossia se $x \equiv -1 \pmod{18}$, si ha automaticamente che x non è divisibile per 3, quindi, per il Teorema di Eulero, $x^{x+1} \equiv 1 \pmod{27}$. Quindi $x \equiv -1 \pmod{18}$ è una soluzione.

Consideriamo ora gli altri ordini possibili di un elemento in $(\mathbb{Z}/27\mathbb{Z})^*$ per vedere se ci sono altre soluzioni.

Se $k = 9$, per le considerazioni iniziali, si deve avere $x + 1 \equiv 0 \pmod 9$. Ma questa equazione implica, in particolare, che $x \equiv -1 \pmod 3$. Allora l'ordine di

x modulo 3, e quindi anche modulo 27, è pari. Ma poiché avevamo assunto che l'ordine fosse 9, in questo caso non abbiamo soluzioni.

Se $k = 6$ si deve avere $x + 1 \equiv 0 \pmod 6$, ossia $x = 6a - 1$ per qualche $a \in \mathbb{Z}$. Se $a \geq 0$, sviluppando con il binomio di Newton, si ha $(6a - 1)^{6a} \equiv -36a^2 + 1 \pmod{27}$. Quindi $(6a - 1)^{6a} \equiv 1 \pmod{27}$ se e solo se $a \equiv 0 \pmod 3$, ossia se $x \equiv -1 \pmod{18}$. Quindi anche questo caso non dà nuove soluzioni. Se invece $a < 0$ allora ragioniamo allo stesso modo sviluppando $(6a - 1)^{-6a}$.

Se abbiamo $k = 3$, come nel caso $k = 9$, si deve avere $x \equiv -1 \pmod 3$, quindi l'ordine di x deve essere pari, ossia $x + 1 \equiv 0 \pmod 6$; ci si riconduce quindi al caso precedente, che non dà altre soluzioni.

Se $k = 2$, visto che l'unico elemento di ordine 2 in $(\mathbb{Z}/27\mathbb{Z})^*$ è $x \equiv -1 \pmod{27}$; per avere una soluzione dell'equazione si deve avere $x + 1 \equiv 0 \pmod 2$ e quindi $x \equiv -1 \pmod{54}$. Anche in questo caso non ci sono nuove soluzioni rispetto alle precedenti.

Infine l'unico elemento di ordine 1, cioè per $k = 1$, è $x \equiv 1 \pmod{27}$, ed ovviamente questa è una soluzione dell'equazione.

In conclusione, le soluzioni sono $x \equiv -1 \pmod{18}$ e $x \equiv 1 \pmod{27}$.

117. La prima congruenza del sistema è risolubile se e solo se $(a, 27) \mid 12$, cioè se $(a, 27) = 1, 3$. La seconda congruenza si può spezzare nelle due congruenze $a^3x^2 \equiv 9 \pmod 3$ e $a^3x^2 \equiv 9 \pmod{13}$. La prima è sempre risolubile, infatti ha, per esempio, la soluzione $x \equiv 0 \pmod 3$. Per la risolubilità della seconda è innanzitutto necessario che $a \not\equiv 0 \pmod{13}$.

Sia poi g un generatore del gruppo $(\mathbb{Z}/13\mathbb{Z})^*$ e poniamo $a = g^i$, $x = g^j$, $3 = g^k$. Si deve avere $3i + 2j \equiv 2k \pmod{12}$, da cui $i = 2i'$ deve essere pari, ossia a deve essere un quadrato modulo 13, inoltre se $i = 2i'$, l'ultima congruenza si semplifica in $3i' + j \equiv k \pmod 6$, che ha chiaramente per soluzione $j \equiv k - 3i' \pmod 6$.

Veniamo ora alle soluzioni del sistema. Per il Teorema Cinese dei Resti, se le due singole congruenze sono risolubili, l'unica ostruzione all'esistenza di una soluzione del sistema può venire dal fatto che le soluzioni modulo il massimo comune divisore dei moduli $(27, 39) = 3$ non sono compatibili. Se $(a, 27) = 1$ la soluzione della prima equazione è $x \equiv 12a^{-1} \pmod{27}$ e dunque in particolare $x \equiv 0 \pmod 3$ che è anche soluzione della seconda equazione. Se $(a, 27) = 3$, poniamo $a = 3b$ con $(b, 3) = 1$; la seconda congruenza diventa $27b^3x^2 \equiv 9 \pmod{39}$, che, considerata modulo 3, ha per soluzioni tutti gli interi.

Pertanto il sistema è risolubile se e solo se sono risolubili entrambe le congruenze, ossia se $(a, 27) = 1, 3$, cioè $a \not\equiv 0 \pmod 9$, e $a \equiv \pm 1, \pm 3, \pm 4 \pmod{13}$, cioè a è un quadrato non nullo modulo 13.

118. Guardiamo innanzitutto quando le singole congruenze sono risolubili e quante soluzioni hanno.

La prima congruenza è risolubile se e solo se $2a$ è un quadrato modulo 5. Visto che i quadrati modulo 5 sono $0, \pm 1$, la congruenza è risolubile se se solo se $a \equiv 0 \pmod 5$, per cui vi è una sola soluzione, $x \equiv 0 \pmod 5$, o $a \equiv \pm 2 \pmod 5$, con due soluzioni, le due radici quadrate di $2a$.

La seconda congruenza è risolubile se e solo se è risolubile per i moduli 5 e 7 e se le soluzioni per questi moduli sono compatibili. In linea generale, le congruenze

modulo 5 e modulo 7 sono risolubili se la classe di 3 fa parte del sottogruppo moltiplicativo generato dalla classe di a.

Poiché 3 è un generatore di $(\mathbb{Z}/5\mathbb{Z})^*$, la congruenza $a^x \equiv 3 \pmod 5$ è risolubile se e solo se a è un generatore, ossia se e solo se $a \equiv \pm 2 \pmod 5$. In entrambi i casi avremo una sola soluzione modulo $4 = \phi(5)$; inoltre tale classe sarà sicuramente dispari perché, altrimenti, a^x sarebbe un quadrato e quindi non un generatore.

⟦Risolvendo esplicitamente abbiamo che se $a \equiv 2 \pmod 5$ la soluzione è $x \equiv 3 \pmod 4$, mentre, se $a \equiv -2 \pmod 5$, la soluzione è $x \equiv 1 \pmod 4$.⟧

Analogamente, poiché 3 è un generatore di $(\mathbb{Z}/7\mathbb{Z})^*$, la congruenza $a^x \equiv 3 \pmod 7$ è risolubile se e solo se a è un generatore, ossia se e solo se $a \equiv 3, 5 \pmod 7$. Anche per questa congruenza, avremo una sola soluzione modulo $6 = \phi(7)$; inoltre, per lo stesso motivo di prima, anche tale classe è dispari.

⟦Risolvendo esplicitamente abbiamo che per $a \equiv 3 \pmod 7$ si ha $x \equiv 1 \pmod 6$, per $a \equiv 5 \pmod 7$ si ha $x \equiv 5 \pmod 6$.⟧

Ne segue che la seconda equazione è risolubile se e solo se $a \equiv \pm 2 \pmod 5$ e $a \equiv 3, 5 \pmod 7$ ossia $a \equiv 3, 12, 17, 33 \pmod{35}$: abbiamo visto che questa è una condizione necessaria; la condizione è anche sufficiente perché nei casi considerati le soluzioni sono concordi modulo $2 = (4, 6)$. Inoltre, la soluzione sarà una sola classe di congruenza modulo 12, il minimo comune multiplo di 4 e 6.

Riassumendo, visto che i moduli delle soluzioni sono primi fra loro, il sistema è risolubile quando le due equazioni sono risolubili contemporaneamente, ossia se $a \equiv 3, 12, 17, 33 \pmod{35}$. Quindi il sistema è risolubile per tutti i valori di a sopra elencati ed ha 2 soluzioni modulo 5, per la prima equazione, e una soluzione modulo 12, per la seconda equazione. In conclusione, due soluzioni modulo 60, il minimo comune multiplo di 5 e 12.

119. La prima equazione si risolve direttamente, essendo 13 primo, usando la formula per le equazioni di secondo grado, o anche per tentativi, e ha le due soluzioni $x \equiv 3, 9 \pmod{13}$.

La risolubilità della seconda equazione dipende dalla condizione $(a, 78) \mid 27$. Visto che $78 = 2 \cdot 3 \cdot 13$ e $27 = 3^3$, la condizione equivale a $(a, 2) = (a, 13) = 1$. Scomponiamo l'equazione nei moduli 2, 13 e 3. Per i valori di a compatibili modulo 2 e modulo 13 si hanno rispettivamente, le soluzioni $x \equiv 1 \pmod 2$ e $x \equiv a^{-1} \pmod{13}$. Per quanto riguarda il modulo 3 non ci sono condizioni su a; però, se $(a, 3) = 1$ l'unica soluzione è $x \equiv 0 \pmod 3$, mentre per $3 \mid a$ tutti gli interi x sono soluzioni.

Per la risolubilità del sistema, ci devono essere soluzioni della prima equazione che sono anche soluzioni della seconda equazione. Per la soluzione $x \equiv 3 \pmod{13}$ è quindi necessario che $3a \equiv 27 \pmod{13}$, ossia che $a \equiv 9 \pmod{13}$. Per la soluzione $x \equiv 9 \pmod{13}$ è necessario che $9a \equiv 27 \pmod{13}$, ossia che $a \equiv 3 \pmod{13}$.

Concludendo, il sistema è risolubile se e solo se $a \equiv 1 \pmod 2$ e $a \equiv 9, 3 \pmod{13}$, cioè se e solo se $a \equiv 9, 3 \pmod{26}$. Se $(a, 3) = 1$, cioè se $a \equiv 35, 61$ e $a \equiv 29, 55 \pmod{78}$, le soluzioni sono rispettivamente $x \equiv 1 \pmod 2$, $x \equiv 3, 9 \pmod{13}$, $x \equiv 0 \pmod 3$, ossia $x \equiv 3, 9 \pmod{78}$. Se, infine, $3 \mid a$, cioè $a \equiv 9, 3$

(mod 78), non c'è nessuna condizione sulla classe di x modulo 3 e quindi le soluzioni sono rispettivamente $x \equiv 3, 9 \pmod{26}$.

120. Spezziamo la prima congruenza con il Teorema Cinese dei Resti

$$\begin{cases} x^2 + x + 3 \equiv 0 & (\text{mod } 5) \\ x^2 - x \equiv 0 & (\text{mod } 3) \\ 30x \equiv -6 & (\text{mod } 81). \end{cases}$$

Risolviamo ora le singole equazioni.

Poiché 5 è primo, la formula risolutiva per le equazioni di secondo grado fornisce le soluzioni 1 e 3 dell'equazione $x^2 + x + 3 \equiv 0 \pmod{5}$.

Per verifica diretta oppure osservando che 3 è primo e quindi vale il Principio di Annullamento del Prodotto, si ha che le soluzioni di $x^2 - x = x(x-1) \equiv 0 \pmod{3}$ sono 0 e 1.

Dividendo per 6 otteniamo che $30x \equiv -6 \pmod{81}$ è equivalente a $5x \equiv -1 \pmod{27}$ e poi, moltiplicando per 11 che è l'inverso di 5, ricaviamo $x \equiv 16 \pmod{27}$.

Il sistema assegnato è quindi equivalente all'unione dei sistemi

$$\begin{cases} x \equiv 1, 3 & (\text{mod } 5) \\ x \equiv 0, 1 & (\text{mod } 3) \\ x \equiv 16 & (\text{mod } 27). \end{cases}$$

Per $x \equiv 0 \pmod{3}$ il sottosistema dato dalle ultime due equazioni, e quindi il sistema, non ha soluzione. Il sottosistema

$$\begin{cases} x \equiv 1 & (\text{mod } 3) \\ x \equiv 16 & (\text{mod } 27) \end{cases}$$

ha invece soluzione $x \equiv 16 \pmod{27}$.

Le soluzioni del sistema iniziale sono quindi le due classi modulo $5 \cdot 27 = 135$ che risolvono i due sistemi

$$\begin{cases} x \equiv 1, 3 & (\text{mod } 5) \\ x \equiv 16 & (\text{mod } 27). \end{cases}$$

È semplice verificare che le due soluzioni sono $x \equiv 16 \pmod{135}$ e $x \equiv 43 \pmod{135}$.

121. Per il Teorema Cinese dei Resti, la congruenza assegnata è equivalente al sistema

$$\begin{cases} x(x^{100} - 1) \equiv 0 & (\text{mod } 7) \\ x(x^{100} - 1) \equiv 0 & (\text{mod } 11) \\ x(x^{100} - 1) \equiv 0 & (\text{mod } 13). \end{cases}$$

Indichiamo con p un numero primo e contiamo le soluzioni della generica equazione $x(x^{100} - 1) \equiv 0 \pmod{p}$. Poiché p è primo questo prodotto è 0 se e solo se

uno dei due fattori è 0, quindi $x \equiv 0 \pmod{p}$ oppure $x^{100} \equiv 1 \pmod{p}$. Le soluzioni dell'equazione $x^{100} \equiv 1 \pmod{p}$ sono gli elementi di $(\mathbb{Z}/p\mathbb{Z})^*$ il cui ordine divide 100, e quindi, poiché l'ordine di un elemento divide l'ordine del gruppo, sono gli elementi il cui ordine divide $(100, p-1)$. Essendo $(\mathbb{Z}/p\mathbb{Z})^*$ un gruppo ciclico di ordine multiplo di $(100, p-1)$, contiene esattamente $(100, p-1)$ soluzioni dell'equazione $x^{100} \equiv 1 \pmod{p}$. In tutto l'equazione ha quindi $(100, p-1)+1$ soluzioni.

Da questo segue che le tre equazioni del sistema hanno rispettivamente $(100, 6)+1 = 3$ soluzioni modulo 7, $(100, 10)+1 = 11$ soluzioni modulo 11 e $(100, 12)+1 = 5$ modulo 13.

Le soluzioni del sistema si ottengono mettendo a sistema una qualsiasi soluzione modulo 7 con una qualsiasi soluzione modulo 11 e con una qualsiasi soluzione modulo 13. Le soluzioni si trovano quindi risolvendo i $3 \cdot 11 \cdot 5 = 165$ sistemi del tipo

$$\begin{cases} x \equiv a & \pmod 7 \\ x \equiv b & \pmod{11} \\ x \equiv c & \pmod{13}. \end{cases}$$

Per il Teorema Cinese dei Resti, ognuno di questi sistemi ha un'unica soluzione modulo $7 \cdot 11 \cdot 13 = 1001$ e le soluzioni di sistemi diversi sono diverse, quindi le soluzioni dell'equazione assegnata sono 165.

122. Passando modulo 2 si vede che ogni soluzione x deve essere pari; sia quindi $x = 2y$. Sostituendo abbiamo $2^5y^5 - 2^5y = 2^5y(y^4-1) \equiv 0 \pmod{2^{10}}$, da cui otteniamo $y(y^4-1) \equiv 0 \pmod{2^5}$. Osserviamo che uno solo tra y e y^4-1 è pari, quindi si ha $y \equiv 0 \pmod{2^5}$, oppure $y^4 - 1 \equiv 0 \pmod{2^5}$.

La congruenza $y \equiv 0 \pmod{2^5}$ dà le soluzioni $x \equiv 0 \pmod{2^6}$ che costituiscono 2^4 classi modulo 2^{10}.

Consideriamo la congruenza $y^4 - 1 \equiv 0 \pmod{2^5}$. Fattorizzando si ha $y^4 - 1 = (y-1)(y+1)(y^2+1) \equiv 0 \pmod{2^5}$.

Chiaramente in questo caso y è dispari e quindi i fattori $y-1$, $y+1$ e y^2+1 sono sono tutti e tre pari. D'altra parte, è immediato vedere che $y^2+1 \equiv 2 \pmod 4$, cioè y^2+1 è divisibile per 2 ma non per 4; l'equazione è quindi equivalente a $(y-1)(y+1) \equiv 0 \pmod{2^4}$. Ora, essendo $y-1$ e $y+1$ due numeri pari consecutivi, uno sarà divisibile esattamente per 2 quindi le soluzioni sono $y \equiv 1 \pmod{2^3}$ e $y \equiv -1 \pmod{2^3}$. Questo caso dà le soluzioni $x = 2y \equiv \pm 2 \pmod{2^4}$, cioè $2 \cdot 2^6 = 2^7$ soluzioni modulo 2^{10}.

La congruenza assegnata ha quindi $2^4 + 2^7 = 144$ soluzioni modulo 2^{10}.

123. Risolviamo la prima congruenza. Si calcola che, in $(\mathbb{Z}/17\mathbb{Z})^*$, $\mathrm{ord}(2) = 8$, $\mathrm{ord}(3) = 16$ e $2 = 3^{14}$, da cui si ottiene $3^{14x} \equiv 3^{x+a^2} \pmod{17}$ che è equivalente a $14x \equiv x + a^2 \pmod{16}$. Risolvendo si ha $x \equiv 5a^2 \pmod{16}$.

La congruenza $3x \equiv a^{23} \pmod{24}$ ha soluzione se e solo se $3 = (3, 24) \mid a^{23}$ cioè se e solo se $a \equiv 0 \pmod 3$. In tal caso, usando il Teorema Cinese dei Resti, il

sistema diventa

$$\begin{cases} x \equiv 5a^2 & (\text{mod } 16) \\ 3x \equiv a^{23} & (\text{mod } 3) \\ 3x \equiv a^{23} & (\text{mod } 8). \end{cases}$$

Poiché la seconda equazione è sempre verificata, e la terza può essere risolta come $x \equiv 3a^{23} \pmod 8$, il sistema è risolubile se e solo se $8 = (16, 8) \mid 5a^2 - 3a^{23}$, cioè se e solo se $5a^2 - 3a^{23} \equiv 0 \pmod 8$.

Ora $a^2(5 - 3a^{21}) \equiv 0 \pmod 8$ è verificata se e solo se $a^2 \equiv 0 \pmod 8$ oppure $5 - 3a^{21} \equiv 0 \pmod 8$ in quanto i due fattori hanno sempre parità opposta. Risolviamo ora queste due equazioni singolarmente. Per la prima abbiamo $a^2 \equiv 0 \pmod 8$ se e solo se $a \equiv 4 \pmod 4$; per la seconda invece $5 - 3a^{21} \equiv 0 \pmod 8$ se e solo se $a^{21} \equiv -1 \pmod 8$ e, quindi, usando che $a^2 \equiv 1 \pmod 8$ essendo a dispari, se e solo se $a \equiv -1 \pmod 8$.

Mettendo insieme le condizioni trovate si ha che il sistema è risolubile se e solo se

$$\begin{cases} a \equiv 0 & (\text{mod } 3) \\ a \equiv 0 & (\text{mod } 4) \end{cases} \quad \text{oppure} \quad \begin{cases} a \equiv 0 & (\text{mod } 3) \\ a \equiv -1 & (\text{mod } 8) \end{cases}$$

e risolvendo si calcola che il sistema è risolubile se $a \equiv 0, 12, 15 \pmod{24}$, mentre non è risolubile per le altre classi modulo 24.

124. La prima equazione ha soluzione se e solo se $3 = (3, 9) \mid a + 1$ cioè se e solo se $a \equiv 2 \pmod 3$. Quindi il sistema non ha soluzione se $a \not\equiv 2 \pmod 3$. Assumiamo allora che $a \equiv 2 \pmod 3$, possiamo quindi scrivere $a = 2 + 3b$ con $b \in \mathbb{Z}$. La prima equazione diventa $x \equiv b + 1 \pmod 3$.

Usando il Teorema Cinese dei Resti la seconda equazione è equivalente al sistema

$$\begin{cases} (x - 1)(x - a) \equiv 0 & (\text{mod } 3) \\ (x - 1)(x - a) \equiv 0 & (\text{mod } 5). \end{cases}$$

Poiché 3 e 5 sono numeri primi, vale il Principio di Annullamento del Prodotto, quindi le soluzioni della prima equazione sono $x \equiv 1 \pmod 3$ e $x \equiv a \equiv 2 \pmod 3$, e quelle della seconda sono $x \equiv 1 \pmod 5$ e $x \equiv a \equiv 2 + 3b \pmod 5$. Otteniamo che il sistema è equivalente a

$$\begin{cases} x \equiv b + 1 & (\text{mod } 3) \\ x \equiv 1, 2 & (\text{mod } 3) \\ x \equiv 1, 3b + 2 & (\text{mod } 5) \end{cases}$$

ed è quindi risolubile se e solo se c'è compatibilità tra le due equazioni modulo 3. In particolare, se $b \equiv 2 \pmod 3$, cioè $a \equiv 8 \pmod 9$, non ci sono soluzioni; se $b \equiv 0 \pmod 3$, cioè $a \equiv 2 \pmod 9$, il sistema iniziale è equivalente a

$$\begin{cases} x \equiv 1 & (\text{mod } 3) \\ x \equiv 1, 3b + 2 & (\text{mod } 5), \end{cases}$$

mentre se $b \equiv 1 \pmod 3$, cioè $a \equiv 5 \pmod 9$, il sistema iniziale è equivalente al sistema

$$\begin{cases} x \equiv 2 & (\text{mod } 3) \\ x \equiv 1, 3b+2 & (\text{mod } 5). \end{cases}$$

Contiamo il numero di soluzioni del primo sistema: se le due soluzioni dell'equazione modulo 5 coincidono, cioè se $2 + 3b \equiv 1 \pmod 5$, ovvero $b \equiv 3 \pmod 5$, abbiamo che il sistema ha un'unica soluzione modulo 15, quindi ha 6 soluzioni modulo 90. Se invece $b \not\equiv 3 \pmod 5$ il sistema ha due soluzioni modulo 15, quindi 12 soluzioni modulo 90. Lo stesso discorso vale per il secondo sistema.

Per il sistema iniziale, mettendo insieme le condizioni trovate possiamo quindi concludere che: se $a \equiv 0, 1 \pmod 3$ la prima equazione e quindi il sistema non ha soluzione; se invece $a \equiv 2 \pmod 3$ dobbiamo distinguere i seguenti sottocasi.

(1) Se $a \equiv 8 \pmod 9$ non c'è compatibilità tra le due equazioni modulo 3, quindi il sistema non ha soluzione. (2) Se $a \equiv 2 \pmod 9$ il sistema ha soluzione e modulo 90 ha 6 soluzioni se $a \equiv 11 \pmod{45}$ mentre ne ha 12 altrimenti, cioè se $a \equiv 2, 20, 29, 38 \pmod{45}$. (3) Se, infine, $a \equiv 5 \pmod 9$ il sistema ha soluzione e modulo 90 ha 6 soluzioni se $a \equiv -4 \pmod{45}$ mentre ne ha 12 altrimenti, cioè se $a \equiv 5, 14, 23, 32 \pmod{45}$.

125. Risolviamo innanzitutto le singole equazioni. Per la prima equazione abbiamo $x^2(x^{25} - 1) \equiv 0 \pmod{144}$ e, usando il Teorema Cinese dei Resti, l'equazione è equivalente al sistema

$$\begin{cases} x^2(x^{25} - 1) \equiv 0 & (\text{mod } 16) \\ x^2(x^{25} - 1) \equiv 0 & (\text{mod } 9). \end{cases}$$

Osserviamo che x^2 e $x^{25} - 1$ sono primi tra loro per ogni intero x. Nella prima equazione di quest'ultimo sistema, questo significa che o $x^2 \equiv 0 \pmod{16}$, e quindi $x \equiv 0 \pmod 4$, o $x^{25} \equiv 1 \pmod{16}$ e, quindi, in particolare $(x, 2) = 1$. In quest'ultimo caso, visto che $\phi(16) = 8$, per il Teorema di Eulero abbiamo $x^8 \equiv 1 \pmod{16}$, da cui $x^{25} = x^{1+3\cdot 8} \equiv x \pmod{16}$ e quindi la soluzione $x \equiv 1 \pmod{16}$.

Analogamente, per la seconda equazione o vale $x^2 \equiv 0 \pmod 9$, e quindi $x \equiv 0 \pmod 3$ o, usando $\phi(9) = 6$, vale $x^{25} = x^{1+6\cdot 4} \equiv x \pmod 9$ e quindi l'altra soluzione $x \equiv 1 \pmod 9$.

Consideriamo ora la seconda equazione del sistema iniziale, cioè l'equazione $10x \equiv a \pmod{25}$ con $a \in \mathbb{Z}$. Affinché l'equazione sia risolubile dobbiamo avere $5 = (25, 10) \mid a$, quindi $a = 5b$ per qualche $b \in \mathbb{Z}$. Dividendo per 5 otteniamo l'equazione equivalente $2x \equiv b \pmod 5$ e quindi la soluzione $x \equiv 2^{-1}b \equiv 3b \pmod 5$.

Studiamo infine l'ultima equazione $2^{x-1} \equiv 4 \pmod{11}$. Dato che si ha $2^2 \equiv 4 \pmod{11}$, l'equazione è risolubile. Calcoliamo l'ordine di 2 (mod 11); visto che $2^2 \equiv 4$ e $2^5 \equiv -1 \pmod{11}$ e quindi $2^d \not\equiv 1 \pmod{11}$ per ogni divisore massimale di $10 = \phi(11)$, risulta che l'ordine cercato è 10. La soluzione dell'equazione è dunque $x - 1 \equiv 2 \pmod{10}$, cioè $x \equiv 3 \pmod{10}$. Usando il Teorema Cinese dei

Resti, possiamo infine riscrivere questa soluzione tramite il sistema

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 3 \pmod 5. \end{cases}$$

Torniamo ora alla soluzione del sistema. Sempre per il Teorema Cinese dei Resti, le singole equazioni sono compatibili tutte le volte che i moduli sono primi tra loro. Dobbiamo dunque verificare solo le seguenti compatibilità.

Dalla prima equazione abbiamo $x \equiv 0 \pmod 4$ oppure $x \equiv 1 \pmod{16}$, mentre dalla terza abbiamo $x \equiv 1 \pmod 2$. Dobbiamo quindi escludere il caso $x \equiv 0 \pmod 4$ e, poiché evidentemente $x \equiv 1 \pmod{16}$ implica $x \equiv 1 \pmod 2$, la condizione è $x \equiv 1 \pmod{16}$.

Inoltre dalla seconda equazione abbiamo $x \equiv 3b \pmod 5$ mentre $x \equiv 3 \pmod 5$ dalla terza equazione. La compatibilità si ha evidentemente per $b \equiv 1 \pmod 5$ e dà la condizione $x \equiv 3 \pmod 5$.

Riassumendo: la condizione di risolubilità è $a = 5b$ con $b \equiv 1 \pmod 5$, ossia $a \equiv 5 \pmod{25}$. Se questa è verificata, le soluzioni si trovano risolvendo i due sistemi

$$\begin{cases} x \equiv 1 \pmod{16} \\ x \equiv 0 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases} \qquad \begin{cases} x \equiv 1 \pmod{16} \\ x \equiv 1 \pmod 9 \\ x \equiv 3 \pmod 5. \end{cases}$$

Con facili calcoli si trovano le soluzioni $x \equiv 33 \pmod{240}$ e $x \equiv 433 \pmod{720}$.

126. La prima equazione può essere semplificata dividendo per 2, ottenendo

$$2^{2y^2-5y+3} \equiv 1 \pmod{18}.$$

Quindi 2^{2y^2-5y+3} deve essere invertibile $\pmod{18}$, ovvero $(2^{2y^2-5y+3}, 18) = 1$. Questo è possibile se e solo se $2y^2 - 5y + 3 = (y-1)(2y-3) = 0$. Ma, visto che cerchiamo soluzione intere, dobbiamo avere $y = 1$.

Consideriamo ora la terza equazione. È immediato vedere che $x \equiv -1 \pmod{100}$ è una soluzione. D'altra parte, se x è una soluzione, certamente deve essere $(x, 100) = 1$, e quindi, per il Teorema di Eulero, $x^{\phi(100)} = x^{40} \equiv 1 \pmod{100}$. Visto che l'inverso di 23 modulo 40 è 7, l'equazione $x^{23} \equiv -1 \pmod{100}$ implica $x \equiv x^{23\cdot 7} \equiv (-1)^7 \equiv -1 \pmod{100}$. Ne segue che la soluzione della terza equazione è $x \equiv -1 \pmod{100}$. Per l'uso successivo di questa soluzione con il Teorema Cinese dei Resti, la scriviamo nella forma

$$\begin{cases} x \equiv -1 \pmod 4 \\ x \equiv -1 \pmod{25}. \end{cases}$$

Consideriamo infine la seconda equazione. Possiamo sostituire $y = 1$, ottenendo $(2x^2 + 17)(2x^2 + 5x + 2)^{-1} \equiv 1 \pmod{592}$.

Fattorizzando, otteniamo $592 = 2^4 \cdot 37$ e $2x^2 + 5x + 2 = (x+2)(2x+1)$. Dunque $2x^2 + 5x + 2$ è invertibile modulo 592 se e solo se $x + 2$ e $2x + 1$ sono entrambi

invertibili modulo 2 e modulo 37. La condizione $x \equiv -1 \pmod{100}$, in particolare x dispari, assicura che sia $x+2$ che $2x+1$ sono invertibili modulo 2. L'invertibilità modulo 37 equivale a $x+2 \not\equiv 0 \pmod{37}$, cioè $x \not\equiv -2 \pmod{37}$, e $2x+1 \not\equiv 0 \pmod{37}$, cioè $x \not\equiv 18 \pmod{37}$.

Sotto queste condizioni, $(2x^2+17)(2x^2+5x+2)^{-1} \equiv 1 \pmod{592}$ equivale a $x \equiv 3 \pmod{592}$ e questa soluzione è compatibile sia con $x \equiv -1 \pmod{4}$ che con $x \not\equiv -2, 18 \pmod{37}$. Ne segue che $(x, 1)$ è una soluzione del sistema iniziale se e solo se x è una soluzione del sistema di congruenze

$$\begin{cases} x \equiv 3 & \pmod{16} \\ x \equiv 3 & \pmod{37} \\ x \equiv -1 & \pmod{25} \end{cases}$$

cioè, dopo qualche calcolo, $x \equiv 7699 \pmod{14800}$. Le soluzioni del sistema di congruenze sono quindi $(7699 + 14800t, 1)$ con $t \in \mathbb{Z}$.

127. La seconda congruenza ha soluzione se e solo se $(a, 10) = 1$; in tale caso la soluzione è $x \equiv a^{-1} \pmod{10}$; in particolare $(x, 10) = 1$.

La prima congruenza è equivalente al sistema

$$\begin{cases} a^x \equiv 1 & \pmod{11} \\ a^x \equiv 1 & \pmod{7}. \end{cases}$$

Una condizione certamente necessaria affinché le due equazioni del sistema siano risolubili è $a \not\equiv 0 \pmod{11}$ e $a \not\equiv 0 \pmod{7}$. Queste condizioni sono certamente compatibili con $(a, 10) = 1$ poiché $(10, 77) = 1$.

Supposto $a \not\equiv 0 \pmod{11}$, si ha $a^{10} \equiv 1 \pmod{11}$ per il Piccolo Teorema di Fermat; ma, per la risolubilità del sistema, è necessario anche che $a^x \equiv 1 \pmod{11}$ per qualche x con $(x, 10) = 1$. Pertanto l'ordine di a in $(\mathbb{Z}/11\mathbb{Z})^*$ deve dividere $(x, 10) = 1$ e quindi deve essere $a \equiv 1 \pmod{11}$. In questo caso, ogni intero x è soluzione dell'equazione $a^x \equiv 1 \pmod{11}$.

Supposto $a \not\equiv 0 \pmod{7}$, dato che le soluzioni della seconda equazione possono essere solo numeri dispari, l'ordine di a in $(\mathbb{Z}/7\mathbb{Z})^*$ deve essere un divisore di un numero dispari, e quindi un numero dispari. Poiché l'ordine di ogni elemento di $(\mathbb{Z}/7\mathbb{Z})^*$ è un divisore di 6, possiamo avere $\mathrm{ord}(a) = 1$, e quindi $a \equiv 1 \pmod{7}$, oppure $\mathrm{ord}(a) = 3$, e quindi $a \equiv 2, 4 \pmod{7}$. Se $a \equiv 1 \pmod{7}$, l'equazione $a^x \equiv 1 \pmod{7}$ ha per soluzione tutti gli interi. Se $a \equiv 2, 4 \pmod{7}$, l'equazione $a^x \equiv 1 \pmod{7}$ ha per soluzione $x \equiv 0 \pmod{3}$. Questa soluzione è certamente compatibile con $x \equiv a^{-1} \pmod{10}$ perché $(3, 10) = 1$.

Riassumendo, per la risolubilità del sistema dobbiamo avere: $(a, 10) = 1$, $a \equiv 1 \pmod{11}$, $a \equiv 1, 2, 4 \pmod{7}$.

Consideriamo dapprima il caso $a \equiv 1 \pmod{7}$. Allora la prima equazione ha per soluzione tutti gli interi x e quindi la soluzione del sistema è $x \equiv a^{-1} \pmod{10}$.

Elencando i casi, si ha

$$\begin{array}{llll} a \equiv 1 \pmod{10} \implies a \equiv 1 \pmod{770}, & & x \equiv 1 \pmod{10}, \\ a \equiv 3 \pmod{10} \implies a \equiv 463 \pmod{770}, & & x \equiv 7 \pmod{10}, \\ a \equiv 7 \pmod{10} \implies a \equiv 617 \pmod{770}, & & x \equiv 3 \pmod{10}, \\ a \equiv 9 \pmod{10} \implies a \equiv 309 \pmod{770}, & & x \equiv 9 \pmod{10}. \end{array}$$

Consideriamo ora il caso $a \equiv 2, 4 \pmod 7$. Abbiamo

$$\begin{array}{llll} a \equiv 1 \pmod{10} \implies a \equiv 331, 221 \pmod{770}, & & x \equiv 21 \pmod{30}, \\ a \equiv 3 \pmod{10} \implies a \equiv 23, 683 \pmod{770}, & & x \equiv 27 \pmod{30}, \\ a \equiv 7 \pmod{10} \implies a \equiv 177, 67 \pmod{770}, & & x \equiv 3 \pmod{30}, \\ a \equiv 9 \pmod{10} \implies a \equiv 639, 529 \pmod{770}, & & x \equiv 9 \pmod{30}. \end{array}$$

128. Usando il Teorema Cinese dei Resti, dividiamo l'equazione modulo 200 in modulo 8 e modulo 25, ottenendo il sistema equivalente a quello dato

$$\begin{cases} 7^x \equiv a \pmod 8 \\ (x+a)^4 \equiv 0 \pmod 8 \\ (x+a)^4 \equiv 0 \pmod{25}. \end{cases}$$

La prima equazione di questo nuovo sistema dà come condizione necessaria $a \equiv \pm 1 \pmod 8$; in particolare, a deve essere dispari. Visto che a deve essere dispari, la seconda equazione dà come condizione necessaria che anche x deve essere dispari; d'altra parte, se a e x sono entrambi dispari, allora $2 \mid a + x$, quindi $16 \mid (a + x)^4$ e la seconda equazione è soddisfatta. Ritornando alla prima equazione, x dispari implica che $a \equiv 7 \pmod 8$. Viceversa, se $a \equiv 7 \pmod 8$ le prime due equazioni sono risolubili, e hanno per soluzione $x \equiv 1 \pmod 2$.

La terza equazioni è risolubile per ogni valore di a ed ha per soluzione $x \equiv -a \pmod 5$, infatti, come prima, se $5 \mid x + a$ allora $5^4 \mid (x + a)^4$.

In conclusione, il sistema è risolubile se e solo se $a \equiv 7 \pmod 8$, con le seguenti soluzioni.

Se $a \equiv 0 \pmod 5$, ossia $a \equiv 15 \pmod{40}$, $x \equiv 0 \pmod 5$ e $x \equiv 1 \pmod 2$, ossia $x \equiv 5 \pmod{10}$.

Se $a \equiv 1 \pmod 5$, ossia $a \equiv 31 \pmod{40}$, $x \equiv 4 \pmod 5$ e $x \equiv 1 \pmod 2$, ossia $x \equiv 9 \pmod{10}$.

Se $a \equiv 2 \pmod 5$, ossia $a \equiv 7 \pmod{40}$, $x \equiv 3 \pmod 5$ e $x \equiv 1 \pmod 2$, ossia $x \equiv 3 \pmod{10}$.

Se $a \equiv 3 \pmod 5$, ossia $a \equiv 23 \pmod{40}$, $x \equiv 2 \pmod 5$ e $x \equiv 1 \pmod 2$, ossia $x \equiv 7 \pmod{10}$.

Se $a \equiv 4 \pmod 5$, ossia $a \equiv 39 \pmod{40}$, $x \equiv 1 \pmod 5$ e $x \equiv 1 \pmod 2$, ossia $x \equiv 1 \pmod{10}$.

129. Esaminiamo la prima equazione. Perché essa abbia soluzioni dobbiamo avere $(7a, 49) \mid a$. Per il valore di $(7a, 49)$ abbiamo due possibilità.

Se $7 \nmid a$, allora $(7a, 49) = 7$ e quindi la condizione necessaria $7 \mid a$ non è mai verificata. In questo caso non ci sono soluzioni. Se, invece, $7 \mid a$, allora $(7a, 49) = 49$

e quindi la condizione diventa $49 \mid a$, ovvero $a \equiv 0 \pmod{49}$. L'equazione $7ax \equiv a \pmod{49}$ diviene $0 \equiv a \pmod{49}$ che è sempre verificata in questo caso.

Riassumendo, la prima equazione ha soluzioni se e solo se $a \equiv 0 \pmod{49}$ e, in tal caso, tutti gli interi sono soluzioni.

Per quanto riguarda la seconda equazione, distinguiamo tre casi.

(1) Se $x \equiv 0 \pmod 3$ abbiamo $x^a \equiv 0^a \equiv 0 \pmod 3$ per ogni $a > 0$; l'equazione perde significato sia per $a = 0$ sia per $a < 0$, in quanto x non è invertibile modulo 3. Dunque questo caso non dà soluzioni per nessun valore di a. (2) Se $x \equiv 1 \pmod 3$ l'equazione è soddisfatta per ogni $a \in \mathbb{Z}$. (3) Se, infine, $x \equiv 2 \pmod 3$ l'equazione diviene $2^a \equiv 1 \pmod 3$, che è soddisfatta se e solo se $a \equiv 0 \pmod 2$.

La seconda equazione ha quindi soluzione $x \equiv 1 \pmod 3$ per ogni $a \in \mathbb{Z}$, e soluzione $x \equiv 2 \pmod 3$ se $a \equiv 0 \pmod 2$.

Concludendo, le soluzioni del sistema posso essere così riassunte.

Se $a \equiv 0 \pmod{49}, a \equiv 0 \pmod 2$, ovvero $a \equiv 0 \pmod{98}$, abbiamo le soluzioni $x \equiv 1, 2 \pmod 3$. Se, invece, $a \equiv 0 \pmod{49}, a \not\equiv 0 \pmod 2$, ovvero $a \equiv 49 \pmod{98}$ abbiamo la soluzione $x \equiv 1 \pmod 3$. Per gli altri valori di $a \in \mathbb{Z}$ non ci sono soluzioni, perché la prima equazione non ha soluzioni.

130. Risolviamo la prima equazione. Dato che $1000 = 8 \cdot 125$ per il Teorema Cinese dei Resti essa è equivalente al sistema

$$\begin{cases} x^3 \equiv 0 & \pmod 8 \\ x^3 \equiv 2^3 & \pmod{125}. \end{cases}$$

Le soluzioni di $x^3 \equiv 0 \pmod 8$ sono chiaramente tutti gli x pari. Per la seconda equazione di questo nuovo sistema, osserviamo che 2 è invertibile in $(\mathbb{Z}/125\mathbb{Z})^*$ e, di conseguenza, lo è anche x. Possiamo quindi risolvere l'equazione in $(\mathbb{Z}/125\mathbb{Z})^*$ riscrivendola come $(x/2)^3 \equiv 1 \pmod{125}$ e, visto che 3 non divide $|(\mathbb{Z}/125\mathbb{Z})^*| = \phi(125) = 100$, otteniamo $x/2 \equiv 1 \pmod{125}$. Possiamo concludere che l'equazione $x^3 \equiv 8 \pmod{125}$ ha quindi come unica soluzione $x \equiv 2 \pmod{125}$.

Mettendo assieme le soluzioni abbiamo il sistema

$$\begin{cases} x \equiv 2 & \pmod{125} \\ x \equiv 0 & \pmod 2 \end{cases}$$

che ha soluzioni $x \equiv 2, 252, 502, 752 \pmod{1000}$. Quindi abbiamo i quattro sistemi

$$\begin{cases} x \equiv 0, 252, 502, 752 & \pmod{1000} \\ x \equiv 2 & \pmod 3 \end{cases}$$

con il vincolo $0 \le x < 3001$. Ancora per il Teorema Cinese dei Resti, ciascuno di essi ha un'unica soluzione modulo 3000, quindi abbiamo esattamente 4 soluzioni.

131. (i) Risolviamo la congruenza $x^{36} \equiv x \pmod 9$ distinguendo due casi.

(1) Se $(x, 3) \neq 1$, allora $x = 3y$ per qualche $y \in \mathbb{Z}$. Di conseguenza, $x^{36} = (3y)^{36} \equiv 3^{36} y^{36} \equiv 0 \pmod 9$, quindi $x \equiv x^{36} \equiv 0 \pmod 9$.

(2) Se invece $(x, 3) = 1$, allora $x \in (\mathbb{Z}/9\mathbb{Z})^*$. In questo caso l'equazione data è equivalente a $x^{35} \equiv 1 \pmod 9$. Per il Teorema di Eulero abbiamo $x^{\phi(9)} = x^6 \equiv 1 \pmod 9$ e quindi $x^{35} \equiv x^{-1} \pmod 9$. La nostra equazione diventa $x^{-1} \equiv 1 \pmod 9$, cioè $x \equiv 1 \pmod 9$.

Concludiamo che la congruenza data ha due soluzioni, $x \equiv 0, 1 \pmod 9$.

(ii) Risolviamo ora la congruenza $x^2 - x = x(x-1) \equiv 0 \pmod{64}$. È chiaro che x e $x-1$ sono primi tra loro, le uniche soluzioni sono $x \equiv 0 \pmod{64}$ e $x \equiv 1 \pmod{64}$.

Il sistema originario ha quindi per soluzioni quelle dei quattro sistemi

$$\begin{cases} x \equiv 0 \text{ o } 1 & (\text{mod } 9) \\ x \equiv 0 \text{ o } 1 & (\text{mod } 64). \end{cases}$$

Svolgendo i calcoli si trovano le quattro soluzioni $x \equiv 0, 1, 64, 513 \pmod{576}$.

132. Se $a = 0$ l'equazione è un'identità e quindi tutte le classi modulo 584 la risolvono; nel seguito supponiamo quindi $a > 0$. Abbiamo $584 = 2^3 \cdot 73$ e $x^{a+5} - x^a - x^5 + 1 = (x^a - 1)(x^5 - 1)$. In virtù del Teorema Cinese dei Resti, l'equazione assegnata è equivalente al sistema

$$\begin{cases} (x^5 - 1)(x^a - 1) \equiv 0 & (\text{mod } 8) \\ (x^5 - 1)(x^a - 1) \equiv 0 & (\text{mod } 73). \end{cases}$$

Studiamo la prima equazione. Osserviamo, prima di tutto, che chiaramente nessun numero pari verifica la congruenza. Inoltre, poiché il quadrato di ogni numero dispari è congruo a 1 modulo 8, limitandoci ai soli numeri dispari, si ha che $x^5 \equiv x \pmod 8$, mentre x^a è congruo a 1 se a è pari ed è congruo a x se a è dispari.

Quindi, se $a \equiv 0 \pmod 2$,

$$(x^5 - 1)(x^a - 1) \equiv 0 \pmod 8 \iff x \equiv 1 \pmod 2,$$

mentre se $a \equiv 1 \pmod 2$

$$\begin{aligned} (x^5 - 1)(x^a - 1) \equiv 0 \pmod 8 &\iff (x-1)^2 \equiv 0 \pmod 8 \\ &\iff x \equiv 1 \pmod 4. \end{aligned}$$

Passiamo alla seconda congruenza: 73 è primo, quindi modulo 73 vale il principio di annullamento del prodotto

$$(x^5 - 1)(x^a - 1) \equiv 0 \pmod{73} \iff x^5 \equiv 1 \pmod{73} \text{ o } x^a \equiv 1 \pmod{73}.$$

Ora $x^5 \equiv 1 \pmod{73}$ se e solo se l'ordine di x in $(\mathbb{Z}/73\mathbb{Z})^*$ divide 5. Poiché l'ordine di x deve anche dividere $\phi(73) = 72$ e $(5, 72) = 1$, si ha $x^5 \equiv 1 \pmod{73}$ se e solo se $x \equiv 1 \pmod{73}$. Per lo stesso motivo $x^a \equiv 1 \pmod{73}$ se e solo se $x^{(a,72)} \equiv 1 \pmod{73}$: essendo $(\mathbb{Z}/73\mathbb{Z})^*$ un gruppo ciclico, questa equazione ha esattamente $(a, 72)$ soluzioni modulo 73. In particolare, poi, l'unica soluzione $x \equiv 1 \pmod{73}$ di $x^5 - 1 \equiv 0 \pmod{73}$ è anche soluzione di $x^a - 1 \equiv 0 \pmod{73}$.

Tornando al sistema si ha che la seconda equazione ha $(a, 72)$ soluzioni modulo 73, e la prima ne ha una modulo 2, cioè 4 modulo 8, se a è pari, e una modulo 4, cioè 2 modulo 8, se a è dispari. Usando il Teorema Cinese dei Resti, possiamo concludere che le soluzioni modulo 584 sono $4(a, 72)$ se a è pari e $2(a, 72)$ se a è dispari.

133. In virtù del Teorema Cinese dei Resti il problema è equivalente al sistema di congruenze

$$\begin{cases} x^5 - 4x + 400 \equiv 0 \pmod{2^{10}} \\ x^5 - 4x + 400 \equiv 0 \pmod{5^{10}}. \end{cases}$$

La prima condizione implica $x \equiv 0 \pmod 4$; posto $x = 4y$, abbiamo che $x^5 \equiv 2^{10}y^5 \equiv 0 \pmod{2^{10}}$, da cui otteniamo $y \equiv 25 \pmod{2^6}$ e quindi $x \equiv 100 \pmod{2^8}$.

La seconda equazione del sistema implica che $x^5 - 4x + 400 \equiv 0 \pmod{5^2}$, da cui $x(x^4 + 1) \equiv 0 \pmod{25}$. Ora, $x^4 + 1 \equiv 1$ o $x^4 + 1 \equiv 2 \pmod 5$ per il Piccolo Teorema di Fermat, in particolare $x^4 + 1$ è sempre invertibile modulo 25. Ne segue che $x(x^4 + 1) \equiv 0 \pmod{25}$ se e solo se $x \equiv 0 \pmod{25}$, cioè $x = 5^2 t$ per qualche $t \in \mathbb{Z}$. Sostituendo questa condizione nell'equazione iniziale, si ottiene

$$5^{10}t^5 - 2^2 5^2 t + 2^4 5^2 \equiv -2^2 5^2 t + 2^4 5^2 \equiv 0 \pmod{5^{10}}$$

da cui $t \equiv 4 \pmod{5^8}$ e $x \equiv 100 \pmod{5^{10}}$. Il sistema iniziale si riduce a

$$\begin{cases} x \equiv 100 \pmod{2^8} \\ x \equiv 100 \pmod{5^{10}}. \end{cases}$$

La cui soluzione è $x \equiv 100 \pmod{2^8 \cdot 5^{10}}$. Concludiamo che le soluzioni modulo 10^{10} sono $10^{10}/(2^8 \cdot 5^{10}) = 4$.

3.4 Gruppi

134. Dimostriamo che B e C sono sottogruppi di $\mathrm{Hom}(G, G')$, mentre A e D non lo sono.

L'elemento neutro di $\mathrm{Hom}(G, G')$ è l'omomorfismo identicamente nullo, ossia l'omomorfismo e definito da $e(x) = 0$ per ogni $x \in G$. L'opposto di un omomorfismo f è l'omomorfismo $-f$ definito da $(-f)x = -f(x)$ per ogni $x \in G$.

Si ha $e \in B$, perché $\mathrm{Ker}(e) = G \supseteq H$. Se $f, g \in B$ e $h \in H$, allora $f(h) = g(h) = 0$, quindi $(f + g)(h) = 0$ e $f + g \in B$. Infine, se $f \in B$ e $h \in H$, allora $f(h) = 0$, quindi $(-f)(h) = 0$ e $-f \in B$.

Quindi B è un sottogruppo di $\mathrm{Hom}(G, G')$. Analogamente, C è un sottogruppo di $\mathrm{Hom}(G, G')$. Infatti $e \in C$, perché $e(G) = 0 \in H'$. Poi, se $f, g \in C$ e $x \in G$, allora $f(x), g(x) \in H'$ da cui $f(x) + g(x) \in H'$ e $f + g \in C$. E, infine, se $f \in C$ e $x \in G$, allora $f(x) \in H'$, da cui $(-f)(x) = -f(x) \in H'$ e $-f \in C$.

Osserviamo invece che, poiché H ed H' sono sottogruppi propri di G e G', l'elemento neutro e di $\mathrm{Hom}(G, G')$ non appartiene né ad A né a D, che quindi non possono essere sottogruppi.

135. (i) Poiché $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/nZ$ quando m ed n sono primi fra loro, abbiamo

$$G \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

Poniamo $G_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $G_3 = \mathbb{Z}/3\mathbb{Z}$, $G_5 = \mathbb{Z}/5\mathbb{Z}$. Se $(x, y, z) \in G_2 \times G_3 \times G_5$, abbiamo $o(x, y, z) = [o(x), o(y), o(z)] = o(x)o(y)o(z)$.

Pertanto (x, y, z) ha ordine 60 se e solo se $o(x) = 4$, $o(y) = 3$, $o(z) = 5$. Gli elementi di ordine 4 in G_2 sono 4: tutti tranne le 4 coppie (x_1, x_2) tali che $2(x_1, x_2) = (0, 0)$. Gli elementi di ordine 3 in G_3 sono 2: tutti tranne l'elemento neutro. Infine gli elementi di ordine 5 in G_5 sono 4: tutti tranne l'elemento neutro. Pertanto gli elementi di G di ordine 60 sono $4 \cdot 2 \cdot 4 = 32$.

(ii) Analogamente al primo punto, (x, y, z) ha ordine 30 se e solo se $o(x) = 2$, $o(y) = 3$, $o(z) = 5$. Le coppie $(x_1, x_2) \in G_2$ di ordine 2 sono 3: le quattro coppie per cui $2(x_1, x_2) = (0, 0)$ tranne l'elemento neutro. Per cui si ottiene che il numero di elementi di G di ordine 30 è uguale a 24.

Ora ogni elemento di ordine 30 genera un sottogruppo ciclico di ordine 30, mentre i modi in cui un sottogruppo ciclico di ordine 30 può essere generato da un elemento è pari al numero di elementi di ordine 30 in un gruppo ciclico di ordine 30, e cioè a $\phi(30) = 8$. Pertanto i sottogruppi ciclici di G di ordine 30 sono $24/8 = 3$.

(iii) Tutti gli omomorfismi $f : \mathbb{Z}/12\mathbb{Z} \longrightarrow G$ sono del tipo $f(\overline{n}) = ng$, dove $g \in G$. Infatti, se $f(\overline{1}) = g$, la proprietà di omomorfismo dice che necessariamente $f(\overline{n}) = f(\overline{1} + \cdots + \overline{1}) = g + \cdots + g = ng$. Si vede immediatamente che una tale applicazione, se è ben definita, è anche un omomorfismo: infatti si ha $f(\overline{m} + \overline{n}) = (m + n)g = mg + ng = f(\overline{m}) + f(\overline{n})$.

Per quanto riguarda la buona definizione, la condizione è che $\overline{m} = \overline{n} \Rightarrow mg = ng$. Se inoltre si richiede che l'omomorfismo sia iniettivo, la condizione diventa

$$\overline{m} = \overline{n} \Longleftrightarrow mg = ng.$$

Questa condizione è rispettata se e solo se $\mathrm{ord}(g) = 12$. Di nuovo come nel primo punto, (x, y, z) ha ordine 12 se e solo se $\mathrm{ord}(x) = 4, \mathrm{ord}(y) = 3, \mathrm{ord}(z) = 1$. Per i calcoli già eseguiti, il numero di elementi di G di ordine 12, e quindi anche il numero di omomorfismi iniettivi $f : \mathbb{Z}/12\mathbb{Z} \longrightarrow G$, è uguale a 8.

136. (i) La funzione identica $\mathrm{Id} : \mathbb{Z}/72\mathbb{Z} \longrightarrow \mathbb{Z}/72\mathbb{Z}$, $\mathrm{Id}(x) = x$, che è l'elemento neutro di G, appartiene ad H, poiché $\mathrm{Id}(\overline{12}) = \overline{12}$.

Date $f, g \in H$, $f(x) = ax$ e $g(x) = bx$ con $(a, 72) = (b, 72) = 1$, la funzione composta è $f \circ g(x) = abx$ e, visto che $(ab, 72) = 1$ e $f \circ g(\overline{12}) = f(\overline{12}) = \overline{12}$, essa appartiene ad H.

Se $f \in H$, $f(x) = ax$ con $(a, 72) = 1$ ed a' è tale che $aa' \equiv 1 \pmod{72}$, allora $(a', 72) = 1$ e la funzione g definita da $g(x) = a'x$ è l'inversa di f e, poiché se $f(\overline{12}) = \overline{12}$ anche $f^{-1}(\overline{12}) = \overline{12}$, essa appartiene ad H.

Pertanto H è un sottogruppo di G.

Per calcolarne l'ordine, si osservi che $f(\overline{12}) = \overline{12}$ equivale a $12a \equiv 12 \pmod{72}$, ossia $a \equiv 1 \pmod 6$. Ci sono esattamente 12 classi modulo 72 che sono congrue ad 1 modulo 6, ed esse sono tutte relativamente prime con 72 in quanto sono coprime con 6 e 6 ha gli stessi fattori primi di 72. Pertanto l'ordine di H è 12.

(ii) Il sottogruppo H non è ciclico. Infatti, presa comunque un'applicazione $f \in H$, $f(x) = ax$ con $a \equiv 1 \pmod 6$, si ha $f^6(x) = a^6 x$ e, da $a \equiv 1 \pmod 2$ segue $a^2 \equiv 1 \pmod 8$ e quindi $a^6 \equiv 1 \pmod 8$. Analogamente, da $a \equiv 1 \pmod 3$ segue $a^3 \equiv 1 \pmod 9$ e quindi $a^6 \equiv 1 \pmod 9$.

In definitiva, $a^6 \equiv 1 \pmod{72}$ e dunque ogni applicazione di H ha per ordine un divisore di 6.

137. (i) Un omomorfismo è iniettivo se e solo se il suo nucleo è il solo elemento neutro. Il nucleo dell'applicazione $f(x) = (ax, bx)$ è $\{x \in G \mid (ax, bx) = (\overline{0}, \overline{0})\}$. Siano u, v numeri interi che rappresentano le classi di resto a, b, rispettivamente. Si ha $ax = 0$ se e solo se l'ordine di x è un divisore di $(u, 12)$, e $bx = 0$ se e solo se l'ordine di x è un divisore di $(v, 12)$. Dunque il nucleo dell'omomorfismo è costituito da tutti gli elementi il cui ordine è un divisore di $(u, v, 12)$ e pertanto l'omomorfismo è iniettivo se e solo se $(u, v, 12) = 1$.

Sia Y l'insieme delle coppie cercate e, per d divisore di 12, sia Y_d l'insieme delle coppie (a, b) tali che $d \mid u$ e $d \mid v$. Abbiamo

$$|Y| = 12^2 - |Y_2 \cup Y_3| = 12^2 - |Y_2| - |Y_3| + |Y_6| = 12^2 - 6^2 - 4^2 + 2^2 = 96.$$

(ii) Con le notazioni precedenti, si ha $g \circ f(x) = (a + b)x$ e quindi $g \circ f$ è iniettivo se e solo se $(u + v, 12) = 1$. Per ogni $a \in G$, esistono esattamente $\phi(12) = 4$ valori di b per cui $(u + v, 12) = 1$, per cui il numero di coppie cercato è $12 \cdot 4 = 48$.

138. Sia $G = (\mathbb{Z}/p^2\mathbb{Z})^*$ e dimostriamo che $H = \{x \in G \mid x \equiv 1 \pmod p\} = \{1 + tp \mid t = 0, 1, \ldots, p-1\}$ è un sottogruppo di G. Infatti, $1 \in H$, e se $x, y \equiv 1 \pmod p$ allora anche $xy \equiv 1 \pmod p$ e $x^{-1} \equiv 1 \pmod p$. Il sottogruppo H ha p elementi, pertanto tutti i suoi elementi salvo l'elemento neutro hanno ordine p. In particolare, l'elemento $a = \overline{p+1}$ ha ordine p.

Sia $b \in G$ tale che la classe di b modulo p sia un generatore del gruppo ciclico $(\mathbb{Z}/p\mathbb{Z})^*$. Se $b^n \equiv 1 \pmod{p^2}$ allora abbiamo anche $b^n \equiv 1 \pmod p$ e quindi $n \equiv 0 \pmod{p-1}$; questo prova che l'ordine di b in G è un multiplo di $p - 1$.

Allora il sottogruppo ciclico generato da b ha per ordine un multiplo di $p - 1$, pertanto possiede un sottogruppo ciclico di ordine $p - 1$. Un generatore di questo sottogruppo è un elemento di ordine $p - 1$.

139. Dimostriamo innanzitutto che HK è un sottogruppo di G. Per prima cosa $e \in HK$: infatti $e = e \cdot e$, ed $e \in H, e \in K$ perché H, K sono sottogruppi di G. Poi, se $hk, h'k' \in HK$, usando che H è un sottogruppo normale di G si ha che $kH = Hk$ e pertanto esiste $h'' \in H$ tale che $kh' = h''k$; abbiamo dunque $hkh'k' = hh''kk' \in HK$ in quanto, essendo H e K sottogruppi di G, si ha $hh'' \in H$ e $kk' \in K$. Infine se

$hk \in HK$, allora $(hk)^{-1} = k^{-1}h^{-1}$ e, sfruttando la normalità di H come sopra, si ha che, per qualche $h' \in H$, vale $k^{-1}h^{-1} = h'k^{-1} \in HK$.

Dimostriamo infine che HK è un sottogruppo normale di G. Per ogni $g \in G$, per ogni $h \in H$ e per ogni $k \in K$ si ha $ghkg^{-1} = (ghg^{-1})(gkg^{-1})$ e quest'ultimo elemento appartiene ad HK in quanto, per la normalità di H e K, $ghg^{-1} \in H$ e $gkg^{-1} \in K$.

140. (i) Visto che $\mathrm{Ker}(f) \cap \mathrm{Im}(f)$ è un sottogruppo di G esso contiene l'elemento neutro. Viceversa, sia $x \in \mathrm{Ker}(f) \cap \mathrm{Im}(f)$; da $x \in \mathrm{Ker}(f)$ si ha $f(x) = e$, mentre, da $x \in \mathrm{Im}(f)$, si ottiene che esiste $y \in G$ tale che $x = f(y)$. Ne segue che $x = f(y) = f \circ f(y) = f(x) = e$.

(ii) È chiaro che $\mathrm{Ker}(f) \cdot \mathrm{Im}(f) \subseteq G$. Viceversa, scriviamo, per ogni $x \in G$, $x = xf(x^{-1}) \cdot f(x)$. Abbiamo che $f(xf(x^{-1})) = f(x) \cdot f \circ f(x^{-1}) = f(x) \cdot f(x^{-1}) = e$, da cui $xf(x^{-1}) \in \mathrm{Ker}(f)$. Poiché evidentemente $f(x) \in \mathrm{Im}(f)$ si ha la tesi.

141. (i) Si ha $|(\mathbb{Z}/49\mathbb{Z})^*| = \phi(49) = 42$. Gli elementi di ordine 2 e di ordine 3 sono, rispettivamente, le soluzioni diverse da $\overline{1}$ della congruenza $x^2 \equiv 1 \pmod{49}$ e della congruenza $x^3 \equiv 1 \pmod{49}$.

Dalla condizione $x^2 - 1 = (x-1)(x+1) \equiv 0 \pmod{49}$ troviamo: o $x - 1 \equiv 0 \pmod{49}$, che però darebbe come soluzione la classe di $\overline{1}$ che abbiamo escluso, o $x + 1 \equiv 0 \pmod{49}$, che effettivamente fornisce la classe di $-\overline{1}$ che ha ordine 2, oppure il sistema delle due equazioni $x - 1 \equiv 0 \pmod 7$ e $x + 1 \equiv 0 \pmod 7$, che non ha però alcuna soluzione.

Concludiamo che in $(\mathbb{Z}/49\mathbb{Z})^*$ abbiamo il solo elemento $-\overline{1}$ di ordine 2.

Se $x^3 \equiv 1 \pmod{49}$ allora $x^3 \equiv 1 \pmod 7$ e quest'ultima congruenza ha soluzione $x \equiv 1, 2, -3 \pmod 7$ per verifica diretta. Ne segue che le soluzioni della congruenza modulo 49 vanno cercate tra gli interi della forma $x = a + 7t$ con $a = 1$, 2 o -3 e $t \in \mathbb{Z}$. Osserviamo ora che $(a+7t)^3 \equiv a^3 + 21a^2t \pmod{49}$ e quindi, sostituendo si verifica che le uniche soluzioni di $x^3 \equiv 1 \pmod{49}$ sono $x \equiv 1, -19, 18 \pmod{49}$. In conclusione, ci sono 2 elementi di ordine 3 in $(\mathbb{Z}/49\mathbb{Z})^*$.

(ii) Gli omomorfismi da $\mathbb{Z}/6\mathbb{Z}$ in $(\mathbb{Z}/49\mathbb{Z})^*$ sono tanti quanti gli elementi di $(\mathbb{Z}/49\mathbb{Z})^*$ di ordine che divide 6 e questi sono esattamente le soluzioni di $x^6 \equiv 1 \pmod{49}$.

Le soluzioni di questa congruenza sono da ricercarsi tra gli interi che risolvono $x^6 \equiv 1 \pmod 7$ cioè tra gli interi della forma $x = a + 7t$ con $a \in \{1, 2, 3, 4, 5, 6\}$ e $t \in \mathbb{Z}$. Sostituendo si ottiene $(a+7t)^6 \equiv a^6 + 42a^5t \equiv 1 \pmod{49}$. Poiché $7 \mid a^6 - 1$ l'equazione diventa del tipo $6a^5t \equiv b \pmod 7$, con $b = (a^6 - 1)/7$, e, visto che $6a^5$ è invertibile modulo 7 per ogni a considerato, essa ha un'unica soluzione per t modulo 7. Possiamo concludere che l'equazione $x^6 \equiv 1 \pmod 7$ ha 6 soluzioni modulo 49.

Gli omomorfismi cercati sono quindi 6.

142. (i) Abbiamo $Z(H) \neq \varnothing$ perché esso contiene l'elemento neutro del gruppo. Se $x, y \in Z(H)$ allora, per ogni $h \in H$, vale $(xy)h = x(yh) = x(hy) = (xh)y = (hx)y = h(xy)$ cioè $xy \in Z(H)$; inoltre se $x \in Z(H)$ si ha $xh = hx$ per ogni $x \in H$, da cui si ottiene $hx^{-1} = x^{-1}xhx^{-1} = x^{-1}hxx^{-1} = x^{-1}h$ e quindi $x^{-1} \in Z(H)$. Possiamo concludere che $Z(H)$ è un sottogruppo di G.

(ii) Supponiamo che H sia normale in G e siano $x \in Z(H)$ e $g \in G$. Mostriamo che $gxg^{-1} \in Z(H)$: infatti

$$(gxg^{-1})h(gx^{-1}g^{-1}) = gx(g^{-1}hg)x^{-1}g^{-1} = g(g^{-1}hg)xx^{-1}g^{-1} = h$$

visto che $g^{-1}hg \in H$ e $x \in Z(H)$. Questo prova che $Z(H)$ è normale in G.

(iii) Sia $x \in Z(H)$, allora $f(x)f(h) = f(xh) = f(hx) = f(h)f(x)$ per ogni $h \in H$ e quindi per ogni $f(h) \in f(H)$. Abbiamo fatto vedere che ogni elemento di $f(Z(H))$ commuta con ogni elemento di $f(H)$, cioè che $f(Z(H)) \subseteq Z(f(H))$ come richiesto.

(iv) Basta prendere $G = \mathbb{Z}/2\mathbb{Z}$, $G' = \mathsf{S}_3$, $f(\overline{0}) = \mathrm{Id}$, $f(\overline{1}) = \sigma$ dove $\sigma(1) = 2$, $\sigma(2) = 1$, e $\sigma(3) = 3$, e $H = G$. Si verifica che $Z(f(G)) = \{\mathrm{Id}, \sigma\} \neq G'$.

143. (i) Vediamo che H è un sottogruppo di G. È chiaro che $e \in H$ in quanto l'elemento neutro ha ordine 1. Siano $a, b \in H$, e sia $\mathrm{ord}(a) = m$, $\mathrm{ord}(b) = n$; allora $(ab)^{mn} = a^{mn}b^{mn} = e$, quindi ab ha ordine finito e appartiene ad H. Infine, se $a \in H$ anche $a^{-1} \in H$ perché $\mathrm{ord}(a) = \mathrm{ord}(a^{-1})$ e questo finisce la dimostrazione che H è un sottogruppo.

Sia $G = \mathbb{C}^*$ allora $H = \{z \in \mathbb{C}^* \mid z^n = 1 \text{ per qualche } n\}$. Poiché per ogni $n \in \mathbb{N}$ il polinomio $x^n - 1$ ha n radici in $\mathbb{C}$ e queste appartengono ad H, si ha $|H| \geq n$ per ogni $n \in \mathbb{N}$, quindi H è infinito.

(ii) Sia gH un elemento di ordine finito in G/H e sia n il suo ordine. Allora da $g^nH = H$ otteniamo $g^n \in H$ e quindi esiste un intero d per cui $(g^n)^d = g^{nd} = e$, cioè $g \in H$. Quindi $gH = H$ e abbiamo provato che solo l'elemento neutro ha ordine finito in G/H.

(iii) In un isomorfismo di gruppi gli elementi di ordine finito corrispondono tra loro. Ma, per quanto provato nel punto precedente, G/H ha solo l'elemento neutro di ordine finito e quindi in G abbiamo $H = \{e\}$.

(iv) Sia $\varphi : G \longrightarrow \mathbb{Z}$ un omomorfismo, sia $x \in H$ con $n = \mathrm{ord}(x)$. Allora $\mathrm{ord}(\varphi(x)) \,|\, n$ cioè $\varphi(x)$ è un elemento di ordine finito del gruppo $\mathbb{Z}$. Poiché 0 è l'unico elemento di ordine finito di $\mathbb{Z}$, necessariamente $\varphi(x) = 0$, cioè $x \in \mathrm{Ker}(\varphi)$.

144. (i) Sia $H_1 \times H_2$ che $G_1 \times G_2$ sono gruppi con le operazioni componente per componente. Poiché le operazioni su H_1 e H_2 sono restrizione rispettivamente di quelle su G_1 e G_2, segue che $H_1 \times H_2$ è un sottogruppo di $G_1 \times G_2$.

Sia $(x, y) \in G_1 \times G_2$, allora $(x, y)(H_1 \times H_2)(x, y)^{-1} = (x, y)(H_1 \times H_2)(x^{-1}, y^{-1}) = xH_1x^{-1} \times yH_2y^{-1} = H_1 \times H_2$ perché H_1 è normale in G_1 e H_2 è normale in G_2. Quindi $H_1 \times H_2$ è normale in $G_1 \times G_2$.

(ii) Per ogni $(x, y) \in \mathcal{H}$ si ha $x = \pi_1(x, y) \in \pi_1(\mathcal{H})$ e $y = \pi_2(x, y) \in \pi_2(\mathcal{H})$, quindi $(x, y) \in \pi_1(\mathcal{H}) \times \pi_2(\mathcal{H})$.

(iii) Sia $(x, y) \in \pi_1(\mathcal{H}) \times \pi_2(\mathcal{H})$, allora esistono $a \in G_1$ e $b \in G_2$ per cui (x, b), $(a, y) \in \mathcal{H}$. Siano $h, k \in \mathbb{Z}$ tali che $hm + kn = 1$; indicando rispettivamente con e_1 ed e_2 gli elementi neutri di G_1 e G_2, si ha $(x, b)^{kn} = (x^{kn}, b^{kn}) = (x^{1-hm}, e_2) = (x, e_2) \in \mathcal{H}$ e $(a, y)^{hm} = (a^{hm}, y^{1-kn}) = (e_1, y) \in \mathcal{H}$ da cui segue che $(x, y) = (x, e_2)(e_1, y) \in \mathcal{H}$. Questo e il punto precedente danno l'uguaglianza cercata.

145. (i) Trattandosi di gruppi finiti vale $[G_1 : H] = |G_1|/|H|$ e anche $[f(G_1) : f(H)] = |f(G_1)|/|f(H)|$. Il Teorema di Omomorfismo, applicato all'omomorfismo $f : G_1 \longrightarrow G_2$ e alla sua restrizione ad H, $f_{|H} : H \longrightarrow G_2$, assicura che $f(G_1) \simeq G_1/\operatorname{Ker}(f)$ e $f(H) \simeq H/\operatorname{Ker}(f_{|H})$. Poiché $\operatorname{Ker}(f) \subseteq H$, si ha $\operatorname{Ker}(f_{|H}) = \operatorname{Ker}(f)$, e passando alle cardinalità

$$\begin{aligned}[f(G_1) : f(H)] &= \big|f(G_1)\big|/\big|f(H)\big| \\ &= \big(|G_1|/|\operatorname{Ker}(f)|\big)\big(\operatorname{Ker}(f)|/|H|\big) \\ &= |G_1|/|H| = [G_1 : H].\end{aligned}$$

(ii) Se $\operatorname{Ker}(f) \not\subseteq H$ il risultato del primo punto in generale non è piú vero. Siano infatti $G_1 = G_2 = \mathbb{Z}/2\mathbb{Z}$, $H = \{0\}$ e f l'omomorfismo nullo. Si ha quindi $[G_1 : H] = 2$ mentre $[f(G_1) : f(H)] = [\{0\} : \{0\}] = 1$.

(iii) Se $G_1 = \mathbb{Z}$ e G_2 è un gruppo finito si ha che $\operatorname{Ker}(f) = n\mathbb{Z}$ con $n > 0$. Sia $H = m\mathbb{Z}$, da $H \supseteq \operatorname{Ker}(f)$ abbiamo $m \,|\, n$ e, in particolare, $|H/\operatorname{Ker}(f)| = n/m$ inoltre $[G_1 : H] = |G_1/H| = m$. Allora argomentando come nel primo punto, si ottiene

$$\begin{aligned}[f(G_1) : f(H)] &= \big|f(G_1)\big|/\big|f(H)\big| \\ &= \big(\big|G_1/\operatorname{Ker}(f)\big|\big) : \big(\big|H/\operatorname{Ker}(f)\big|\big) \\ &= nm/n \\ &= m \\ &= [G_1 : H].\end{aligned}$$

Il risultato continua, quindi, a rimanere vero anche in questo caso.

146. (i) Essendo intersezione di sottogruppi anche N è un sottogruppo di G. Sia $g \in G$ e sia M un sottogruppo di G, si ha che M è massimale se e solo se gMg^{-1} è massimale, infatti: $M \subsetneq H$ se e solo se $gMg^{-1} \subsetneq gHg^{-1}$ e, inoltre, $H = G$ se solo se $gHg^{-1} = G$. Da questo segue che l'insieme dei sottogruppi massimali di G è invariante per coniugio, allora anche l'intersezione N lo è, quindi N è normale.

(ii) I sottogruppi di $\mathbb{Z}/n\mathbb{Z}$ sono i gruppi $d\mathbb{Z}/n\mathbb{Z}$ con $d \,|\, n$. Poiché $d\mathbb{Z}/n\mathbb{Z} \subseteq m\mathbb{Z}/n\mathbb{Z}$ se e solo se $m \,|\, d$, i sottogruppi massimali di $\mathbb{Z}/n\mathbb{Z}$ sono i gruppi $p\mathbb{Z}/n\mathbb{Z}$ al variare di p tra i divisori primi del numero n. Ne segue che, se $n = p_1^{e_1} \cdots p_r^{e_r}$,

$$N = \bigcap_{i=1}^{r} p_i\mathbb{Z}/n\mathbb{Z} = p_1 \cdots p_r\mathbb{Z}/n\mathbb{Z}.$$

In particolare N è banale se e solo se $p_1 p_2 \cdots p_r = n$, cioè se e solo se n è libero da quadrati.

(iii) Da quanto appena provato si ha che per $n = 100$ risulta $N = 10\mathbb{Z}/100\mathbb{Z}$.

147. Sia $\pi : G \longrightarrow G/N$ l'omomorfismo di proiezione, cioè l'applicazione definita da $\pi(g) = gN$ per ogni $g \in G$, e sia $F = \pi \circ f : G \longrightarrow G/N$.

L'applicazione F è un omomorfismo suriettivo in quanto composizione di omomorfismi suriettivi e $\mathrm{Ker}(F) = \{g \in G \mid F(g) = f(g)N = N\} = N$ perché $f(g) \in N$ se e solo se $g \in N$.

Per il teorema di omomorfismo applicato a F, l'applicazione $\varphi : G/N \longrightarrow G/N$ definita da $\varphi(gN) = f(g)N$ è ben definita ed è un isomorfismo.

148. (i) Il gruppo G è isomorfo a $(\mathbb{Z}/5\mathbb{Z})^* \times (\mathbb{Z}/7\mathbb{Z})^*$; visto che 5 e 7 sono numeri primi, $G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ e infine, poiché $(2, 3) = 1$, $G \simeq H \times K$, dove $H = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ e $K = \mathbb{Z}/3\mathbb{Z}$.

Un elemento $(h, k) \in H \times K$ ha per ordine il minimo comune multiplo degli ordini di h e k.

Ogni elemento di $h = (h_1, h_2) \in H$ soddisfa banalmente $4h = (\overline{0}, \overline{0})$; l'equazione $2h = (\overline{0}, \overline{0})$ ha 4 soluzioni: $(\overline{0}, \overline{0})$, $(\overline{0}, \overline{1})$, $(\overline{2}, \overline{0})$, $(\overline{2}, \overline{1})$. Infine $(\overline{0}, \overline{0})$, che è l'elemento neutro, ha ordine 1. Per differenza, H ha $8 - 4 = 4$ elementi di ordine 4, $4 - 1 = 3$ elementi di ordine 2 ed un elemento di ordine 1.

In K ci sono 2 elementi di ordine 3 ed un elemento di ordine 1, cioè l'elemento neutro.

Pertanto in G ci sono: $4 \cdot 2 = 8$ elementi di ordine 12, $4 \cdot 1 = 4$ elementi di ordine 4, $3 \cdot 2 = 6$ elementi di ordine 6, $3 \cdot 1 = 3$ elementi di ordine 2, $1 \cdot 2 = 2$ elementi di ordine 2 ed un elemento di ordine 1. Non ci sono elementi di ordine n per ogni $n \neq 1, 2, 3, 4, 6, 12$.

(ii) Dimostriamo innanzitutto che un sottogruppo C di G di ordine 6 deve essere ciclico. Infatti, supponiamo per assurdo che C non abbia elementi di ordine 6: l'ordine degli elementi diversi dall'elemento neutro, che deve essere un divisore di 6, sarà allora solo 2 o 3.

Gli elementi di G diversi dall'elemento neutro non possono avere tutti ordine 2, perché altrimenti C sarebbe un sottogruppo di $H \times \{\overline{0}\}$, cosa impossibile visto che $6 \nmid 8$. Similmente, non possono avere tutti ordine 3, perché altrimenti C sarebbe un sottogruppo di $\{\overline{0}\} \times K$, che ha ordine 3.

Quindi esistono almeno un elemento di ordine 2, necessariamente della forma $(h, \overline{0})$ con $h \in H$, ed un elemento di ordine 3, necessariamente della forma $(\overline{0}, k)$ con $k \in K$. Ma allora (h, k) ha ordine 6, contro l'ipotesi.

Poiché un gruppo ciclico di ordine 6 contiene esattamente $\phi(6) = 2$ elementi di ordine 6 e G possiede 6 elementi di ordine 6, G ha $6/2 = 3$ sottogruppi di ordine 6.

149. (i) Sia $N = \{x \in G \mid f(x) = g(x)\}$ e indichiamo con e l'elemento neutro di G. Osserviamo che, per prima cosa, $f(e) = g(e) = \overline{0}$, quindi $e \in N$. Poi, se $x, y \in N$, quindi $f(x) = g(x)$ e $f(y) = g(y)$, allora $f(xy) = f(x) + f(y) = g(x) + g(y) = g(xy)$, e $xy \in N$. Infine se $x \in N$, e quindi $f(x) = g(x)$, allora $f(x^{-1}) = -f(x) = -g(x) = g(x^{-1})$, cioè $x^{-1} \in N$. Abbiamo provato che N è un sottogruppo di G.

Inoltre siano $y \in G$, $x \in N$; usando che $\mathbb{Z}/12\mathbb{Z}$ è abeliano si ha $f(yxy^{-1}) = f(y) + f(x) - f(y) = f(x) = g(x) = g(y) + g(x) - g(y) = g(yxy^{-1})$ e pertanto $yxy^{-1} \in N$.

⟦La stessa dimostrazione funziona con un qualsiasi gruppo abeliano al posto di $\mathbb{Z}/12\mathbb{Z}$.⟧

(ii) Si noti che H è un sottogruppo normale di G, in quanto $\langle(123)\rangle$ è normale in S_3, perché ha indice 2. La condizione $f(h) = \overline{0}$ per ogni $h \in H$ si può riscrivere

come $H \subseteq \mathrm{Ker}(f)$. Quindi gli omomorfismi con questa proprietà corrispondono biunivocamente agli omomorfismi $\varphi : G/H \longrightarrow \mathbb{Z}/12\mathbb{Z}$.

Ora $G/H \simeq \langle \overline{(12)} \rangle \times \langle \overline{1} \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Ne segue che, a loro volta, gli omomorfismi $\varphi : G/H \longrightarrow \mathbb{Z}/12\mathbb{Z}$ corrispondono biunivocamente agli omomorfismi $\psi : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}/12\mathbb{Z}$ il cui nucleo contiene $2\mathbb{Z} \times 2\mathbb{Z}$.

Gli omomorfismi $\psi : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}/12\mathbb{Z}$ sono tutti e soli della forma $\psi(m, n) = \overline{ma + nb}$, con $a, b \in \mathbb{Z}/12\mathbb{Z}$. Il nucleo di un tale omomorfismo contiene $2\mathbb{Z} \times 2\mathbb{Z}$ se e solo se $\psi(2, 0) = \psi(0, 2) = \overline{0}$, che corrisponde a imporre $\overline{2a} = \overline{2b} = \overline{0}$, ossia $\overline{a} = \overline{6a'}, \overline{b} = \overline{6b'}$ con $a', b' \in \{0, 1\}$. Quindi gli omomorfismi cercati sono 4, e sono descritti dalle possibili scelte di (a', b').

150. Osserviamo innanzitutto che $G \simeq H \times K = (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$, un prodotto diretto di due gruppi ciclici di ordine $p-1$ e $q-1$, rispettivamente. Vista la struttura di gruppo di un prodotto diretto, si avrà $G^{(2)} \simeq H^{(2)} \times K^{(2)}$ e $G^{(3)} \simeq H^{(3)} \times K^{(3)}$; dove $H^{(2)}$, $H^{(3)}$, $K^{(2)}$ e $K^{(3)}$ sono definiti per H e K analogamente a G.

Denotiamo con φ e ψ gli omomorfismi di H in sé definiti da $\varphi(x) = x^2$, $\psi(x) = x^3$; tratteremo poi K allo stesso modo. I sottogruppi $H^{(2)}, H^{(3)}$ sono le immagini di questi omomorfismi. Per quanto riguarda i nuclei, essi sono costituiti dalle soluzioni delle equazioni $x^2 \equiv 1 \pmod{p}$, $x^3 \equiv 1 \pmod{p}$. La prima equazione ha per soluzioni $x \equiv \pm 1 \pmod{p}$ e la seconda ha 3 soluzioni o una soluzione secondo che H abbia o meno elementi di ordine 3, ossia secondo che 3 divida $p-1$ o no. Osserviamo inoltre che per $p = 2$ le due soluzioni della prima equazione coincidono.

Vista la relazione fra l'ordine del nucleo e l'ordine dell'immagine di un omomorfismo, e sapendo che ogni sottogruppo di un gruppo ciclico è ciclico, se ne deduce che: $H^{(2)}$ è un gruppo ciclico di ordine $(p-1)/2$ se $p > 2$ o di ordine 1 se $p = 2$ e $H^{(3)}$ è un gruppo ciclico di ordine $(p-1)/(3, p-1)$.

Possiamo quindi concludere quanto segue. L'ordine di $G^{(2)}$ è $(p-1)/2 \cdot (q-1)/2$ se $p > 2$, o $(q-1)/2$ se $p = 2$, e l'ordine di $G^{(3)}$ è $(p-1)/(3, p-1) \cdot (q-1)/(3, q-1)$. Il sottogruppo $G^{(2)}$, che è un prodotto diretto di gruppi ciclici, è ciclico se e solo se gli ordini dei due fattori sono primi fra loro, ossia se e solo se $((p-1)/2, (q-1)/2) = 1$ se $p > 2$ e per ogni q se $p = 2$. Analogamente, $G^{(3)}$ è ciclico se e solo se gli ordini dei suoi fattori sono primi fra loro. Si noti però che tali ordini sono sempre pari, salvo il caso $p = 2$, per cui l'ordine del primo fattore è 1. Quindi questo gruppo è ciclico se $p = 2$ e non lo è se $p > 2$.

151. (i) Poiché G è un gruppo, è evidente che $H + K \subseteq G$. Per l'inclusione opposta, osserviamo che, dato $x \in G$ e indicata con $\overline{x}_H$ la sua proiezione in G/H, si ha $m\overline{x}_H = \overline{e}_H$ visto che G/H ha ordine m. Questo prova che, per ogni $x \in G$, vale $mx \in H$ e, analogamente, $nx \in K$. Ora siano a, b due interi tali che $am + bn = 1$ e sia $x \in G$. Si ha $x = amx + bnx \in H + K$, e quindi la tesi è dimostrata.

(ii) Consideriamo l'applicazione $f : G \longrightarrow G/H \times G/K$ data da $f(x) = (\overline{x}_H, \overline{x}_K)$. Essa è evidentemente un omomorfismo. Il nucleo di f è dato dall'insieme degli elementi x per cui $(\overline{x}_H, \overline{x}_K) = (\overline{e}_H, \overline{e}_K)$, ossia è uguale a $H \cap K$.

Inoltre, f è un omomorfismo suriettivo. Infatti, sia $(\overline{x}_H, \overline{y}_k) \in G/H \times G/K$; osservando che, con le notazioni precedenti, $bn \equiv 1 \pmod{m}$, $bn \equiv 0 \pmod{n}$ e

$am \equiv 0 \pmod{m}, am \equiv 1 \pmod{n}$, si ha $f(bnx + amy) = f(bnx) + f(amy) = (\overline{x}_H, \overline{e}_K) + (\overline{e}_H, \overline{y}_K) = (\overline{x}_H, \overline{y}_K)$.

Otteniamo l'isomorfismo cercato usando il Teorema di Omomorfismo.

152. Un omomorfismo $f : G \longrightarrow G$ è indotto da un omomorfismo $g : \mathbb{Z} \times \mathbb{Z} \longrightarrow G$ per cui $20\mathbb{Z} \times 8\mathbb{Z} \subseteq \mathrm{Ker}(g)$. Inoltre, scelti comunque x, y in G, c'è uno ed un solo omomorfismo $g : \mathbb{Z} \times \mathbb{Z} \longrightarrow G$ tale che $g(1,0) = x$, $g(0,1) = y$; quest'omomorfismo è infatti definito ponendo $g(a,b) = ax + by$.

La condizione sul nucleo di g è equivalente a $g(20,0) = 20x = (\overline{0}, \overline{0})$ e $g(0,8) = 8y = (\overline{0}, \overline{0})$.

Le scelte possibili per x sono tutte le coppie rappresentate da interi (x_1, x_2) tali che $20x_1 \equiv 0 \pmod{20}$ e $20x_2 \equiv 0 \pmod{8}$. La prima equazione è verificata per ogni valore di x_1, mentre la seconda equazione è verificata se e solo se $x_2 \equiv 0 \pmod{2}$, e cioè per 4 classi modulo 8. In totale i valori possibili per x sono dunque $20 \cdot 4 = 80$.

Analogamente, le scelte possibili per y sono tutte le coppie rappresentate da interi (y_1, y_2) tali che $8y_1 \equiv 0 \pmod{20}$ e $8y_2 \equiv 0 \pmod{8}$. La prima equazione equivale a $y_1 \equiv 0 \pmod{5}$, e dunque ha 4 soluzioni modulo 20, mentre la seconda equazione è sempre verificata. In totale ci sono dunque $4 \cdot 8 = 32$ valori possibili per y.

Il numero degli omomorfismi cercato è quindi $80 \cdot 32 = 2560$.

(i) Il nucleo di f_n è costituito dalle coppie (x_1, x_2) tali che $nx_1 \equiv 0 \pmod{20}$ e $nx_2 \equiv 0 \pmod{8}$. La prima equazione ha per soluzione $x_1 \equiv 0 \pmod{20/(n,20)}$ e la seconda $x_2 \equiv 0 \pmod{8/(n,8)}$.

Il nucleo di f_n è quindi il prodotto diretto di un gruppo ciclico di ordine $(n,20)$ per un gruppo ciclico di ordine $(n,8)$. Il prodotto diretto di due gruppi ciclici finiti è ciclico se e solo se gli ordini dei due gruppi sono primi fra loro.

Visto che, nel nostro caso, se n è dispari l'ordine del secondo gruppo è uguale a 1, mentre se n è pari gli ordini dei due gruppi sono entrambi pari, il gruppo prodotto è ciclico se e solo se n è dispari.

(ii) Per il Teorema di Omomorfismo, l'immagine di f_n è isomorfa a $G/\mathrm{Ker}(f_n)$, cioè al prodotto di due gruppi ciclici aventi ordine $20/(n,20)$ e $8/(n,8)$ rispettivamente. Poiché $(20,8) = 4$, questi ordini sono primi fra loro se e solo se 4 divide sia $(n,20)$ che $(n,8)$, cioè se e solo se $4 \mid n$.

153. (i) Sia $x \in G$ tale che la sua proiezione $\overline{x}$ in G/H generi G/H. In particolare quindi $\mathrm{ord}(\overline{x}) = n$. Allora da $\mathrm{ord}(\overline{x}) \mid \mathrm{ord}(x)$ abbiamo $\mathrm{ord}(x) = nk$ per qualche intero positivo k.

Sia ora y un generatore di H e sia $z = x^k$. Abbiamo $\mathrm{ord}(y) = m$, $\mathrm{ord}(z) = n$ e vogliamo dimostrare che $\mathrm{ord}(yz) = mn$, ossia che yz è un generatore di G. Poiché $yz \in G$, è ovvio che $\mathrm{ord}(yz) \mid mn = |G|$.

Supponiamo ora che d sia un intero positivo per cui $(yz)^d = e$. Poiché G è abeliano, possiamo scrivere $y^d z^d = e$ e anche $y^d = z^{-d}$.

Esaminando quest'ultima uguaglianza, si vede che y^d appartiene ad H e z^{-d} appartiene al sottogruppo generato da z. Questi due sottogruppi hanno per intersezione il solo elemento neutro, avendo ordini primi tra loro, quindi necessariamente $y^d = e$

e $z^d = e^{-1} = e$. Poiché y e z sono di ordine m ed n rispettivamente, si deve avere $m \mid d$ ed $n \mid d$ e, visto che $(m, n) = 1$, si ha $mn \mid d$, e quindi la tesi è dimostrata.

(ii) Una serie di esempi è data dai gruppi della forma $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ con $(m, n) > 1$. Prendendo $H = \mathbb{Z}/m\mathbb{Z} \times \{e\}$ si ha che $G/H \cong \mathbb{Z}/n\mathbb{Z}$. Infatti $\mathbb{Z}/n\mathbb{Z}$ è l'immagine della proiezione canonica di G sul secondo fattore, e questa proiezione ha per nucleo esattamente H. Quindi H e G/H sono ciclici ma G non lo è, in virtù dell'ipotesi $(m, n) > 1$.

In particolare, un esempio specifico è $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

154. (i) Poiché in un gruppo di ordine n ogni elemento elevato alla n dà l'elemento neutro, si ha $f_{n-1}(x) = x^{n-1} = x^{-1}$. Se f_{n-1} è un omomorfismo, allora per ogni $x, y \in G$ si ha $(xy)^{-1} = x^{-1}y^{-1}$. Facendo l'inverso di entrambi i membri si ottiene $xy = yx$.

(ii) Se f_8 è un omomorfismo, allora lo è anche $f_8 \circ f_8 = f_{64}$. Ma dal fatto che per ogni $x \in G$ si ha $x^{62} = e$ si ricava che $f_{64}(x) = f_2(x) = x^2$. Se f_2 è un omomorfismo, allora per ogni $x, y \in G$, si ha $(xy)^2 = x^2y^2$, ossia $xyxy = xxyy$. Moltiplicando a sinistra per x^{-1} e a destra per y^{-1} si ottiene $yx = xy$.

(iii) Sia $G = \mathsf{S}_3$ e $k = 2$. Allora $f_2((12)(13)) = f_2((132)) = (132)^2 = (123)$ mentre $f((12))f((13)) = (12)^2(13)^2 = e \cdot e = e$.

155. Usiamo la notazione additiva, e denotiamo con 0 l'elemento neutro di G.

(i) Dimostriamo innanzitutto che G_p è un sottogruppo di G. L'elemento neutro è in G_p in quanto $\mathrm{ord}(0) = 1$.

Siano $x, y \in G_p$, e sia $\mathrm{ord}(x) = p^k$, $\mathrm{ord}(y) = p^h$. Se $m = \max\{k, h\}$ abbiamo $p^m(x + y) = p^m x + p^m y = 0$, quindi l'ordine di $x + y$ è un divisore di p^m e quindi una potenza di p.

Infine, per ogni intero r si ha $rx = 0$ se e solo se $r(-x) = 0$. Abbiamo così provato che G_p è un sottogruppo.

Sia ora q un primo che divide l'ordine di G_p. Per il Teorema di Cauchy esiste un elemento $x \in G_p$ di ordine q, ma per definizione di G_p abbiamo che $q = p$ e questo prova che l'ordine di G_p è una potenza di p.

(ii) Sia $x + G_p$ un elemento del gruppo quoziente G/G_p, e sia $\mathrm{ord}(x) = r$. Scriviamo r nella forma $r = p^k m$, dove $(m, p) = 1$. Allora $p^k(mx) = 0$, da cui $mx \in G_p$. Ne segue che $m(x + G_p) = mx + G_p = G_p$ è la classe dell'elemento neutro in G/G_p, ossia $\mathrm{ord}(x + G_p)$ è un divisore di m. Esso è, quindi, relativamente primo con p.

(iii) Poniamo $|G_p| = p^{a'}$, $|G_q| = q^{b'}$, per qualche $a', b' \in \mathbb{N}$. Poiché si tratta di sottogruppi di G, abbiamo $a' \le a$, $b' \le b$. Consideriamo l'omomorfismo $f : G \to G$ dato da $f(x) = p^a x$. Mostriamo che $\mathrm{Ker}(f) = G_p$: infatti se $x \in \mathrm{Ker}(f)$ allora il suo ordine è un divisore di p^a e, se $x \in G_p$, allora $p^{a'}x = 0$ e, a maggior ragione, $p^a x = 0$. Per il teorema di omomorfismo, l'immagine di f è isomorfa a G/G_p che, per il punto (ii), contiene solo elementi di ordine potenza di q. Pertanto $\mathrm{Im}(f) \le G_q$. In particolare $|\mathrm{Im}(f)|$ è una potenza di q, diciamo $|\mathrm{Im}(f)| = q^{b''}$, con $b'' \in \mathbb{N}$. Abbiamo

$$p^a q^b = |G| = |\mathrm{Ker}(f)| \cdot |\mathrm{Im}(f)| = p^{a'} q^{b''},$$

da cui $a = a'$ e $b = b''$. Poiché $b'' \leq b' \leq b$, ne segue che $b'' = b' = b$ e dunque $G/G_p \simeq \mathrm{Im}(f) = G_q$.

156. Sia $q = a/b$ un numero razionale, con $(a, b) = 1$ e $b = 2^r 5^s h$ con $r, s \geq 0$, $h > 0$ e $(h, 10) = 1$. Dalla definizione di L abbiamo che $mq \in L$ se e solo se $h \mid m$; infatti il fattore m deve semplificare ogni primo diverso da 2 e 5 che appaia nel denominatore di q. In particolare, $x = q + L$ ha ordine k in $\mathbb{Q}/L$ se e solo se $h = k$; inoltre, x risolve $kx = 0$ se e solo se $h \mid k$.

Occupiamoci, per prima cosa, di rispondere alle domande (i) e (ii) nel caso $(k, 10) = 1$.

Osserviamo che $1/k + L$ ha ordine k in $\mathbb{Q}/L$, per quanto visto sopra. Inoltre tutti gli elementi del gruppo ciclico G generato da $1/k + L$ in $\mathbb{Q}/L$ risolvono l'equazione $kx = 0$.

Viceversa, sia x una qualsiasi soluzione di questa equazione, vogliamo provare che $x \in G$. Per quanto osservato in precedenza, avremo $x = q + L$, $q = a/(2^r 5^s h)$ con $h \mid k$.

Consideriamo ora la congruenza $ht + a \equiv 0 \pmod{2^r 5^s}$ in t. Essa è risolubile visto che $(h, 10) = 1$; sia $t_0 \in \mathbb{Z}$ una sua soluzione e sia $ht_0 + a = c2^r 5^s$ con $c \in \mathbb{Z}$. Allora

$$q - \frac{c}{h} = \frac{a}{2^r 5^s h} - \frac{ht_0 + a}{2^r 5^s h} = \frac{t_0}{2^r 5^s} \in L$$

e quindi $x = q + L = c/h + L$ appartiene al sottogruppo generato da $1/h + L$ che è un sottogruppo di G. Abbiamo quindi provato che G è l'insieme delle soluzioni di $kx = 0$ in $\mathbb{Q}/L$. Pertanto il numero di tali soluzioni è k e il numero di elementi di ordine k è $\phi(k)$ visto che G è un gruppo ciclico.

Vediamo ora il caso $(k, 10) > 1$. Possiamo scrivere $k = 2^r 5^s k_1$ con $(k_1, 10) = 1$. Dalla discussione iniziale sull'ordine in $\mathbb{Q}/L$ segue che ogni elemento ha ordine primo con 10. In particolare non ci sono elementi di ordine k e le soluzioni di $kx = 0$ sono le stesse di $k_1 x = 0$; abbiamo quindi k_1 soluzioni.

157. (i) Sì, esistono sottogruppi ordine 3: basta prendere rotazioni di multipli di $2\pi/3$ intorno ad una retta congiungente due vertici diametralmente opposti del cubo.

(ii) In G ci sono due tipi di movimenti: quelli che preservano la figura e quelli in cui i segmenti paralleli ai lati vengono ruotati di $\pi/2$. Si vede subito infatti che, se viene ruotato il segmento all'interno di una faccia allora devono essere ruotati anche quelli delle facce adiacenti, in quanto segmenti interni a due facce adiacenti non si intersecano nei loro estremi.

I movimenti del primo tipo formano il sottogruppo H. Inoltre esistono movimenti del secondo tipo; basta considerare, ad esempio, una rotazione di $\pi/2$ intorno all'asse che congiunge i centri di due facce opposte. Osserviamo poi che i movimenti del secondo tipo sono una classe laterale di H. Infatti, se α e β sono due movimenti del secondo tipo, il movimento $\alpha \circ \beta^{-1}$ preserva la figura, quindi $\alpha \circ \beta^{-1} \in H$.

Pertanto l'indice di H in G è uguale a 2.

(iii) Sappiamo che H è un sottogruppo di indice 2 in G allora H è un sottogruppo normale di G.

158. (i) Ogni elemento di G genera un sottogruppo ciclico. Inoltre un sottogruppo ciclico di ordine d, è generato da $\phi(d)$ elementi distinti. Pertanto il numero dei sottogruppi ciclici di un gruppo finito G è dato dall'espressione

$$\sum_{d\,||G|} \frac{1}{\phi(d)} \cdot (\text{numero di elementi di ordine } d).$$

Nel caso del gruppo G, ogni $x \in G$ verifica $6x = 0$, quindi l'ordine di x può essere solo $1, 2, 3$, o 6. L'unico elemento di ordine 1 è l'elemento neutro. Un elemento $x = (a, b)$ di ordine 2 verifica $(2a, 2b) = (0, 0)$, e quest'ultima equazione ha per soluzione $a = \overline{0}, \overline{3}$, $b = \overline{0}, \overline{3}$. Togliendo da queste quattro possibilità l'elemento neutro, che è l'unico che non ha ordine 2, si ottengono $4 - 1 = 3$ elementi di ordine 2.

In modo perfettamente analogo si contano gli elementi di ordine 3: essi sono $9 - 1 = 8$. Tutti gli altri elementi, che sono in numero di $36 - 1 - 3 - 8 = 24$ elementi, hanno ordine uguale a 6. La nostra espressione quindi diventa

$$\frac{1}{\phi(1)} + \frac{3}{\phi(2)} + \frac{8}{\phi(8)} + \frac{24}{\phi(6)} = 1 + 3 + 2 + 12 = 18.$$

(ii) È chiaro che, se $\text{ord}(x) = 1, 2, 3, 6$, allora $|G/\langle x\rangle|$ sarà rispettivamente uguale a 36, 18, 12, 6.

Ricordiamo ora che, se $y \in G$ e $\pi : G \longrightarrow G/\langle x\rangle$ è la proiezione canonica, si ha, come per ogni omomorfismo, $\text{ord}(\pi(y)) \mid \text{ord}(y)$. Poiché G non ha elementi di ordine 36, 18, 12, l'unico caso possibile è che $\text{ord}(x) = |G/\langle x\rangle| = 6$. In questo caso, inoltre, $G/\langle x\rangle$ è necessariamente ciclico, in quanto possiede un elemento a di ordine 2, un elemento b di ordine 3, e la loro somma $a + b$ ha necessariamente ordine 6. Quindi il numero cercato è il numero di elementi di G di ordine 6 che, come visto prima, è uguale a 24.

159. (i) Dividiamo $\mathbb{Z}/60\mathbb{Z}$ nei venti sottoinsiemi disgiunti $A_0, A_1, \ldots, A_{19}$ con $A_h = \{\overline{h}, \overline{h+20}, \overline{h+40}\}$ per $h = 0, 1, \ldots, 19$.

L'insieme G è quindi dato da tutte le possibili permutazioni di $\mathbb{Z}/60\mathbb{Z}$ che mandano A_h in sé per ogni $h = 0, 1, \ldots, 19$. Da questa descrizione vediamo che G è un gruppo ed è isomorfo al prodotto diretto $\mathsf{S}(A_0) \times \mathsf{S}(A_1) \times \cdots \times \mathsf{S}(A_{19}) \simeq \mathsf{S}_3^{\times 20}$ dei gruppi di permutazione degli insiemi $A_0, A_1, \ldots, A_{19}$. In particolare G ha 6^{20} elementi.

(ii) È chiaro che G non ha sottogruppi di ordine 10 in quanto 10 non divide 6^{20}.

Osservando poi che l'ordine di un elemento in un prodotto diretto è il minimo comune multiplo degli ordini delle coordinate dell'elemento, e, visto che gli elementi di S_3 hanno ordini 1, 2, o 3, abbiamo: esistono sottogruppi ciclici di ordine 6, non esistono sottogruppi ciclici di ordine 8 e 12.

Esistono invece sottogruppi di ordine 8: sia infatti H un sottogruppo di ordine 2 in S_3, allora $H \times H \times H \times \text{Id} \times \text{Id} \times \cdots \times \text{Id}$ è un sottogruppo di ordine 8 in $\mathsf{S}_3^{\times 20}$. Allo stesso modo, se K è un sottogruppo di ordine 3 in S_3 allora $K \times H \times H \times \text{Id} \times \cdots \times \text{Id}$ è un sottogruppo di ordine 12 in $\mathsf{S}_3^{\times 20}$.

160. Sia $\varphi : G \longrightarrow 3G$ l'applicazione definita da $\varphi(x) = 3x$ per ogni $x \in G$. Osserviamo che φ è un omomorfismo, in quanto, usando che G è abeliano, si ha $\varphi(x + y) = 3(x + y) = 3x + 3y = \varphi(x) + \varphi(y)$.

Sia H un sottogruppo di G tale che $(|H|, 3) = 1$, e consideriamo la restrizione $\psi = \varphi_{|H}$ ad H dell'omomorfismo φ. Il nucleo di ψ è costituito dagli elementi $h \in H$ tali che $3h = 0$, ossia dagli elementi di H che hanno per ordine un divisore di 3. Poiché 3 non divide l'ordine di H, in H non ci sono elementi di ordine 3 e dunque il nucleo di ψ è costituito dal solo elemento neutro. Ne segue che ψ è iniettivo e quindi H è isomorfo alla sua immagine $\psi(H)$. Ma $\psi(H)$ è un sottogruppo di un gruppo ciclico, quindi è esso stesso ciclico. Allora anche H è ciclico.

161. Un omomorfismo $f : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$ è completamente determinato una volta assegnato $f(1) = (a, b) \in \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$, con la condizione $\mathrm{ord}(a, b) \mid n = \mathrm{ord}(1)$. Si tratta, quindi, di contare gli elementi $(a, b) \in \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$ tali che $n(a, b) = 0$.

Per $n = 0$, cioè nel caso di omomorfismi $\mathbb{Z} \longrightarrow \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$, tutte le scelte di (a, b) verificano la condizione richiesta e, quindi, ci sono 200 omomorfismi, nessuno dei quali è iniettivo perché $\mathbb{Z}$ è infinito mentre il codominio è finito.

Sia ora $n \geq 1$. Dobbiamo contare gli elementi $(a, b) \in \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$ tali che $na = \overline{0}$ e $nb = \overline{0}$, cioè le soluzioni delle congruenze $na \equiv 0 \pmod{10}$ e $nb \equiv 0 \pmod{20}$. Ora

$$na \equiv 0 \pmod{10} \iff a \equiv 0 \left(\mathrm{mod}\ \frac{10}{(n, 10)}\right)$$

e questa equazione ha esattamente $(n, 10)$ soluzioni in $\mathbb{Z}/10\mathbb{Z}$. Analogamente l'equazione $nb \equiv 0 \pmod{20}$ ha esattamente $(n, 20)$ soluzioni in $\mathbb{Z}/20\mathbb{Z}$. In tutto le coppie (a, b) che verificano la condizione richiesta, e quindi gli omomorfismi cercati, sono $(n, 10)(n, 20)$.

La condizione affinché un omomorfismo tra quelli descritti sia iniettivo è che $\mathrm{ord}(a, b) = \mathrm{ord}(1) = n$; gli omomorfismi iniettivi sono quindi tanti quanti gli elementi di ordine n in $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$. Allora, condizione necessaria affinché esistano omomorfismi iniettivi è che $n \mid 20$, cioè che $n = 1, 2, 4, 5, 10, 20$ e in tal caso gli omomorfismi iniettivi sono tanti quanti gli elementi di ordine n in $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$.

Calcoliamo, quindi, il numero d_n di elementi $(a, b) \in \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$ di ordine n, per ogni possibile valore di n, ricordando che $\mathrm{ord}(a, b)$ è il minimo comune multiplo di $\mathrm{ord}(a)$ e $\mathrm{ord}(b)$ e che, se $d \mid m$, in $\mathbb{Z}/m\mathbb{Z}$ ci sono $\phi(d)$ elementi di ordine d.

In un qualsiasi gruppo l'unico elemento di ordine 1 è l'elemento neutro, quindi $d_1 = 1$.

Gli elementi (a, b) di ordine 2 soddisfano $2(a, b) = 0$. Ci sono due scelte per a e due scelte per b, in tutto 4 scelte a cui dobbiamo togliere l'elemento neutro; quindi $d_2 = 3$.

Allo stesso modo, alle 25 soluzioni dell'equazione $5(a, b) = 0$, togliamo l'elemento neutro per avere gli elementi di ordine 5; cioè $d_5 = 24$.

Possiamo ora calcolare d_{10} come il numero di soluzioni di $10(a,b)=0$ a cui togliamo gli elementi di ordine 1, 2, 5; abbiamo quindi $d_{10}=100-d_1-d_2-d_5=100-1-3-24=72$.

Un elemento (a,b) ha ordine 4 se e solo se b ha ordine 4 e $\mathrm{ord}(a)\,|\,(4,10)=2$. L'elemento b può essere scelto in 2 modi visto che in $\mathbb{Z}/20\mathbb{Z}$ ci sono $\phi(4)=2$ elementi di ordine 4, mentre per a ci sono 2 possibilità in quanto in $\mathbb{Z}/10\mathbb{Z}$ ci sono 2 elementi di ordine 1 o 2. Abbiamo quindi $d_4=4$.

Infine possiamo ottenere d_{20} come differenza $d_{20}=10\cdot 20-d_1-d_2-d_4-d_5-d_{10}=200-1-3-4-24-72=96$.

⟦Alternativamente, possiamo calcolare d_{20} osservando che (a,b) ha ordine 20 se e solo se: b ha ordine 20 e a è qualsiasi oppure b ha ordine 4 e a ha ordine 5 o 10. Nel primo caso ci sono $\phi(20)=8$ possibilità per b e 10 per a, mentre nel secondo abbiamo 2 possibilità per b e $8=\phi(5)+\phi(10)$ per a, in totale 16 scelte. Troviamo così $d_{20}=80+16=96$.⟧

162. (i) Sia $g=(g_1,g_2,g_3)$ un elemento di G con $g_1\in\mathbb{Z}/5\mathbb{Z}$, $g_2\in\mathbb{Z}/10\mathbb{Z}$ e $g_3\in\mathbb{Z}/36\mathbb{Z}$. L'elemento g è nel nucleo di f se e solo $f(g)=78(g_1,g_2,g_3)=(3g_1,-2g_2,6g_3)=(0,0,0)$; e quindi se e solo se $g_1\equiv 0 \pmod 5$, $g_2\equiv 0 \pmod 5$ e $g_3\equiv 0 \pmod 6$.

Concludiamo che $\mathrm{Ker}(f)$ ha $1\cdot 2\cdot 6=12$ elementi. Da cui $\mathrm{Im}(f)\simeq G/\mathrm{Ker}(f)$ ha $|G|/|\mathrm{Ker}(f)|=5\cdot 10\cdot 36/12=150$ elementi.

(ii) Sia $g\in G$, allora $\mathrm{ord}(f(g))\,|\,(|\mathrm{Im}(f)|,\mathrm{ord}(g))=(150,\mathrm{ord}(g))$. Ricordiamo che, se $g=(g_1,g_2,g_3)\in G$, allora

$$\mathrm{ord}(g)=\big[\mathrm{ord}(g_1),\mathrm{ord}(g_2),\mathrm{ord}(g_3)\big]\,|\,[5,10,36]=180.$$

Da questo segue che $\mathrm{ord}(f(g))\,|\,(180,150)=30$ per ogni $g\in G$.

D'altra parte, per $g=(1,1,1)$ si ha $f(g)=(3,-2,6)$ e, quindi, $\mathrm{ord}(f(g))=[5,5,6]=30$ che, per quanto visto, è il massimo valore possibile.

163. (i) Osserviamo che $0_G=2\cdot 0_G\in Q$. Inoltre, se $x_1,x_2\in Q$, allora $x_1=2g_1$ e $x_2=2g_2$ con $g_1,g_2\in G$ e quindi $x_1+x_2=2g_1+2g_2=2(g_1+g_2)\in Q$; infine $-x_1=-2g_1=2(-g_1)\in Q$. Questo prova che Q è un sottogruppo di G.

⟦Un altro modo per vedere che Q è un sottogruppo è osservare che, poiché G è abeliano, l'applicazione $\varphi: G\longrightarrow G$ definita da $\varphi(g)=2g$ è un omomorfismo e che $Q=\mathrm{Im}(\varphi)$.⟧

(ii) L'applicazione $G\ni g\overset{\varphi}{\longmapsto}2g\in G$ è un omomorfismo perché G è abeliano, inoltre $Q=\mathrm{Im}(\varphi)$ e si ha $|G/Q|=|\mathrm{Ker}(\varphi)|$. Ora $\mathrm{Ker}(\varphi)=\{g\in G\,|\,2g=0_G\}$, quindi gli elementi di $\mathrm{Ker}(\varphi)$ diversi da 0_G hanno ordine 2. Dal Teorema di Cauchy per i gruppi abeliani segue che, se $|G/Q|=|\mathrm{Ker}(\varphi)|$ è finito, allora esso è una potenza di 2. Questo dimostra quindi che non si può avere $m=3$.

Vediamo, invece, che 1, 2 e 4 si possono ottenere per qualche gruppo G. Sia $G=\mathbb{Z}/3\mathbb{Z}$; poiché $\mathbb{Z}/3\mathbb{Z}$ non ha elementi di ordine 2, si ha $\mathrm{Ker}(\varphi)=\{\overline{0}\}$, quindi $|G/Q|=1$. Per $G=\mathbb{Z}/2\mathbb{Z}$ abbiamo $\mathrm{Im}(\varphi)=\overline{0}$, quindi $m=2$. Sia, infine, $G=\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$; anche in questo caso tutti gli elementi di G hanno ordine 1 o 2, quindi φ è l'omomorfismo nullo e $|G/Q|=|G|=4$.

164. (i) Sia $(a,b)\in G$, abbiamo che $\mathrm{ord}(a,b)=[\mathrm{ord}(a),\mathrm{ord}(b)]$ è uguale a 11 se e solo se $\mathrm{ord}(a)\,|\,11$, $\mathrm{ord}(b)\,|\,11$ e $(a,b)\neq(0,0)$. Tenendo conto che per d che divide

m in $\mathbb{Z}/m\mathbb{Z}$ ci sono d elementi di ordine che divide d, otteniamo che le coppie (a, b) che stiamo cercando sono $11 \cdot 11 - 1 = 120$.

Poiché 11 è un numero primo, i sottogruppi di ordine 11 sono tutti ciclici e il loro numero è uguale al numero di elementi di ordine 11 diviso il numero di generatori di un gruppo ciclico con 11 elementi, cioè $\phi(11)$. Ci sono, quindi, 12 sottogruppi di ordine 11.

(ii) Per ogni sottogruppo H di ordine 11 si ha $|G/H| = |G|/|H| = 3^3 \cdot 11 = 297$, quindi se G/H fosse ciclico possiederebbe un elemento di ordine 297. Questo non è possibile perché in G ogni elemento ha ordine che divide 99 e per ogni $x \in G$ si ha $\mathrm{ord}(x + H) \mid \mathrm{ord}(x)$.

(iii) Non esiste alcun omomorfismo suriettivo. Infatti se f fosse un tale omomorfismo dovrebbe esistere $x \in G$ tale che $\mathrm{ord}(f(x)) = 121$; mentre questo non è possibile perché $\mathrm{ord}(f(x)) \mid \mathrm{ord}(x)$ e, per il gruppo G si ha $\mathrm{ord}(x) \mid 99$.

165. Sia $\pi : G \ni x \longmapsto xH \in G/H$ la proiezione sul quoziente. Poiché π è un omomorfismo si ha $\mathrm{ord}(xH) \mid \mathrm{ord}(x)$. Supponiamo che G/H abbia un elemento xH di ordine m, allora $\mathrm{ord}(x) = mk$ e quindi $\mathrm{ord}(x^k) = m$.

Viceversa sia $x \in G$ un elemento di ordine m, allora $\mathrm{ord}(xH) = d \mid m$, quindi $(xH)^d = H$ da cui $x^d \in H$. Per il Teorema di Lagrange abbiamo quindi che $x^{dn} = e$, da cui $m = \mathrm{ord}(x) \mid nd$. Dalla relazione $(n, m) = 1$ otteniamo $d \mid m$ e, infine, $d = m$.

166. (i) Tutti gli elementi $x = (a, b)$ di un sottogruppo di ordine 4 devono avere un ordine che è un divisore di 4, e quindi devono soddisfare la relazione $4x = (4a, 4b) = (\overline{0}, \overline{0})$. Risolvendo le congruenze, si ottiene $a \equiv 0 \pmod 2$, cioè $a \in \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$ e $b \equiv 0 \pmod 3$, cioè $b \in \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$.

Tra i $4 \cdot 4 = 16$ elementi riportati, 4 soddisfano anche l'equazione $(2a, 2b) = (\overline{0}, \overline{0})$, e cioè gli elementi $(\overline{0}, \overline{0})$, $(\overline{0}, \overline{6})$, $(\overline{4}, \overline{0})$, $(\overline{4}, \overline{6})$, mentre gli altri 12 hanno ordine uguale a 4. Ciascuno di questi 12 elementi genera un sottogruppo ciclico di ordine 4, ma in ciascun sottogruppo ciclico di ordine 4 ci sono due elementi di ordine 4, quindi il numero dei sottogruppi ciclici di ordine 4 è $12/2 = 6$. Essi si possono elencare scegliendo per ciascuno un generatore, per esempio $(\overline{0}, \overline{3})$, $(\overline{2}, \overline{0})$, $(\overline{2}, \overline{3})$, $(\overline{2}, \overline{6})$, $(\overline{2}, \overline{9})$, $(\overline{4}, \overline{3})$.

Inoltre le quattro soluzioni di $(2a, 2b) = (\overline{0}, \overline{0})$ formano un altro sottogruppo, non ciclico, di ordine 4. Infatti $(\overline{0}, \overline{0})$ è una soluzione; inoltre se (a, b) e (a', b') sono soluzioni, allora anche $(a + b, a' + b')$ è una soluzione, perché $2(a + b, a' + b') = 2(a, b) + 2(a', b') = (\overline{0}, \overline{0})$ e, infine, se (a, b) è una soluzione, allora anche $-(a, b)$ lo è, perché $2(-(a, b)) = -2(a, b) = (\overline{0}, \overline{0})$.

(ii) Sia H un sottogruppo di G di ordine 48. Poiché G è abeliano, H è certamente un sottogruppo normale di G, e quindi il quoziente G/H ha una struttura di gruppo, inoltre esso è evidentemente isomorfo a $\mathbb{Z}/2\mathbb{Z}$. Poiché, per ogni $g \in G$ si ha $2(gH) = (2g)H = H$, ricaviamo $2G \subseteq H$.

I sottogruppi che contengono $2G$ sono in corrispondenza biunivoca con i sottogruppi di $G/2G = (\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z})/(2\mathbb{Z}/8\mathbb{Z} \times 2\mathbb{Z}/12\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Ora $2G$ ha ordine $8/2 \times 12/2 = 24$, e quindi un sottogruppo H di G di ordine 48 corrisponde ad un sottogruppo di $G/2G$ di ordine 2, che sarà quindi formato dall'elemento neutro e da uno qualsiasi dei tre elementi di ordine 2 di $G/2G$. Ne segue che G ha

esattamente tre sottogruppi di ordine 48, che sono l'unione di $2G$ con una classe laterale $x + 2G$ di ordine 2 in $G/2G$. Per esempio, come rappresentanti di queste tre classi laterali di $G/2G$ diverse dall'elemento neutro si possono scegliere gli elementi $x = (\overline{1}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{1})$.

167. Vediamo come entrambi i punti hanno una risposta positiva.

(i) Sia $\pi : \mathbb{Z}/p^2\mathbb{Z}$ l'applicazione, $[x]_{p^2} \longmapsto [x]_p$; essa è ben definita perché se $x \equiv y \pmod{p^2}$ allora *a fortiori* $x \equiv y \pmod{p}$. Inoltre π è un omomorfismo, perché $[xy]_{p^2} = [x]_{p^2}[y]_{p^2}$ e quindi vale, a maggior ragione, $[xy]_p = [x]_p[y]_p$. Infine, π è suriettiva, perché se $(x, p) = 1$ allora anche $(x, p^2) = 1$.

(ii) Il gruppo G_1 è ciclico di ordine $p - 1$, in quanto p è un numero primo. Sia x un generatore di G_1, sia π la funzione definita nel punto precedente e sia $y \in G_2$ tale che $\pi(y) = x$. Allora abbiamo che $p - 1 = \mathrm{ord}(x) \mid \mathrm{ord}(y)$. Supponiamo che $\mathrm{ord}(y) = k(p - 1)$; allora $\mathrm{ord}(y^k) = p - 1$. Ne segue che l'applicazione $G_1 \ni x^h \mapsto y^{kh} \in G_2$ è un isomorfismo fra i due gruppi ciclici $G_1 = \langle x \rangle$ e $\langle y^k \rangle \subseteq G_2$, in particolare abbiamo costruito un omomorfismo iniettivo.

168. (i) Verifichiamo che H è un sottogruppo di G: $0 \in H$ visto che $p^a 0 = 0$; se $x, y \in H$, allora $p^a(x + y) = p^a x + p^a y$, in quanto G è abeliano, e quindi $p^a(x + y) = 0 + 0 = 0$; infine, se $x \in H$ allora $p^a(-x) = -p^a x = 0$, quindi $-x \in H$.

(ii) Supponiamo, per assurdo, che $x + H \in G/H$ sia un elemento di ordine p. Allora, in particolare, $p(x + H) = px + H = H$, ossia $px \in H$. Per definizione di H, questo significa che $p^a(px) = 0$, ossia che l'ordine di x è un divisore di p^{a+1}. D'altra parte, l'ordine di x deve dividere l'ordine di G, e quindi anche $(p^{a+1}, |G|) = p^a$. Segue che $p^a x = 0$, cioè $x \in H$ e la classe $x + H$ coincide con la classe H, che ha ordine 1, contraddicendo l'ipotesi.

(iii) Tutti gli elementi di H hanno un ordine divisore di p^a. Quindi, se $x \in H$ ha per ordine un numero primo, allora $\mathrm{ord}(x) = p$. Per il Teorema di Cauchy, l'ordine di H deve essere una potenza di p, infatti se così non fosse, ci sarebbe un altro primo q che divide $|H|$ e quindi in H ci sarebbe un elemento di ordine q. Sia allora $|H| = p^b$, per qualche naturale b, allora $p^b \,||G|$ visto che, per il Teorema di Lagrange, l'ordine di un sottogruppo divide l'ordine di un gruppo. Quindi $b \leq a$ e se fosse, per assurdo, $b < a$, il gruppo G/H avrebbe un ordine multiplo di p e quindi, ancora per il Teorema di Cauchy, un elemento di ordine p, contro quanto dimostrato al secondo punto.

169. (i) Se f, g sono due omomorfismi da G in $\mathbb{C}^*$, allora lo è anche fg, in quanto $(fg)(x + y) = f(x + y)g(x + y) = f(x)f(y)g(x)g(y) = f(x)g(x)f(y)g(y) = (fg)(x) \cdot (fg)(y)$. Possiamo quindi definire un'operazione $(f, g) \longmapsto fg$ in $\mathrm{Hom}(G, \mathbb{C}^*)$.

Quest'operazione è associativa, perché la moltiplicazione in $\mathbb{C}^*$ lo è. L'insieme $\mathrm{Hom}(G, \mathbb{C}^*)$ possiede un elemento neutro, e cioè l'applicazione $e : G \ni x \longmapsto 1 \in \mathbb{C}^*$. Proviamo, infine, che ogni omomorfismo $f \in \mathrm{Hom}(G, \mathbb{C}^*)$ ha un inverso. Detta infatti $f^{-1} : G \to \mathbb{C}^*$ la funzione definita da $f^{-1}(x) = f(x)^{-1}$ per ogni $x \in G$, si ha che $f^{-1}(xy) = (f(xy))^{-1} = f(x)^{-1}f(y)^{-1} = f^{-1}(x)f^{-1}(y)$, e quindi $f^{-1} \in \mathrm{Hom}(G, \mathbb{C}^*)$. Inoltre, $(ff^{-1})(x) = (f^{-1}f)(x) = f(x)^{-1}f(x) = 1 = e(x)$ per ogni $x \in G$, quindi $ff^{-1} = f^{-1}f = e$.

(ii) Un omomorfismo iniettivo φ è possibile solo se $\varphi(G) \simeq G$. Ma $\varphi(G)$ è un sottogruppo moltiplicativo finito di un campo, quindi è ciclico. Ne segue che G deve essere ciclico, ossia che $(m, n) = 1$.

D'altra parte, se $(m, n) = 1$, $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ è ciclico di ordine mn. Sia g un suo generatore, sia $\zeta = \zeta_{mn}$ una radice mn–esima primitiva dell'unità in $\mathbb{C}^*$ e consideriamo la funzione $f : G \to \mathbb{C}^*$ data da $f(g^k) = \zeta^k$.

La funzione è ben definita, in quanto se $k \equiv h \pmod{mn}$ allora $\zeta^k = \zeta^h$. Essa è un omomorfismo, perché $f(g^k g^h) = f(g^{k+h}) = \zeta^{k+h} = \zeta^k \zeta^h = f(g^k) f(g^h)$. L'omomorfismo è iniettivo, perché $\zeta^k = 1$ implica che $k \equiv 0 \pmod{mn}$ e quindi $g^k = id$.

170. (i) È ovvio che pG e qG sono contenuti in G, quindi $pG + qG \subseteq G$. Viceversa, sia $x \in G$ e siano a, b numeri interi tali che $pa + qb = 1$. Allora $x = pax + qbx \in pG + qG$, e quindi $G \subseteq pG + qG$.

(ii) Se $pq \nmid n$, allora almeno uno dei primi p, q non divide n e possiamo supporre, per simmetria, che $p \nmid n$. L'applicazione $f : G \to G$ data da $f(x) = px$ è un omomorfismo iniettivo, in quanto non esistono in G elementi di ordine p. Poiché G è un gruppo finito, f è anche un'applicazione suriettiva e quindi la sua immagine, pG, è uguale a G. A maggior ragione, $G = pG + qG$.

Supponiamo ora che $pq \mid n$, quindi $p \mid n$ e $q \mid n$. Allora, per il Teorema di Cauchy, G ha elementi sia di ordine p che di ordine q, quindi i nuclei degli omomorfismi $x \longmapsto px$ e $x \longmapsto qx$ sono diversi dal solo elemento neutro. Ne segue che le immagini di questi due omomorfismi, pG e qG, sono diverse da G. Ma l'unione di due sottogruppi di un gruppo è a sua volta un sottogruppo se e solo se i due sottogruppi sono uno contenuto nell'altro. Quindi in questo caso, siccome i due sottogruppi sono propri, anche se l'unione fosse un sottogruppo non potrebbe essere uguale a tutto G.

(iii) Come nel caso precedente, se $pqr \nmid n$ almeno uno dei primi, per esempio p, non divide n, e quindi $G = pG$. Se invece $pqr \mid n$, siccome G ha un elemento x di ordine p, allora l'omomorfismo $x \longmapsto px$ ha un nucleo di ordine almeno p, e di conseguenza la sua immagine, pG ha non più di n/p elementi. Similmente, $|qG| \leq n/q$ e $|rG| \leq n/r$, da cui

$$|pG \cup qG \cup rG| \leq \left(\frac{1}{p} + \frac{1}{q} + \frac{1}{r}\right) n \leq \left(\frac{1}{3} + \frac{1}{5} + \frac{1}{7}\right) n < n = |G|$$

e quindi non si avrà mai $pG \cup qG \cup rG = G$.

171. Usiamo una notazione additiva. Se $x \in G$ ha per ordine un numero primo p, questo numero primo deve essere un divisore di 200, cioè $p = 2, 5$. Per il Teorema di Cauchy, in G esistono sia elementi di ordine 2 che di ordine 5. Un elemento x di ordine 2 genera un sottogruppo di ordine 2, che ha x stesso come unico elemento di ordine 2; un elemento y di ordine 5 genera un sottogruppo di ordine 5, che contiene 4 elementi di ordine 5: $y, 2y, 3y, 4y$. Pertanto ogni gruppo G di ordine 200 contiene almeno $1 + 4 = 5$ elementi di ordine primo. Questo è esattamente il caso del gruppo ciclico $\mathbb{Z}/200\mathbb{Z}$, che contiene $\phi(d)$ elementi di ordine d per ogni d divisore di 200. Il valore minimo cercato è quindi 5.

Un elemento di ordine 2 appartiene al sottogruppo $G_2 = \{x \in G \mid 2x = 0\}$ che, per il Teorema di Cauchy, ha ordine una potenza di 2. Inoltre, poiché l'ordine di G_2 deve dividere l'ordine di G, si ha che $|G_2|$ divide 8. Un gruppo di ordine m ha al massimo $m - 1$ elementi di ordine 2, tutti meno l'elemento neutro, quindi G può avere al massimo 7 elementi di ordine 2.

Analogamente, un elemento di ordine 5 deve appartenere al sottogruppo $G_5 = \{x \in G \mid 5x = 0\}$, che ha al massimo 25 elementi e quindi al massimo 24 elementi di ordine 5.

Ne segue che il massimo numero di elementi di ordine primo in un gruppo G di ordine 200 non supera $7 + 24 = 31$. Nel caso in cui $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ l'uguaglianza è verificata, quindi 31 è il massimo cercato.

172. Per il Teorema di Cauchy, in G ci sono sia elementi di ordine p che elementi di ordine q. Sia x un elemento di ordine p e sia y un elemento di ordine q. Allora xy ha ordine pq: infatti $(xy)^{pq} = x^{pq}y^{pq} = e$ e, per i divisori propri di pq, si ha ovviamente: $(xy)^1 = xy \neq 1$, $(xy)^p = y^p \neq 1$, $(xy)^q = x^q \neq 1$. D'altra parte, un sottogruppo di ordine pq deve contenere sia un sottogruppo di ordine p che uno di ordine q; ne segue che esso è ciclico e generato dal prodotto di questi due elementi.

Poniamo $H = \langle x \rangle$ e $K = \langle y \rangle$, da cui $HK = \langle xy \rangle$. Allora l'applicazione $(H, K) \longmapsto HK$ è biunivoca fra le coppie (H, K) di sottogruppi di ordine p e q, rispettivamente, e i sottogruppi di ordine pq. Infatti la suriettività segue dal fatto che ogni sottogruppo di ordine pq contiene un sottogruppo di ordine p ed uno di ordine q. Inoltre l'applicazione è iniettiva in quanto un gruppo ciclico di ordine pq contiene *esattamente un* sottogruppo di ordine p ed *un* sottogruppo di ordine q. Pertanto $h_{pq} = h_p h_q$.

Per la seconda formula, basta osservare che $m_{pq} = \phi(pq)h_{pq}$, $m_p = \phi(p)h_p$, $m_q = \phi(q)h_q$. Sostituendo, ed usando l'identità $\phi(pq) = \phi(p)\phi(q)$, si ottiene la formula cercata.

173. (i) Per ipotesi i gruppi G/H e G/K hanno ordine p e, quindi, sono isomorfi a $\mathbb{Z}/p\mathbb{Z}$. Per mostrare la tesi basta provare che $G \simeq G/H \times G/K$.

Sia $\varphi : G \longrightarrow G/H \times G/K$ definita da $g \longmapsto (gH, gK)$. Tale applicazione è un omomorfismo perché

$$\begin{aligned} \varphi(xy) &= (xyH, xyK) \\ &= (xHyH, xKyK) \\ &= (xH, xK)(yH, yK) \\ &= \varphi(x)\varphi(y). \end{aligned}$$

Inoltre, visto che $\mathrm{Ker}(\varphi) = \{g \in G \mid (gH, gK) = (H, K)\} = H \cap K = \{e\}$, si ha che φ è iniettivo.

Infine, per provare che φ è suriettivo, basta mostrare che $|G| = p^2$. Poiché G si immerge in $G/H \times G/K$ che ha cardinalità p^2, basta escludere che $|G| = p$, e questo è vero perché G ha due sottogruppi distinti di indice p.

(ii) Poiché p è primo, i sottogruppi di ordine p sono tutti ciclici e quindi il loro numero è uguale al numero degli elementi di ordine p di G diviso per $\phi(p)$.

Inoltre, poiché gli isomorfismi conservano l'ordine degli elementi, è equivalente contare gli elementi di ordine p in $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Essi sono chiaramente tutti tranne l'elemento neutro, cioè $p^2 - 1$.

Concludiamo che in G ci sono $(p^2 - 1)/\phi(p) = p + 1$ sottogruppi di ordine p.

⟦Visto che $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{F}_p^2$ come gruppi abeliani, il numero di sottogruppi di ordine p in $\mathbb{F}_p^2$, e quindi in G, è dato dal numero di sottospazi vettoriali di dimensione 1, cioè dal numero di rette nel piano $\mathbb{F}_p^2$ passanti per l'origine. Queste sono chiaramente $p + 1$.⟧

174. (i) Mostriamo che G^k è un sottogruppo di G. Infatti, per prima cosa osserviamo che $e = e^k \in G^k$. Poi, per ogni $a^k, b^k \in G^k$ si ha $a^k b^k = (ab)^k$ visto che G è abeliano, e quindi $a^k b^k = (ab)^k \in G^k$. Infine da $a^k \in G^k$ abbiamo $(a^k)^{-1} = (a^{-1})^k \in G^k$. Inoltre, poiché G è abeliano, G^k è anche normale.

Consideriamo il quoziente G/G^k e sia xG^k un suo elemento. Allora, si ha $(xG^k)^k = x^k G^k = G^k$, quindi l'ordine di un qualsiasi elemento del quoziente è un divisore di k, ed è, quindi, finito.

(ii) Sia $G \cong \mathbb{Z}/n\mathbb{Z}$ allora $G^k \simeq \langle [k]_n \rangle$, un gruppo ciclico di ordine uguale a $\mathrm{ord}([k]_n) = n/(n,k)$. Ne segue che $|G/G^k| = |G|/|G^k| = (n,k)$.

⟦Sappiamo anche che G/G^k è ciclico perché quoziente di un gruppo ciclico quindi $G/G^k \simeq \mathbb{Z}/(n,k)\mathbb{Z}$.⟧

(iii) Consideriamo il gruppo $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$, allora $G^{10} = \{(0,0)\}$ infatti per ogni $(a,b) \in G$ si ha $10(a,b) = (10a, 10b) = (0,0)$. Per tale gruppo chiaramente $G/G^k = G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.

⟦Più in generale se $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ si ha $G^k = \{(ka, kb) \mid (a,b) \in G\} = \mathbb{Z}/(m/(m,k))\mathbb{Z} \times \mathbb{Z}/(n/(n,k))\mathbb{Z}$ e $G/G^k \simeq \mathbb{Z}/(m,k)\mathbb{Z} \times \mathbb{Z}/(n,k)\mathbb{Z}$. Ne segue che, per $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, vale $G/G^{10} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ se e solo se $(m, 10) = 2$ e $(n, 10) = 10$.⟧

175. (i) Visto che $\mathbb{Z}/m\mathbb{Z}$ è ciclico ed è generato da $\overline{1}$, un omomorfismo $\varphi : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ è completamente definito una volta assegnato il valore di $\varphi(\overline{1}) = \overline{a}$ con la condizione che $\mathrm{ord}(\overline{a}) \mid m$; questo assegnamento definisce l'omomorfismo $\overline{k} \longmapsto \varphi(\overline{k}) = k\overline{a}$. Dato che $a \in \mathbb{Z}/n\mathbb{Z}$ la condizione $\mathrm{ord}(\overline{a}) \mid m$ è equivalente alla condizione $\mathrm{ord}(\overline{a}) \mid (m,n) = d$. Gli omomorfismi cercati sono allora tanti quanti gli elementi di $\mathbb{Z}/n\mathbb{Z}$ il cui ordine divide d. Essi sono, quindi, in numero di d e sono definiti da $\varphi(\overline{k}) = k\overline{a}$ con $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ e $\mathrm{ord}(a) \mid d$.

Da quanto detto segue che l'applicazione $\Phi : \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \longrightarrow \mathbb{Z}/n\mathbb{Z}$ definita da $\Phi(\varphi) = \varphi(\overline{1})$ ha come immagine il sottogruppo di ordine d di $\mathbb{Z}/n\mathbb{Z}$. Per avere la tesi basta mostrare che essa è un omomorfismo iniettivo. È immediato vedere che è un omomorfismo, infatti per ogni coppia φ_1, φ_2 in $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ si ha $\Phi(\varphi_1 + \varphi_2) = (\varphi_1 + \varphi_2)(\overline{1}) = \varphi_1(\overline{1}) + \varphi_2(\overline{1}) = \Phi(\varphi_1) + \Phi(\varphi_2)$. Per l'iniettività basta, infine, osservare che $\Phi(\varphi) = \overline{0}$ se e solo se $\varphi(\overline{1}) = \overline{0}$ e quindi se e solo se $\varphi(\overline{k}) = k\overline{0} = \overline{0}$ per ogni $\overline{k} \in \mathbb{Z}/m\mathbb{Z}$, cioè φ è l'omomorfismo nullo.

(ii) Visto che $12 \mid (360, 420) = 60 = |\mathrm{Hom}(\mathbb{Z}/360\mathbb{Z}, \mathbb{Z}/420\mathbb{Z})|$, per quanto provato nel primo punto esiste un solo sottogruppo di ordine 12 ed è quello che, con l'isomorfismo dato, corrisponde al sottogruppo di ordine 12 di $\mathbb{Z}/420\mathbb{Z}$, cioè a $\langle \overline{35} \rangle$. Il sottogruppo richiesto è quindi costituito dagli omomorfismi $\varphi : \mathbb{Z}/360\mathbb{Z} \longrightarrow \mathbb{Z}/420\mathbb{Z}$ definiti da $\varphi(\overline{1}) = \overline{a}$ con $a \equiv 0 \pmod{35}$.

176. (i) Sia $e \in G$ l'elemento neutro, allora (e, e) è l'elemento neutro di $G \times G$ e appartiene a Δ. Siano (x, x) e $(y, y) \in \Delta$, chiaramente $(x, x)(y, y) = (xy, xy) \in \Delta$. Infine, sia $(x, x) \in \Delta$; il suo inverso in $G \times G$ è l'elemento (x^{-1}, x^{-1}), ancora un elemento di Δ . Questo prova che Δ è un sottogruppo di $G \times G$.

(ii) Se G è abeliano anche $G \times G$ lo è, quindi tutti i suoi sottogruppi sono normali. Viceversa, supponiamo che Δ sia normale in $G \times G$, allora per ogni $g \in G$ e per ogni $x \in G$ si ha $(g, e)(x, x)(g^{-1}, e) = (gxg^{-1}, x) \in \Delta$ e questo implica che per ogni $g, x \in G$ vale $gxg^{-1} = x$, cioè il gruppo G è abeliano.

(iii) Consideriamo la mappa $\varphi : G \times G \longrightarrow G$ definita da $\varphi(x, y) = xy^{-1}$. Poiché G è abeliano questa mappa è un omomorfismo, infatti $\varphi((x, y)(u, v)) = \varphi(xu, yv) = xu(yv)^{-1} = xuv^{-1}y^{-1} = xy^{-1}uv^{-1} = \varphi(x, y)\varphi(u, v)$. Inoltre l'omomorfismo è chiaramente suriettivo in quanto $\varphi(x, e) = x$ per ogni $x \in G$. Osserviamo anche che $\mathrm{Ker}(\varphi) = \{(x, y) \mid xy^{-1} = e\} = \Delta$. Dal Teorema di Omomorfismo otteniamo quindi che $G \times G/\Delta \simeq G$.

177. (i) Per prima cosa $0 \in G_p$, in quanto $p^0 0 = 1 \cdot 0 = 0$. Siano $x, y \in G_p$ e siano $k, h \in \mathbb{N}$ tali che $p^k x = 0$, $p^h y = 0$; ponendo $m = \max\{k, h\}$, si ha $p^m(x + y) = p^m x + p^m y = 0 + 0 = 0$, dunque $x + y \in G_p$. Infine, se $x \in G_p$ e $p^k x = 0$ allora anche $p^k(-x) = -p^k x = 0$, da cui $-x \in G_p$. Abbiamo quindi provato che G_p è un sottogruppo di G.

(ii) Se $\mathrm{ord}(x) = a$, allora $kax = 0$ per ogni $k \in \mathbb{N}$. Analogamente, se $\mathrm{ord}(y) = b$, allora $hby = 0$ per ogni $h \in N$. Quindi $ab(x+y) = abx+aby = 0+0 = 0$, pertanto $\mathrm{ord}(x + y) \mid ab$.

Supponiamo ora che $s(x + y) = 0$. Abbiamo $sx = -sy$. Il primo termine appartiene al sottogruppo generato da x, mentre il secondo appartiene al sottogruppo generato da y. L'intersezione dei due sottogruppi è costituita dal solo elemento 0, in quanto si tratta di un sottogruppo il cui ordine deve dividere sia a che b, e quindi deve avere ordine $1 = (a, b)$. Ma allora $sx = 0$, e quindi $a \mid s$, e $sy = 0$, e quindi $b \mid s$. Poiché, di nuovo, $(a, b) = 1$, abbiamo $ab \mid s$, e quindi $ab \mid \mathrm{ord}(x + y)$.

(iii) Una implicazione è ovvia: se G è ciclico allora tutti i suoi sottogruppi sono ciclici, e in particolare tutti i G_p sono sottogruppi ciclici. Per l'altra implicazione, dimostriamo innanzitutto che, se p^a è la massima potenza di p che divide n, allora l'ordine di G_p è uguale a p^a.

Per il Teorema di Cauchy, l'ordine di G_p può essere solo una potenza di p. Consideriamo ora il quoziente G/G_p, e dimostriamo che esso non ha elementi di ordine p. Infatti, se per assurdo $x + G_p \in G/G_P$ è un elemento di ordine p, allora $p(x + G_p) = G_p$, ossia $px = y \in G_p$ e dunque esiste un intero k per cui $p^k y = p^{k+1} x = 0$, da cui $x \in G_p$; ne segue che la classe laterale $x + G_p$ è la classe elemento neutro del quoziente e quindi ha ordine 1, ed abbiamo una contraddizione.

Ora, non avendo G/G_p elementi di ordine p, sempre per il Teorema di Cauchy, segue che p non divide l'ordine di G/G_p. Ma dato che $|G| = |G_p| \cdot |G/G_p|$, abbiamo la tesi che $|G_p| = p^a$.

Sia ora $n = p_1^{e_1} \cdots p_k^{e_k}$ la fattorizzazione di n in primi e siano $x_1, \ldots, x_k \in G$ elementi appartenenti rispettivamente a G_{p_i} di ordine $p_i^{e_i}$. Dimostriamo, per induzione su k, che $x_1 + \cdots + x_k$ ha ordine $p_1^{e_1} \cdots p_k^{e_k}$. Se $k = 0$ non c'è niente

da dimostrare. Supposta vera la tesi per $k-1$, chiamiamo $x = x_1 + \cdots + x_{k-1}$, $y = x_k$, $a = p_1^{e_1} \cdots p_{k-1}^{e_{k-1}}$, $b = p_k^{e_k}$. Da quanto provato nel secondo punto abbiamo che l'ordine di $x + y$ è $ab = n$, cioè l'ordine del gruppo G, da cui G è ciclico.

178. (i) Cominciamo provando che $f + g : G \longrightarrow G'$ è un omomorfismo. Si ha infatti $(f+g)(u+v) = f(u+v) + g(u+v) = f(u) + f(v) + g(u) + g(v) = f(u) + g(u) + f(v) + g(v) = (f+g)(u) + (f+g)(v)$, dove abbiamo usato che G' è abeliano. Inoltre l'operazione $(f, g) \longmapsto f + g$ su $\mathrm{Hom}(G, G')$ è associativa in quanto lo è la somma di elementi in G'. L'elemento neutro è dato dall'omomorfismo $G \ni u \longmapsto 0 \in G'$. L'opposto dell'omomorfismo $G \ni u \longmapsto f(u) \in G'$ è dato dall'applicazione $G \ni u \longmapsto -f(u) \in G'$ che si verifica subito essere un omomorfismo.

Un omomorfismo $f : G \longrightarrow G'$ induce, per restrizione, due omomorfismi $f_1 : \mathbb{Z}/18\mathbb{Z} \longrightarrow G'$ e $f_2 : \mathbb{Z}/12\mathbb{Z} \longrightarrow G'$ dati da $f_1(x) = f(x, \overline{0})$ e $f_2(y) = f(\overline{0}, y)$. Viceversa, dati due omomorfismi $f_1 : \mathbb{Z}/18\mathbb{Z} \longrightarrow G'$ e $f_2 : \mathbb{Z}/12\mathbb{Z} \longrightarrow G'$ si ottiene un omomorfismo dato da $G \ni (x, y) \longmapsto f(x, y) = f_1(x) + f_2(y) \in G'$. Ne segue che gli omomorfismi da G in G' sono in corrispondenza biunivoca con $\mathrm{Hom}(\mathbb{Z}/18\mathbb{Z}, \mathbb{Z}/36\mathbb{Z}) \times \mathrm{Hom}(\mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/36\mathbb{Z})$ e sono quindi $18 \cdot 12 = 216$, visto che $18 = (18, 36)$ e $12 = (12, 36)$.

(ii) Supponiamo che $f(\overline{1}, \overline{0}) = \overline{r}$ e $f(\overline{0}, \overline{1}) = \overline{s}$. Allora necessariamente $\overline{r} = 2\overline{r_1}$ e $\overline{s} = 3\overline{s_1}$, perché gli ordini di $\overline{r}$ e $\overline{s}$ devono dividere, rispettivamente, 18 e 12. L'omomorfismo f risulta definito dalla formula $f(x, y) = \overline{r} \cdot x + \overline{s} \cdot y$, ed è suriettivo se e solo se esistono x, y tali che $\overline{r} \cdot x + \overline{s} \cdot y$ sia un generatore di $\mathbb{Z}/36\mathbb{Z}$, ossia se esistono x, y tali che $(2r_1 x + 3s_1 y, 36) = 1$.

Una condizione necessaria è certamente che $3 \nmid r_1$ e $2 \nmid s_1$, altrimenti tutti i numeri $2r_1 x + 3s_1 y$ sarebbero multipli di 3 o di 2. La condizione è però anche sufficiente, in quanto, se $3 \nmid r_1$ e $2 \nmid s_1$, allora $2r_1 + 3s_1$ non è divisibile né per 3 né per 2, dunque è relativamente primo con 36, e quindi la sua classe resto modulo 36 è un generatore di $\mathbb{Z}/36\mathbb{Z}$.

Abbiamo provato che il numero degli omomorfismi suriettivi è dato dal numero di coppie $(2\overline{r_1}, 3\overline{s_1}) \in G' \times G'$ con $3 \nmid r_1$ e $2 \nmid s_1$, ed è, quindi, uguale a $12 \cdot 6 = 72$.

(iii) Si ha $\varphi_{(a,b)}(f+g) = (f+g)(a,b) = f(a,b) + g(a,b) = \varphi_{(a,b)}(f) + \varphi_{(a,b)}(g)$, pertanto $\varphi_{(a,b)}$ è un omomorfismo. Usando la notazione del punto precedente, e scegliendo $\overline{r} = -\overline{2}$, $\overline{s} = \overline{3}$, si vede che $-\overline{2} + \overline{3} = \overline{1}$ appartiene all'immagine dell'omomorfismo. Poiché, $\overline{1}$ è un generatore di $\mathbb{Z}/36\mathbb{Z}$, l'omomorfismo è suriettivo. Usando infine il Teorema di Omomorfismo, l'immagine è isomorfa a $\mathrm{Hom}(G, G')/\mathrm{Ker}(\varphi_{(\overline{1},\overline{1})})$ e quindi $|\mathrm{Ker}(\varphi_{(\overline{1},\overline{1})})| = |\mathrm{Hom}(G, G')|/|G'| = 216/36 = 6$.

179. (i) È chiaro che il secondo punto implica il primo ma, per completezza, diamo una dimostrazione indipendente del primo punto.

Siano $x_1 + H, \ldots, x_m + H$ le classi laterali di H, e $y_1 + K, \ldots, y_n + K$ le classi laterali di K. È chiaro che

$$G = \bigcup_{i=1}^{m} (x_i + H) = \bigcup_{j=1}^{n} (y_j + K) = \bigcup_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}} (x_i + H) \cap (y_j + K).$$

L'ultima espressione è l'unione di mn sottoinsiemi. Se dimostriamo che ciascuno di essi è incluso in una sola classe laterale di $H \cap K$ la tesi segue. Dimostriamo dunque che per ogni i e per ogni j, presi comunque due elementi $a, b \in (x_i + H) \cap (y_j + K)$, si ha $a + H \cap K = b + H \cap K$. Infatti abbiamo $a - b \in H$, $a - b \in K$, quindi $a - b \in H \cap K$, e questo è equivalente al nostro asserto.

(ii) Consideriamo l'applicazione $f : G \longrightarrow G/H \times G/K$ data da $f(x) = (x + H, x + K)$, si tratta di un omomorfismo perché le due componenti sono le proiezioni di G su G/H e G/K. Il nucleo di f è $\{x \in G \mid x \in H,\ x \in K\} = H \cap K$. Per il Teorema di Omomorfismo, f induce un omomorfismo *iniettivo* $G/(H \cap K) \longrightarrow G/H \times G/K$, e quindi $d = |G/(H \cap K)|$ divide $|G/H| \cdot |G/K| = mn$.

(iii) La tesi equivale a dimostrare che l'omomorfismo f del punto precedente è suriettivo se e solo se $H + K = G$. Supponiamo $H + K = G$, e prendiamo un elemento $(a + H, b + K) \in G/H \times G/K$. Per ipotesi, possiamo scrivere $a - b = h + k$, con $h \in H$, $k \in K$. Scegliamo ora $g = a - h = b + k$. Abbiamo $f(g) = (g + H, g + K) = (a + H, b + K)$, quindi f è suriettivo.

Viceversa, supponiamo che f sia suriettivo. Allora, per ogni $x \in G$, esiste $g \in G$ tale che $f(g) = (x + H, K)$. Questo significa che $g + H = x + H$, ossia $x - g = h \in H$ e che $g + K = K$, ossia $g \in K$. Ne segue che $x = h + g \in H + K$, e quindi $G \subseteq H + K$. L'altra inclusione è ovvia.

180. (i) Se nel gruppo G prendiamo due sottogruppi ciclici isomorfi a $\mathbb{Z}$, diciamo $H_1 = \langle a_1/b_1 \rangle$ e $H_2 = \langle a_2/b_2 \rangle$, essi hanno in comune l'elemento $a_1 a_2 = a_2 b_1 \cdot a_1/b_1 = a_1 b_2 \cdot a_2/b_2$, che è diverso da zero in quanto a_1/b_1 e a_2/b_2 sono diversi da zero. Questa contraddizione porta all'impossibilità dell'esistenza di un sottogruppo di G isomorfo a $\mathbb{Z} \times \mathbb{Z}$.

(ii) Prendiamo, per esempio, i sottogruppi

$$H_m = 2^m G = \left\{ 2^m \frac{a}{b} \mid \frac{a}{b} \in G \right\} \qquad \text{con } m \geq 0$$

e consideriamo i quozienti $G_m = G/H_m$.

La classe laterale $1 + H_m$ ha ordine 2^m, in quanto $k \cdot 1 \in H_m$ se e solo se k è della forma $2^m a/b$ con $(b, 10) = 1$, e quindi se e solo se kb è un multiplo di 2^m; ma poiché $(b, 2^m) = 1$ questo avviene se e solo se $2^m \mid k$.

Inoltre, ogni classe laterale $a/b + H_m$ è un multiplo di $1 + H_m$, in quanto se c è un intero tale che $cb \equiv a \pmod{2^m}$, allora $c - a/b \in H_m$ e quindi $c(1 + H_m) = c + H_m = a/b + H_m$.

Quindi G_m è ciclico di ordine 2^m.

(iii) Supponiamo, per assurdo, che G possieda un quoziente ciclico di ordine 3, ossia un sottogruppo H tale che $|G/H| = 3$. Allora ogni elemento di G/H dovrebbe avere ordine divisibile per 3, ossia, per ogni $x \in G$, $3(x + H) = H$, cioè $3x \in H$ e in definitiva $3G \subseteq H$. Ma in realtà $3G = G$, in quanto per ogni $y \in G$ si ha $y = 3 \cdot y/3 \in 3G$.

181. (i) Assumiamo G finito e proviamo che le condizioni sono necessarie.

Se f è un omomorfismo iniettivo, allora $f(G) \simeq G$ e, poiché $f(G)$ è un sottogruppo di H, allora H è necessariamente finito e $a \mid b$.

Sia ora $b = ac$. Supponiamo per assurdo che $(a, c) > 1$; allora esistono un numero primo p e due interi positivi α, β con $\alpha < \beta$ tali che p^α e p^β sono le massime potenze di p che dividono a e b rispettivamente. Siano $G_p \simeq \mathbb{Z}/p^\alpha\mathbb{Z}$ e $G_p \simeq \mathbb{Z}/p^\beta\mathbb{Z}$ gli unici sottogruppi di G e H di questi ordini, e sia $\gamma = \beta - \alpha$. Allora necessariamente $f(G_p)$ è l'unico sottogruppo di H_p di ordine p^α, ossia $f(G_p) = p^\gamma H_p$. In particolare, se x è un generatore di G_p, allora $f(x)$ non è un generatore di H_p, da cui $f(x) = py$ per qualche $y \in H_p$. Ma allora $g \circ f(x) = pg(y)$ non può essere un generatore di G_p, e questo contraddice l'ipotesi che $g \circ f$ sia un isomorfismo.

Proviamo ora che le condizioni sono sufficienti. Infatti, se $b = ac$ e $(a, c) = 1$, allora $H \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/c\mathbb{Z}$, $f(G)$ è l'unico sottogruppo di H di ordine a, cioè $\mathbb{Z}/a\mathbb{Z} \times \{\overline{0}\}$ e, ponendo g uguale alla proiezione canonica di $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/c\mathbb{Z}$ su $\mathbb{Z}/a\mathbb{Z}$, si ha $g \circ f(G) = G$, per cui $g \circ f$ è suriettivo.

Trattandosi di due insiemi con lo stesso numero di elementi, $g \circ f$ è anche iniettivo, e quindi è un isomorfismo.

(ii) Assumiamo ora G infinito e proviamo, per prima cosa, che la condizione è necessaria. Osserviamo innanzitutto che non esistono applicazioni iniettive da un insieme infinito ad un insieme finito, quindi H deve essere un gruppo ciclico infinito, e quindi isomorfo a $\mathbb{Z}$. Se per assurdo f non fosse suriettivo, allora avremmo $f(1) = k$ con $k \neq \pm 1$. Allora $g(k) = kg(1)$ sarebbe divisibile per k, e quindi $g(k) = g \circ f(1) \neq \pm 1$. Ne segue che l'applicazione $g \circ f$ manderebbe il generatore 1 di $\mathbb{Z}$ in un elemento che non è un generatore, e quindi non sarebbe un isomorfismo.

Dimostriamo ora che la condizione è anche sufficiente. Se $H \simeq \mathbb{Z}$, senza perdita di generalità possiamo assumere $G = H = \mathbb{Z}$, $f(x) = \pm x$ e, ponendo $g(x) = \pm x$, abbiamo che $g \circ f(x) = x$ è un isomorfismo.

182. Dato un sottogruppo H di un gruppo G, chiameremo sottogruppo *intermedio* fra H e G un sottogruppo L tale che $H \subsetneq L \subsetneq G$.

(i) La proiezione $G \ni g \overset{\pi}{\longmapsto} gK \in G/K$ induce una corrispondenza biunivoca, che conserva le inclusioni, fra i sottogruppi di G che contengono K e i sottogruppi di G/K. Poiché i sottogruppi di G che contengono M contengono anche K, esiste un sottogruppo intermedio fra M e G se e solo se esiste un sottogruppo di intermedio fra M/K e G/K, da cui la tesi.

(ii) Supponiamo, per assurdo, che la tesi sia falsa. Allora esistono dei sottogruppi di G non contenuti in nessun sottogruppo massimale. Sia H un sottogruppo di G non contenuto in nessun sottogruppo massimale. Avendo G ordine finito, possiamo anche assumere che H abbia ordine massimo possibile con questa proprietà.

Visto che H stesso non è massimale, esiste un sottogruppo intermedio L fra H e G. Ma $|L| > |H|$ e quindi L è contenuto in un sottogruppo massimale M, da cui $H \subseteq M$, in contraddizione con l'ipotesi su H.

(iii) Usiamo i risultati del primo punto ed il fatto che in un gruppo abeliano tutti i sottogruppi sono normali.

Se $[G : K] = p$ è un numero primo, allora K/K è un sottogruppo massimale di $G/K \cong \mathbb{Z}/p\mathbb{Z}$, in quanto un gruppo di ordine p ha solo sottogruppi banali.

Se $[G : K] = |G/K| = m$ non è un numero primo, sia p un numero primo che divide M. Per il Teorema di Cauchy esiste un sottogruppo di G/K di ordine p, che è evidentemente un sottogruppo intermedio fra K/K e G/K. Ma allora esiste un sottogruppo intermedio fra K e G, e quindi K non è massimale.

183. (i) Il gruppo $\mathbb{Z}/12\mathbb{Z}$ è un gruppo ciclico di ordine 12 generato da $\overline{1}$. Sappiamo che un omomorfismo $\varphi : \mathbb{Z}/12\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \times \mathsf{S}_3$, essendo $\mathbb{Z}/12\mathbb{Z}$ un gruppo ciclico, è completamente determinato dall'immagine di $\overline{1}$. Questa immagine deve essere assegnata rispettando la sola condizione $\mathrm{ord}(\varphi(\overline{1})) \mid \mathrm{ord}(\overline{1}) = 12$. Pertanto, l'immagine di $\overline{1}$ può essere un qualsiasi elemento di ordine divisore di 12 in $\mathbb{Z}/4\mathbb{Z} \times \mathsf{S}_3$.

Il gruppo $\mathbb{Z}/4\mathbb{Z} \times \mathsf{S}_3$ ha per elementi le coppie $(\overline{a}, \sigma)$ con $\overline{a} \in \mathbb{Z}/4\mathbb{Z}$ e $\sigma \in \mathsf{S}_3$. Sappiamo che $\mathrm{ord}(\overline{a}, \sigma) = [\mathrm{ord}(\overline{a}), \mathrm{ord}(\sigma)]$. Ma $\mathrm{ord}(\overline{a}) \mid 4$ e $\mathrm{ord}(\sigma) \mid 6$, quindi $\mathrm{ord}(\overline{a}, \sigma) \mid [4, 6] = 12$. Pertanto, possiamo scegliere come immagine di $\overline{1}$ un qualsiasi elemento di $\mathbb{Z}/4\mathbb{Z} \times \mathsf{S}_3$. Abbiamo in tutto 24 omomorfismi possibili.

L'omomorfismo φ è iniettivo se e soltanto se $\mathrm{ord}(\varphi(\overline{1})) = \mathrm{ord}(\overline{1}) = 12$; per contare gli omomorfismi iniettivi, dobbiamo contare gli elementi di $\mathbb{Z}/4\mathbb{Z} \times \mathsf{S}_3$ di ordine 12. L'ordine di un elemento di $\mathbb{Z}/4\mathbb{Z}$ è uguale a $1, 2$, oppure 4, mentre l'ordine di un elemento di S_3 può essere $1, 2$ o 3. Di conseguenza una coppia $(\overline{a}, \sigma)$ ha ordine 12 se e solo se $\mathrm{ord}(\overline{a}) = 4$ e $\mathrm{ord}(\sigma) = 3$. Ma in $\mathbb{Z}/4\mathbb{Z}$ ci sono $\phi(4) = 2$ elementi di ordine 4, cioè $\overline{1}$ e $\overline{3}$, e in S_3 ci sono 2 elementi di ordine 3, cioè i due 3–cicli (123), (132). Di conseguenza, abbiamo $2 \cdot 2 = 4$ omomorfismi possibili.

(ii) Per quanto detto precedentemente, un omomorfismo φ è completamente determinato dall'immagine di $\overline{1}$; sia $(\overline{a}, \sigma)$ tale immagine. Allora $\varphi(\overline{10}) = 10\varphi(\overline{1}) = (\overline{10a}, \sigma^{10})$.

Ne segue che l'ordine di $\varphi(\overline{10})$ è uguale a 3 se e solo se $[\mathrm{ord}(\overline{10a}), \mathrm{ord}(\sigma^{10})] = 3$. Poiché l'ordine di un elemento di $\mathbb{Z}/4\mathbb{Z}$ è $1, 2$ o 4 e l'ordine di un elemento di S_3 è $1, 2$ o 3, l'unica possibilità è avere $\mathrm{ord}(\overline{10a}) = 1$ e $\mathrm{ord}(\sigma^{10}) = 3$.

Ora $10a \equiv 0 \pmod 4$ se e soltanto se $2a \equiv 0 \pmod 4$, cioè $a \equiv 0 \pmod 2$. Questa equazione ha due soluzioni: $\overline{a} = \overline{0}, \overline{2}$. Per S_3 osserviamo che da $\mathrm{ord}(\sigma^{10}) = 3$ abbiamo $3 \mid \mathrm{ord}(\sigma)$ e, visto che $\sigma \neq e$, necessariamente σ è uno dei due 3–cicli di S_3. Ovviamente entrambi questi elementi soddisfano $\mathrm{ord}(\sigma^{10}) = 3$.

Ne segue che gli omomorfismi con $\mathrm{ord}(\varphi(\overline{10})) = 3$ sono tutti e soli quelli che mandano $\overline{1}$ in un elemento $(\overline{a}, \sigma)$ con $\overline{a} = \overline{0}$ o $\overline{2}$ e $\sigma = (123)$ o $\sigma = (132)$. In tutto quattro omomorfismi.

184. (i) Dal Teorema Cinese dei Resti, poiché $1000 = 8 \cdot 125$ e $(8, 125) = 1$, sappiamo che

$$(\mathbb{Z}/1000\mathbb{Z})^* \cong (\mathbb{Z}/8\mathbb{Z})^* \times (\mathbb{Z}/125\mathbb{Z})^*.$$

Da questo segue che G ha un sottogruppo isomorfo a $(\mathbb{Z}/8\mathbb{Z})^*$. Poiché $(\mathbb{Z}/8\mathbb{Z})^* = \{\overline{\pm 1}, \overline{\pm 3}\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ non è ciclico, neanche G può essere ciclico, in quanto ogni sottogruppo di un gruppo ciclico è ciclico.

(ii) Chiaramente l'elemento neutro appartiene ad H, perché ha ordine $1 = 2^0$. Inoltre siano $g, h \in H$ e sia $2^a = \max\{\mathrm{ord}(g), \mathrm{ord}(h)\}$, allora $(gh)^{2^a} = g^{2^a} h^{2^a} = e$,

quindi l'ordine di gh è una potenza di 2 in quanto divide 2^a. Ne segue che $gh \in H$. Poiché H è finito questo è sufficiente a mostrare che H è un sottogruppo di G.

Calcoliamo ora l'ordine di H. Per il Teorema di Lagrange $|H|$ divide $|G| = \phi(1000) = 2^4 \cdot 5^2$. Inoltre, poiché tutti gli elementi del sottogruppo H hanno ordine una potenza di 2, per il Teorema di Cauchy 2 è l'unico divisore primo dell'ordine di H, quindi $|H|$ divide 2^4. Dimostriamo che in effetti $|H| = 2^4$ facendo vedere che $|G/H| = 2^4 \cdot 5^2/|H|$ è dispari.

Infatti, se tale ordine fosse pari, per il Teorema di Cauchy esisterebbe gH in G/H di ordine 2, cioè $gH \neq H$ e $(gH)^2 = H$, o, equivalentemente, $g \notin H$ e $g^2 \in H$. Ma ciò è impossibile perché in tal caso si avrebbe che g^2 ha ordine una potenza di 2, e quindi anche g avrebbe ordine una potenza di 2 e quindi dovrebbe appartenere ad H. Questo finisce la dimostrazione che $|H| = 2^4$.

(iii) È sufficiente vedere che $(\mathbb{Z}/125\mathbb{Z})^*$ contiene un elemento di ordine 25, cioè che ci sono soluzioni della congruenza $x^{25} \equiv 1 \pmod{125}$ che non risolvono $x^5 \equiv 1 \pmod{125}$. Sia, ad esempio, $x = \overline{6} \in \mathbb{Z}/125\mathbb{Z}$, allora $x^{25} = (1+5)^{25} \equiv 1 + 25 \cdot 5 \equiv 1 \pmod{125}$. Invece $x^5 = (1+5)^5 \equiv 1 + 5 \cdot 5 = 26 \not\equiv 1 \pmod{125}$ e quindi x non risolve $x^5 \equiv 1 \pmod{125}$. Abbiamo così provato che x ha ordine 25.

Sappiamo che $|G/H| = 25$; per mostrare che questo gruppo è ciclico basta osservare che, posto come sopra $x = \overline{6}$, allora la classe quoziente xH ha ordine 25 in G/H. Sia $d = \mathrm{ord}(xH)$, cioè d è il minimo intero positivo per cui $x^d \in H$. Per definizione di H, ogni suo elemento ha ordine una potenza di 2, quindi $\mathrm{ord}(x^d) = 25/(d, 25) = 2^k$, per qualche k. Ma ciò è possibile solo se $k = 0$ e $d = 25$.

185. (i) Poiché G è abeliano, per ogni $g, h \in G$ si ha $g^k h^k = (gh)^k$, quindi l'applicazione $\varphi_k : G \longrightarrow G$ definita da $\varphi_k(g) = g^k$ è un omomorfismo di gruppi e $G^k = \varphi_k(G)$. Poiché l'immagine di un omomorfismo è sempre un sottogruppo, si ottiene che G^k è un sottogruppo di G.

(ii) Consideriamo ancora l'omomorfismo $G \ni g \overset{\varphi_k}{\longmapsto} g^k \in G$. Si ha $G^k = G$ se e solo se φ_k è suriettivo, ed essendo G finito, se e solo se φ_k è iniettivo. Si tratta quindi di vedere per quali valori di k si ha $\mathrm{Ker}(\varphi_k) = \{e\}$.

Supponiamo dapprima che $(n, k) > 1$ e sia p un primo che divide (n, k). Dal Teorema di Cauchy segue che in G esiste un elemento g di ordine p, e poiché $k = pd$ per qualche intero d, $g^k = (g^p)^d = e$, quindi il nucleo di φ_k è non banale e l'omomorfismo non è suriettivo.

Sia invece $(n, k) = 1$. Abbiamo $g^k = e$ se e solo se l'ordine di g divide k, ma poiché esso deve dividere anche n che è l'ordine del gruppo, l'unica possibilità è $g = e$. Quindi φ_k è iniettivo e suriettivo. In conclusione $G^k = G$ se e solo se $(k, n) = 1$.

(iii) Consideriamo, ad esempio, $G = \mathbb{Z}$. È chiaro che G^k è il sottogruppo $k\mathbb{Z}$ dei multipli di k. Ma allora 1 non è un elemento di G^k per ogni $k > 1$ e quindi $G^k \neq G$ per ogni $k > 1$.

⟦Un altro semplice esempio è dato dal gruppo moltiplicativo $\mathbb{Q}^*$, infatti $2 \notin \mathbb{Q}^{*k}$ se $k > 1$, come si può facilmente provare generalizzando la dimostrazione che $\sqrt{2} \notin \mathbb{Q}$.⟧

(iv) In questo caso possiamo considerare il gruppo additivo dei numeri razionali $\mathbb{Q}$. Infatti per ogni $k \geq 1$ e ogni numero razionale a/b si ha

$$\frac{a}{b} = k\frac{a}{kb} \in k\mathbb{Q}$$

e quindi $k\mathbb{Q} = \mathbb{Q}$.

⟦Altri esempi si hanno prendendo come G l'insieme di tutte le radici dell'unità o l'insieme di tutti i punti della circonferenza unitaria in $\mathbb{C}$, cioè i numeri complessi di modulo 1, con operazione data dall'usuale prodotto in $\mathbb{C}^*$. In entrambi i casi è immediato verificare che G è un gruppo, e che ogni $g \in G$ è il quadrato di un qualche elemento di G, il cubo di un qualche elemento di G, la quarta potenza di un qualche elemento di G e via dicendo. ⟧

186. (i) L'ordine di G è $3 \cdot 6 = 18$, quindi per il Teorema di Lagrange, l'ordine di un sottogruppo di G deve dividere 18. D'altra parte se H è un sottogruppo di $\mathbb{Z}/3\mathbb{Z}$ e K è un sottogruppo di S_3 allora $H \times K$ è un sottogruppo di G di ordine $|H| \cdot |K|$.

Per H possiamo prendere il sottogruppo banale, un solo elemento, e tutto $\mathbb{Z}/3\mathbb{Z}$, tre elementi. In S_3 ci sono sottogruppi con 1 elemento, il sottogruppo banale, con 2 elementi, un sottogruppo generato da una qualsiasi trasposizione, con 3 elementi, un sottogruppo generato da un tre ciclo, e tutto il gruppo S_3 con 6 elementi. Possiamo quindi scegliere K di ordine 1, 2, 3 e 6. Concludiamo così che ogni possibile divisore di 18 si ottiene come ordine di un sottogruppo di G.

(ii) Per contare il numero di sottogruppi ciclici di un dato ordine n, contiamo gli elementi di ordine n e poi dividiamo per $\phi(n)$. Infatti ogni sottogruppo ciclico di ordine n contiene $\phi(n)$ elementi di ordine n e se due sottogruppi ciclici hanno in comune un elemento di ordine n allora, essendo generati da tale elemento, coincidono.

L'ordine di un qualunque elemento di G è un divisore di 6, in quanto l'ordine di una coppia in un prodotto diretto è il minimo comune multiplo degli ordini delle sue componenti. Da questo segue che non esistono sottogruppi ciclici di ordine 9 o 18.

Gli elementi di ordine 2 sono quelli del tipo $(\overline{0}, \sigma)$ con σ una delle tre trasposizioni (12), (13) o (23) di S_3. Ci sono quindi $3 = 3/\phi(2)$ sottogruppi ciclici di ordine 2.

Gli elementi di G di ordine 3 sono quelli della forma $(\overline{a}, \sigma) \neq (0, e)$ con $a = 0, 1, 2$ e σ uno dei due 3–cicli (123) o (132) o l'elemento neutro. In tutto abbiamo quindi $3 \cdot 3 - 1 = 8$ elementi di ordine 3 e $4 = 8/\phi(3)$ sottogruppi ciclici di ordine 3.

Infine vi sono 3 sottogruppi ciclici di ordine 6: infatti ci sono 6 elementi di ordine 6, che sono gli elementi del tipo $(\overline{a}, \sigma)$ per $a = 1, 2$ e σ una delle tre trasposizioni di S_3 e $\phi(6) = 2$.

In conclusione G ammette $1 + 3 + 4 + 3 = 11$ sottogruppi ciclici.

3.5 Anelli e campi

187. Decomponiamo innanzitutto il polinomio $f(x)$ in fattori irriducibili. Per verifica diretta, usando il Teorema di Ruffini, si vede che il polinomio è divisibile sia

per $x-2$ che per $x-3$, e quindi per il loro prodotto. Dividendo, si ottiene

$$f(x) = (x-2)(x-3)(x^2-x+3)$$

dove l'ultimo fattore, essendo di secondo grado e senza radici in $\mathbb{F}_7$, è irriducibile. Rappresentiamo un elemento di $\mathbb{F}_7[x]/(f(x))$ nella forma $\overline{g(x)}$, dove $g(x)$ è un polinomio di grado minore o uguale a 3. Un tale elemento è un divisore di zero se e solo se $(g(x), f(x)) \neq 1$ ed è invertibile se e solo se $(g(x), f(x)) = 1$.

I divisori di zero sono dunque l'unione dei multipli di $x-2$, di $x-3$ e di x^2-x+3. I multipli di un polinomio di grado d che hanno grado minore o uguale a 3 sono tanti quanti i polinomi di grado minore o uguale a $3-d$, e cioè 7^{4-d}. Usando questo fatto, e il Principio di Inclusione Esclusione, si vede che i divisori di zero cercati sono

$$7^3 + 7^3 + 7^2 - 7^2 - 7 - 7 + 1 = 673.$$

Per quanto detto prima, $\overline{x+1}$ è invertibile. Per trovarne l'inverso, si noti che

$$\overline{0} = \overline{x^4 + x^3 - 3} = \overline{x+1} \cdot \overline{x^3} - \overline{3}.$$

Pertanto $\overline{x+1} \cdot \overline{x^3} = \overline{3}$, $\overline{x+1} \cdot \overline{5x^3} = \overline{1}$ e quindi $\overline{5x^3}$ è l'inverso di $\overline{x+1}$.

188. Osserviamo innanzitutto che $x^4 - 25 = (x^2-5)(x^2+5)$ e che i due polinomi x^2-5, x^2+5, essendo di grado due e non avendo radici razionali, sono irriducibili in $\mathbb{Q}[x]$.

Il campo di spezzamento di x^4-25 su $\mathbb{Q}$ è $\mathbb{F} = \mathbb{Q}(\sqrt{5}, \sqrt{-5})$. Poiché $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{-5}) : \mathbb{Q}] = 2$ e $\sqrt{-5} \notin \mathbb{Q}(\sqrt{5})$, in quanto $\sqrt{-5} \notin \mathbb{R}$ mentre $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{R}$, si ha $[\mathbb{F} : \mathbb{Q}] = 4$. Inoltre, una base di $\mathbb{F}$ su $\mathbb{Q}$ è data da $1, \sqrt{5}, \sqrt{-5}, \sqrt{-25} = 5i$, o anche, più semplicemente, da $1, \sqrt{5}, i, i\sqrt{5}$.

Sia $\mathbb{K}$ il campo di spezzamento cercato. Se m è della forma $\pm n^2$ oppure della forma $\pm 5n^2$ con $n \in \mathbb{N}$, allora $\sqrt{m} = \pm n, \pm im, \pm\sqrt{5}n, \pm i\sqrt{5}n$ appartiene ad $\mathbb{F}$, e quindi $\mathbb{K} = \mathbb{F}$ ha grado 4 su $\mathbb{Q}$.

Supponiamo ora che m non sia di nessuna delle forme precedenti. Il campo $\mathbb{K}$ contiene sia $\sqrt{m}$ che $i\sqrt{m}$: in definitiva, contiene $\sqrt{|m|}$, dove $|m| \neq n^2, 5n^2$. Dimostriamo che $\sqrt{|m|} \notin \mathbb{F}$. Infatti, se fosse $\sqrt{|m|} \in \mathbb{F}$ avremmo $\sqrt{|m|} = a + b\sqrt{5} + ci + di\sqrt{5}$, con $a, b, c, d \in \mathbb{Q}$.

Poiché $\sqrt{|m|} \in \mathbb{R}$, dovremmo avere $c = d = 0$, e quindi $\sqrt{|m|} = a + b\sqrt{5}$. Elevando al quadrato, $|m| = a^2 + 5b^2 + 2ab\sqrt{5}$, da cui

$$\begin{cases} |m| = a^2 + 5b^2 \\ 2ab = 0 \end{cases}$$

visto che 1 e $\sqrt{5}$ sono linearmente indipendenti su $\mathbb{Q}$.

La seconda equazione dice che $a = 0$ oppure $b = 0$. Se $a = 0$ allora $|m| = 5b^2$, mentre se $b = 0$ allora $|m| = a^2$, contro le ipotesi fatte.

Possiamo quindi concludere che, se m non è della forma $\pm n^2$ o $\pm 5n^2$ con $n \in \mathbb{Z}$, allora $\mathbb{K} = \mathbb{F}(\sqrt{|m|})$ e $\sqrt{|m|} \notin \mathbb{F}$; quindi $[\mathbb{K} : \mathbb{Q}] = 8$.

189. (i) Il polinomio $f(x)$ è irriducibile in $\mathbb{Q}[x]$. Infatti, poiché è di terzo grado, è irriducibile se non ha radici razionali e basta cioè controllare che ± 1 non siano radici: infatti una radice razionale deve avere numeratore che divide il termine noto e denominatore che divide il primo coefficiente. Pertanto $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Chiaramente $1/(\alpha+2) \in \mathbb{Q}(\alpha)$ e $\alpha \in \mathbb{Q}(1/(\alpha+2))$, per cui $\mathbb{Q}(1/(\alpha+2)) = \mathbb{Q}(\alpha)$. Ne segue che il polinomio minimo di $1/(\alpha+2)$ su $\mathbb{Q}$ ha grado 3.

Poniamo $\beta = \alpha + 2$ e $\gamma = 1/\beta = 1/(\alpha+2)$. Poiché α è radice di $f(x)$ si ha che β è radice di $f(x-2) = (x-2)^3 - 3(x-2) + 1 = x^3 - 6x^2 + 15x - 15$, cioè $\beta^3 - 6\beta^2 + 15\beta - 15 = 0$. Moltiplicando quest'ultima relazione per $1/(15\beta^3) \neq 0$ si ottiene

$$\gamma^3 - \gamma^2 + \frac{2}{5}\gamma - \frac{1}{15} = 0$$

ossia che γ è radice del polinomio monico a coefficienti razionali

$$x^3 - x^2 + \frac{2}{5}x - \frac{1}{15}.$$

Visto che questo polinomio ha grado 3, esso è il polinomio minimo di γ su $\mathbb{Q}$.

(ii) Supponiamo che β sia una radice comune di $f(x)$ e $g(x)$ in una chiusura algebrica di $\mathbb{F}_p$. Da $\beta^2 = 2$ segue che $\beta^3 + 3\beta - 1 = 5\beta - 1 = 0$, $5\beta = 1$ e quindi $1 = (5\beta)^2 = 25\beta^2 = 25 \cdot 2 = 50$. Pertanto $1 = 50$ e quindi $p \mid 50 - 1 = 49$, cioè $p = 7$. D'altra parte, se $p = 7$ c'è la radice comune $\beta = 3$.

190. (i) Innanzitutto osserviamo che $f(x)$ è irriducibile in $\mathbb{Z}[x]$ per il Criterio di Eisenstein applicato con primo 2. Allora $f(x)$ è irriducibile anche in $\mathbb{Q}[x]$ per il Lemma di Gauss. Si ha $\alpha^6 + 2 = -4\alpha^3$ e, elevando al quadrato entrambi i membri, $\alpha^{12} + 4\alpha^6 + 4 = 16\alpha^6$, da cui α^2 è radice del polinomio $g(x) = x^6 - 12x^3 + 4$.

Dimostriamo che $g(x)$ è irriducibile. Poiché $\mathbb{Q}(\alpha^2) \subseteq \mathbb{Q}(\alpha)$ e $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^2)] \leq 2$, si ha che $[\mathbb{Q}(\alpha^2) : \mathbb{Q}] = 3, 6$, per cui rimane da escludere solo il caso che $g(x)$ si fattorizzi come prodotto di due polinomi di grado 3.

Usando ancora il Lemma di Gauss, possiamo supporre, per assurdo, che $g(x) = p(x)q(x)$ con p e q due polinomi monici, di grado 3 e a coefficienti interi.

Considerando la riduzione modulo 2, abbiamo necessariamente che $\overline{p} = \overline{q} = x^3$, da cui tutti i coefficienti di p e q, salvo il primo, dovrebbero essere pari. In particolare, i loro termini noti dovrebbero essere entrambi uguali a 2 o entrambi uguali a -2. Scrivendo $p(x) = x^3 + ux^2 + vx \pm 2$, $q(x) = x^3 + u'x^2 + v'x \pm 2$ ed eguagliando i coefficienti di $g(x)$ e di $p(x)q(x)$ si ottiene immediatamente che $u' = -u$, $v' = -v$, per i termini di grado 5 e di grado 1 e $u^2 = v^2 = 0$, per i termini di grado 4 e di grado 2. Siamo quindi giunti ad una contraddizione.

Abbiamo allora $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\alpha)$ e quindi $\mathbb{Q}(1/\alpha^2) = \mathbb{Q}(\alpha^2)$ ha grado 6 su $\mathbb{Q}$. Visto poi che $4(1/\alpha^2)^6 - 12(1/\alpha^2)^3 + 1 = 0$, si deduce che il polinomio minimo di $1/\alpha^2$ su $\mathbb{Q}$ è

$$h(x) = x^6 - 3x^3 + \frac{1}{4}.$$

(ii) Con coefficienti in $\mathbb{F}_7$, si ha $f(x) = (x^3 - 1)(x^3 - 2)$. Controllando poi le eventuali radici dei fattori di terzo grado, si vede che $x^3 - 1 = (x-1)(x-2)(x-4)$, mentre $x^3 - 2$ è irriducibile. Poiché il minimo comune multiplo dei gradi dei fattori irriducibili di $f(x)$ è uguale a 3, il campo di spezzamento di $f(x)$ è uguale a $\mathbb{F}_{7^3}$.

191. Si ha $f(x) = x^6 - 4 = (x^3 + 2)(x^3 - 2)$. Osserviamo che α è una radice del primo fattore se e solo se $-\alpha$ è una radice del secondo fattore. Pertanto il campo di spezzamento di $f(x)$ è lo stesso del campo di spezzamento di $g(x) = x^3 - 2$.

Il polinomio $g(x)$ è irriducibile in $\mathbb{Q}[x]$ per il Criterio di Eisenstein, ed ha una radice reale, $\sqrt[3]{2}$, e due radici complesse coniugate. Il campo di spezzamento $\mathbb{K}$ di $g(x)$ su $\mathbb{Q}$ ha grado al più $3! = 6$ e multiplo di $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Inoltre tale grado non può essere 3, in quanto $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ mentre $\mathbb{K} \not\subseteq \mathbb{R}$. Quindi $[\mathbb{K} : \mathbb{Q}] = 6$.

Il polinomio $g(x)$ non ha radici multiple in $\mathbb{F}_{11}$, in quanto le sue radici sono diverse da zero e $g'(x) = 3x^2$ si annulla solo in 0. Il gruppo moltiplicativo $\mathbb{F}_{11}^*$ è ciclico con 10 elementi. Poiché $(3, 10) = 1$, la mappa $x \longmapsto x^3$ è un isomorfismo. In particolare, è una funzione biiettiva. Ne segue che esiste uno e un solo elemento a tale che $a^3 = 2$, cioè una e una sola radice del polinomio $g(x)$ in $\mathbb{F}_{11}$ e tale radice è semplice. Pertanto i fattori irriducibili di $g(x)$ sono un polinomio di primo grado ed un polinomio di secondo grado, e quindi il grado del campo di spezzamento di $g(x)$ su $\mathbb{F}_{11}$ è 2.

192. Se α è una radice di $f(x) = x^6 + 1$, allora $\alpha^6 = -1$, $\alpha^{12} = 1$ e pertanto l'ordine $\mathrm{ord}(\alpha)$ di α in $\mathbb{F}_p^*$ è un divisore di 12.

Se $\mathrm{ord}(\alpha) = 1$, allora $1^6 + 1 = 0$ e quindi $p = 2$.

Supponiamo ora $p \neq 2$: allora $-1 \neq 1$ e quindi $\mathrm{ord}(\alpha) \nmid 6$. Restano dunque le possibilità $\mathrm{ord}(\alpha) = 4$ e $\mathrm{ord}(\alpha) = 12$. Viceversa, notiamo che se esiste $\alpha \in \mathbb{F}_p$ di ordine 4 allora α è radice del polinomio $x^2 + 1 = (x^4 - 1)/(x^2 - 1)$; poiché questo polinomio divide $f(x)$, allora α è anche radice di $f(x)$. Allo stesso modo se esiste $\alpha \in \mathbb{F}_p$ di ordine 12 allora α è radice del polinomio $f(x) = (x^{12} - 1)/(x^6 - 1)$.

Pertanto esiste una radice di $f(x)$ in $\mathbb{F}_p$ se e solo se $\mathbb{F}_p^*$, che è un gruppo ciclico di ordine $p - 1$, contiene o un elemento di ordine 4 o un elemento di ordine 12, cioè se e solo se $4 \mid p - 1$ oppure $12 \mid p - 1$. Poiché la seconda condizione implica la prima, i primi cercati sono: 2 e tutti i primi p tali che $p \equiv 1 \pmod 4$.

193. (i) Usando che α è una radice di $f(x) = x^4 - 2x^3 + x - 1$ si ha

$$\alpha^4 - 2\alpha^3 + \alpha = 1$$

$$(\alpha^4 - 2\alpha^3 + \alpha)^2 = \alpha^8 - 4\alpha^7 + 4\alpha^6 + 2\alpha^5 - 4\alpha^4 + \alpha^2 = 1$$

$$\alpha^2(\alpha^6 - 4\alpha^5 + 4\alpha^4 + 2\alpha^3 - 4\alpha^2 + 1) = 1.$$

Ne segue che $g(x) = x^6 - 4x^5 + 4x^4 + 2x^3 - 4x^2 + 1$ è uno dei polinomi che risolve il problema.

⟦Il polinomio $g(x)$ trovato non è, comunque, quello di grado minimo; infatti $1/\alpha^2 \in \mathbb{Q}(\alpha)$ e ogni elemento di $\mathbb{Q}(\alpha)$ si può scrivere come un polinomio a coefficienti razionali in α di grado ≤ 3.⟧

(ii) Il polinomio $f(x)$ è irriducibile in $\mathbb{Q}[x]$. Per dimostrare ciò basta far vedere, per il Lemma di Gauss, che esso è irriducibile in $\mathbb{Z}[x]$. Riducendo modulo 2 abbiamo che il polinomio x^4+x+1 è irriducibile in $\mathbb{F}_2[x]$: non ha radici in $\mathbb{F}_2$ e non è il quadrato dell'unico polinomio irriducibile di secondo grado a coefficienti in $\mathbb{F}_2$, x^2+x+1. Quindi $f(x)$ è irriducibile in $\mathbb{Z}[x]$.

Pertanto $f(x)$ è il polinomio minimo di α, $[\mathbb{Q}(\alpha):\mathbb{Q}]=4$ e, poiché $\beta=\alpha^2+k\alpha\in\mathbb{Q}(\alpha)$, $d=[\mathbb{Q}(\beta):\mathbb{Q}]$ è un divisore di 4.

Il grado d non può essere uguale a 1, perché altrimenti $\beta\in\mathbb{Q}$ e quindi α sarebbe radice di un polinomio a coefficienti razionali di grado $2<4$.

Si può avere $d=2$ se e solo se esistono dei numeri razionali a,b, tali che $\beta^2+a\beta+b=0$, ossia

$$\alpha^4+2k\alpha^3+(1+a)\alpha^2+ka\alpha+b=0.$$

Questo succede se e solo se $x^4+2kx^3+(1+a)x^2+kax+b$ è un multiplo di $f(x)$. Poiché entrambi i polinomi sono monici e dello stesso grado, questo significa $2k=-2$, $1+a=0$, $ka=1$, $b=1$, ossia $k=-1$, $a=-1$, $b=1$.

In conclusione, il grado cercato è 2 per $k=-1$ e 4 altrimenti.

194. Per prima cosa osserviamo che il polinomio $f(x)=x^4+2x^2+2$ è irriducibile su $\mathbb{Q}$ per il Criterio di Eisenstein con primo 2, quindi $[\mathbb{Q}[\alpha]:\mathbb{Q}]=4$.

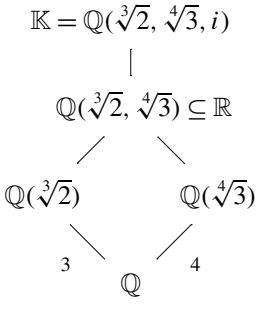
Il polinomio minimo di α^2 è x^2+2x+2, in quanto esso è monico, si annulla in α^2 ed è irriducibile. Quindi il polinomio minimo di α^2+1 è $(x-1)^2+2(x-1)+2=x^2+1$.

Il polinomio $(x-2)^4+2(x-2)^2+2=x^4-8x^3+26x^2-40x+26$ si annulla in $\alpha+2$, quindi il suo reciproco, $26x^4-40x^3+26x^2-8x+1$ si annulla in $1/(\alpha+2)$.

Osserviamo che $\mathbb{Q}(1/(\alpha+2))=\mathbb{Q}(\alpha+2)=\mathbb{Q}(\alpha)$; quindi il polinomio minimo di $1/(\alpha+2)$ ha grado 4. Per quanto visto possiamo concludere che tale polinomio minimo è

$$x^4-\frac{20}{13}x^3+x^2-\frac{4}{13}x+\frac{1}{26}.$$

195. Il polinomio x^3-2 è irriducibile su $\mathbb{Q}$ in quanto ha grado 3 e non ha radici razionali. Le sue radici in $\mathbb{C}$ sono $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta$, $\sqrt[3]{2}\zeta^2$ dove $\zeta=\frac{-1}{2}+\frac{\sqrt{-3}}{2}$ è una radice terza primitiva dell'unità.



Il polinomio x^4-3 è irriducibile su $\mathbb{Q}$ per il Criterio di Eisenstein con primo 3 e per il Lemma di Gauss e le sue radici in $\mathbb{C}$ sono $\sqrt[4]{3}$, $i\sqrt[4]{3}$, $-\sqrt[4]{3}$, $-i\sqrt[4]{3}$. Si verifica facilmente che il campo di spezzamento di $f(x)=(x^3-2)(x^4-3)$ su $\mathbb{Q}$ è quindi il $\mathbb{K}=\mathbb{Q}(\sqrt[3]{2},\sqrt[4]{3},i)$.

Sappiamo che $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$ e che $[\mathbb{Q}(\sqrt[4]{3}):\mathbb{Q}]=4$, quindi $12=[3,4]$ divide $[\mathbb{Q}(\sqrt[3]{2},\sqrt[4]{3}):\mathbb{Q}]\leq 12$. Ne segue che $[\mathbb{Q}(\sqrt[3]{2},\sqrt[4]{3}):\mathbb{Q}]=12$. Inoltre $[\mathbb{K}:\mathbb{Q}(\sqrt[3]{2},\sqrt[4]{3})]=2$ perché $\mathbb{K}$ si ottiene aggiungendo i al campo reale $\mathbb{Q}(\sqrt[3]{2},\sqrt[4]{3})$. Concludiamo $[\mathbb{K}:\mathbb{Q}]=24$.

In $\mathbb{F}_3$ si ha $f(x) = (x-2)^3x^4$ e quindi il campo di spezzamento è $\mathbb{F}_3$. In $\mathbb{F}_{11}$ il polinomio $x^3 - 2$ si spezza come un polinomio di grado 1 per uno di grado 2 irriducibile: infatti basta notare che l'endomorfismo di $\mathbb{F}_{11}^*$ definito da $a \mapsto a^3$ è un automorfismo. D'altra parte $x^4 - 3$ si spezza come $(x^2-5)(x^2+5)$ e quindi, indipendentemente dal fatto che questi due fattori si spezzino ulteriormente o meno, il minimo comune multiplo dei gradi dei fattori irriducibili di $f(x)$ è 2. Il campo di spezzamento cercato è quindi $\mathbb{F}_{11^2}$.

196. (i) Con un semplice calcolo otteniamo $\alpha^2 = 2(2+i\sqrt{5})$ e $\alpha^4 = 4(-1+4i\sqrt{5})$, da cui $\alpha^4 - 8\alpha^2 + 36 = 0$. Quindi α è radice del polinomio $f(x) = x^4 - 8x^2 + 36$.

Tale polinomio $f(x)$ è irriducibile su $\mathbb{Q}$: infatti ha sicuramente α e $\overline{\alpha} = \sqrt{5} - i$ come radici, inoltre poiché contiene solo monomi di grado pari, anche $-\alpha = -\sqrt{5} - i$, e di conseguenza $-\overline{\alpha} = -\sqrt{5} + i$, sono radici di $f(x)$.

Ne segue che $f(x)$ non ha radici razionali e neppure fattori razionali di grado 2, in quanto i fattori reali di grado 2 sono $(x-\alpha)(x-\overline{\alpha}) = x^2 - 2\sqrt{5}x + 6$ e $(x+\alpha)(x+\overline{\alpha}) = x^2 + 2\sqrt{5}x + 6$ e questi non sono razionali. Quindi $f(x)$ è il polinomio minimo di α.

(ii) Il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ è $\mathbb{K} = \mathbb{Q}(\alpha, \overline{\alpha}, -\alpha, -\overline{\alpha})$.

$$\begin{array}{c} \mathbb{K} = \mathbb{Q}(\sqrt{5}, i) \\ 2 \,\big|\, \\ \mathbb{Q}(\sqrt{5}) \subseteq \mathbb{R} \\ 2 \,\big|\, \\ \mathbb{Q} \end{array}$$

È immediato verificare che $\mathbb{K} = \mathbb{Q}(\sqrt{5}, i)$, infatti chiaramente $\mathbb{K} \subseteq \mathbb{Q}(\sqrt{5}, i)$ e inoltre $\sqrt{5} = (\alpha + \overline{\alpha})/2$, $i = (\alpha - \overline{\alpha})/2 \in \mathbb{K}$. Osserviamo che $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$ visto che $x^2 - 5$ è irriducibile per il Criterio di Eisenstein e si annulla su $\sqrt{5}$. Inoltre $[\mathbb{Q}(\sqrt{5})(i) : \mathbb{Q}(\sqrt{5})] = 2$ in quanto i è radice di $x^2 - 1$ ma $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{R}$ mentre $i \notin \mathbb{R}$. Allora $[\mathbb{K} : \mathbb{Q}] = [\mathbb{Q}(\sqrt{5})(i) : \mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2 \cdot 2 = 4$.

Su $\mathbb{F}_7$ si ha $f(x) = x^4 - x^2 + 1 = (x^2-3)(x^2-5)$. Poiché i quadrati di $\mathbb{F}_7$ sono $0, 1, 2, 4$, $x^2 - 3$ e $x^2 - 5$ sono irriducibili, ed il campo di spezzamento di $f(x)$ è quindi $\mathbb{F}_{7^2}$.

197. Il polinomio $f(x) = x^4 - x - 1$ è irriducibile in $\mathbb{F}_2[x]$, infatti non ha radici perché le classi di 0 e 1 non annullano il polinomio, e non è prodotto di due fattori irriducibili di secondo grado perché non è il quadrato dell'unico polinomio $x^2 + x + 1$ irriducibile di grado 2 di $\mathbb{F}_2[x]$. Ne segue che $f(x)$ è irriducibile in $\mathbb{Z}[x]$ e quindi, per il Lemma di Gauss, in $\mathbb{Q}[x]$. Concludiamo che $f(x)$ è il polinomio minimo di α su $\mathbb{Q}$ e $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

Visto che $\mathbb{Q}(\alpha) = \mathbb{Q}(2\alpha - 1)$, il polinomio minimo di $2\alpha - 1$ su $\mathbb{Q}$ ha grado 4. Allora il polinomio $g(x) = 2^4 f((x+1)/2) = x^4 + 4x^3 + 6x^2 - 4x - 23$ è il polinomio minimo di $2\alpha - 1$ visto che si annulla su questo elemento, è monico e ha il grado minimo.

Sia $\beta = \alpha^2$, allora $\mathbb{Q} \subseteq \mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$ e si calcola che $\beta^2 = \alpha + 1$, $\beta^3 = \alpha^3 + \alpha^2$ e $\beta^4 = \alpha^2 + 2\alpha + 1$. Visto che $1, \alpha, \alpha^2, \alpha^3$ sono linearmente indipendenti su $\mathbb{Q}$, si verifica subito che anche $1, \beta, \beta^2, \beta^3$ lo sono. In particolare, β ha grado 4 su $\mathbb{Q}$.

Sia quindi $h(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Z}[x]$ il polinomio minimo di β: allora $0 = h(\beta) = \beta^4 + a\beta^3 + b\beta^2 + c\beta + d = a\alpha^3 + (1 + a + c)\alpha^2 + (2 + b)\alpha + 1 + b + d$. Usando l'indipendenza lineare di $1, \alpha, \alpha^2, \alpha^3$ otteniamo

$$\begin{cases} a = 0 \\ 1 + a + c = 0 \\ 2 + b = 0 \\ 1 + b + d = 0 \end{cases}$$

che ha soluzione $a = 0, b = -2, c = -1, d = 1$. Il polinomio minimo di β è quindi $h(x) = x^4 - 2x^2 - x + 1$.

198. Poiché il polinomio $f(x) = x^4 - 6x^2 - 3$ è biquadratico, usando la formula risolutiva per i polinomi di secondo grado, si calcola che le radici di $f(x)$ sono $\pm\sqrt{3 \pm 2\sqrt{3}}$. Il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ è quindi $\mathbb{K} = \mathbb{Q}(\sqrt{3 + 2\sqrt{3}}, \sqrt{3 - 2\sqrt{3}})$ e $[\mathbb{K} : \mathbb{Q}] = [\mathbb{K} : \mathbb{Q}(\sqrt{3 + 2\sqrt{3}})][\mathbb{Q}(\sqrt{3 + 2\sqrt{3}}) : \mathbb{Q}]$.

$$\begin{array}{c} \mathbb{K} = \mathbb{Q}(\sqrt{3 + 2\sqrt{3}}, \sqrt{3 - 2\sqrt{3}}) \\ | \\ \mathbb{Q}(\sqrt{3 + 2\sqrt{3}}) \subseteq \mathbb{R} \\ | \\ \mathbb{Q} \end{array}$$

Il polinomio f è irriducibile in $\mathbb{Z}[x]$ per il Criterio di Eisenstein con primo 3 e, quindi, è irriducibile anche in $\mathbb{Q}[x]$ per il Lemma di Gauss. Allora è il polinomio minimo delle sue radici; in particolare $[\mathbb{Q}(\sqrt{3 + 2\sqrt{3}}) : \mathbb{Q}] = 4$. Osserviamo inoltre che $3 - 2\sqrt{3} = (\sqrt{3 - 2\sqrt{3}})^2 \in \mathbb{Q}(\sqrt{3 - 2\sqrt{3}})$ ma si ha $\sqrt{3 - 2\sqrt{3}} \notin \mathbb{Q}(\sqrt{3 + 2\sqrt{3}})$ perché $\sqrt{3 - 2\sqrt{3}} \notin \mathbb{R}$ mentre $\mathbb{Q}(\sqrt{3 + 2\sqrt{3}}) \subseteq \mathbb{R}$. Ne segue che $[\mathbb{K} : \mathbb{Q}(\sqrt{3 + 2\sqrt{3}})] = 2$, e quindi$[\mathbb{K} : \mathbb{Q}] = 8$.

In $\mathbb{F}_{13}[x]$ si ha $f(x) = (x^2 - 8)(x^2 + 2)$ e questi fattori sono irriducibili perché 8 e -2 non sono quadrati in $\mathbb{F}_{13}$. Il campo di spezzamento di $f(x)$ su $\mathbb{F}_{13}$ è, quindi, $\mathbb{F}_{13^2}$ ed ha grado 2 su $\mathbb{F}_{13}$.

199. (i) Elevando α al quadrato si ottiene $\alpha^2 - 2 = \sqrt{7}$ da cui $\alpha^4 - 4\alpha^2 - 3 = 0$, cioè α annulla il polinomio $f(x) = x^4 - 4x^2 - 3$. Se dimostriamo che $f(x)$ è irriducibile su $\mathbb{Q}$ otteniamo che esso è il polinomio minimo di α e di conseguenza $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

Essendo il polinomio $f(x)$ biquadratico, si calcola facilmente che le sue radici sono $\pm\sqrt{2 \pm \sqrt{7}}$; mostriamo che esse non sono razionali. Infatti se $\pm\sqrt{2 \pm \sqrt{7}}$ fosse razionale allora, elevando al quadrato, troveremmo che lo sarebbe anche $\sqrt{7}$, cosa ovviamente falsa. Inoltre $\pm\sqrt{2 + \sqrt{7}}$ sono reali mentre $\pm\sqrt{2 - \sqrt{7}}$ sono due numeri non reali e complessi coniugati.

D'altra parte, se $f(x)$ fosse il prodotto di due polinomi irriducibili di secondo grado, allora, necessariamente, uno dei due fattori dovrebbe essere $(x - \sqrt{2 - \sqrt{7}})(x + \sqrt{2 - \sqrt{7}})$ che, invece, non ha coefficienti razionali perché, ad esempio, il suo termine noto $-2 + \sqrt{7} \notin \mathbb{Q}$.

(ii) Sia $\mathbb{K}$ il campo di spezzamento di $f(x)$ su $\mathbb{Q}$.

$$\begin{array}{c} \mathbb{K} = \mathbb{Q}(\sqrt{2+\sqrt{7}}, \sqrt{2-\sqrt{7}}) \\ | \\ \mathbb{Q}(\sqrt{2+\sqrt{7}}) \subseteq \mathbb{R} \\ 4 \; | \\ \mathbb{Q} \end{array}$$

Per quanto detto al punto precedente si ha $\mathbb{K} = \mathbb{Q}(\sqrt{2+\sqrt{7}}, \sqrt{2-\sqrt{7}})$ e quindi $[\mathbb{K} : \mathbb{Q}] = [\mathbb{K} : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$. Osserviamo che $[\mathbb{K} : \mathbb{Q}(\alpha)] = 2$: infatti $\mathbb{K} = \mathbb{Q}(\alpha)(\sqrt{2-\sqrt{7}})$ e $(\sqrt{2-\sqrt{7}})^2 = 2 - \sqrt{7} \in \mathbb{Q}(\alpha)$, inoltre $\mathbb{K}$ non essendo reale non può coincidere con $\mathbb{Q}(\alpha)$ che è contenuto in $\mathbb{R}$. Ne segue che $[\mathbb{K} : \mathbb{Q}] = 8$.

200. (i) Elevando al quadrato entrambi i membri dell'equazione che definisce α si ottiene $\alpha^2 = 2 + i\sqrt{2}$, da cui $\alpha^2 - 2 = i\sqrt{2}$. Elevando nuovamente al quadrato, si ha $\alpha^4 - 4\alpha^2 + 4 = -2$ e quindi α è radice del polinomio $h(x) = x^4 - 4x^2 + 6$.

Per il Criterio di Eisenstein con primo 2, questo polinomio è irriducibile in $\mathbb{Z}[x]$ e quindi anche in $\mathbb{Q}[x]$ per il Lemma di Gauss. Essendo monico, $h(x)$ è il polinomio minimo di α su $\mathbb{Q}$.

Dall'espressione precedente si ricava che $p(x) = x^2 - 4x + 6$ si annulla in α^2. Ne segue che il polinomio $q(x) = p(x-1) = (x-1)^2 - 4(x-1) + 6 = x^2 - 6x + 11$ si annulla in $\alpha^2 + 1$. Anche $q(x)$ è monico e irriducibile in $\mathbb{Q}[x]$, infatti le sue radici non sono reali e quindi neanche razionali. Ne segue che $q(x)$ è il polinomio minimo di $\alpha^2 + 1$ su $\mathbb{Q}$.

(ii) Da $h(\alpha) = 0$ si ricava $(\alpha^2 + 2\alpha)(\alpha^2 - 2\alpha) = \alpha^4 - 4\alpha^2 = -6$, e quindi $(\alpha^2 + 2\alpha)^{-1} = -(\alpha^2 - 2\alpha)/6$.

Allora il polinomio $f(x) = -(x^2 - 2x)/6$ soddisfa le condizioni richieste.

201. In generale, il campo di spezzamento di un polinomio della forma $x^n - a$ su un campo $\mathbb{K}$ di caratteristica zero o prima con n, è dato da $\mathbb{F} = \mathbb{K}(\alpha, \zeta)$ dove α è una radice n–esima di a e ζ è una radice n–esima primitiva di 1.

$$\begin{array}{c} \mathbb{K} = \mathbb{Q}(\sqrt[4]{2}, i) \\ | \\ \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R} \\ 4 \; | \\ \mathbb{Q} \end{array}$$

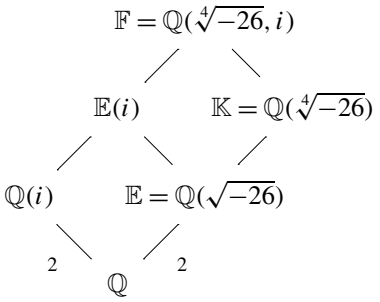
Nel nostro caso si può scegliere $\alpha = \sqrt[8]{4} = \sqrt[4]{2}$ e $\zeta = e^{2\pi i/8} = \frac{\sqrt{2}}{2}(1+i)$. Poiché α è radice del polinomio $x^4 - 2$, irriducibile in $\mathbb{Q}[x]$ per il Lemma di Gauss e il Criterio di Eisenstein con primo 2, si ha $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Osserviamo ora che $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ mentre ζ non è reale, e quindi $\mathbb{Q}(\alpha) \neq \mathbb{F}$, ossia $[\mathbb{F} : \mathbb{Q}(\alpha)] > 1$. Inoltre $\sqrt{2} = \alpha^2 \in \mathbb{Q}(\alpha)$ e quindi $\mathbb{F} \subseteq \mathbb{Q}(\alpha, i)$. L'unità immaginaria i è radice del polinomio $x^2 + 1 \in \mathbb{Q}(\alpha)[x]$, quindi $[\mathbb{F} : \mathbb{Q}(\alpha)] \leq [\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] \leq 2$.

Ne segue che $[\mathbb{F} : \mathbb{Q}] = [\mathbb{F} : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 4 = 8$.

Per $\mathbb{K} = \mathbb{F}_3$ il polinomio si può anche scrivere come $x^8 - 1$, pertanto il campo di spezzamento è $\mathbb{F}_3(\zeta)$. Un campo $\mathbb{F}_{3^n}$ contiene ζ se e soltanto se il suo gruppo moltiplicativo $\mathbb{F}_{3^n}^*$, che è ciclico di ordine $3^n - 1$, contiene un sottogruppo di ordine 8, ossia se e solo se $8 \mid 3^n - 1$. Il più piccolo n per cui questo si verifica è $n = 2$; quindi il campo di spezzamento cercato è $\mathbb{F}_9$, di grado 2 su $\mathbb{F}_3$.

202. Il polinomio $f(x) = x^4 + 26$ è irriducibile in $\mathbb{Q}[x]$ grazie al Lemma di Gauss visto che lo è in $\mathbb{Z}[x]$ per il Criterio di Eisenstein con primo 2. Pertanto, se α è una

radice complessa di $f(x)$ e $\mathbb{K} = \mathbb{Q}(\alpha)$, si ha $[\mathbb{K} : \mathbb{Q}] = 4$. Le radici di $f(x)$ sono $\pm\alpha, \pm i\alpha$, quindi il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ è $\mathbb{F} = \mathbb{K}(i)$. Poiché i ha grado 2 su $\mathbb{Q}$, si ha $[\mathbb{F} : \mathbb{K}] \leq 2$.



Consideriamo ora $\beta = i\sqrt{26}$ e poniamo $\mathbb{E} = \mathbb{Q}(\beta)$ e scegliamo $\alpha = \pm\sqrt{\beta}$. Si ha evidentemente $[\mathbb{E} : \mathbb{Q}] = 2$ e $[\mathbb{K} : \mathbb{E}] = 2$. Osserviamo che $\mathbb{E} \neq \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$, perché due estensioni di un campo con le radici quadrate di due elementi coincidono se e solo se il prodotto di questi due elementi è un quadrato in tale campo, mentre $(-1)(-26) = 26$ non è il quadrato di un numero razionale. Quindi sia $\mathbb{K}$ che $\mathbb{E}(i)$ sono due estensioni quadratiche di $\mathbb{E}$.

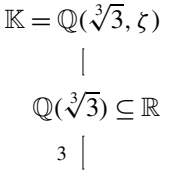
Per lo stesso criterio, esse sono distinte, in quanto $(-1)(i\sqrt{26})$ non è un quadrato in $\mathbb{E}$: infatti una radice quadrata di $-i\sqrt{26}$ è una radice di $f(x)$ e quindi ha grado 4 su $\mathbb{Q}$ e non può appartenere ad $\mathbb{E}$. Pertanto $i \notin \mathbb{K}$ e quindi $[\mathbb{F} : \mathbb{Q}] = [\mathbb{F} : \mathbb{K}][\mathbb{K} : \mathbb{Q}] = 2 \cdot 4 = 8$.

Per quanto riguarda il grado del campo di spezzamento di $f(x)$ su un campo finito, basta fare il minimo comune multiplo dei gradi dei fattori irriducibili di $f(x)$ su tale campo.

Su $\mathbb{F}_5$ si ha $x^4 + 26 = x^4 - 4 = (x^2 - 2)(x^2 + 2)$ e i fattori di secondo grado sono irriducibili perché non hanno radici in $\mathbb{F}_5$. Pertanto il grado del campo di spezzamento è 2.

Su $\mathbb{F}_7$ si ha $x^4 + 26 = x^4 - 9 = (x^2 + 3)(x^2 - 3) = (x^2 - 4)(x^2 - 3) = (x + 2)(x - 2)(x^2 - 3)$ ed il fattore di secondo grado è irriducibile perché non ha radici in $\mathbb{F}_7$. Pertanto il grado del campo di spezzamento è 2.

203. Si ha $f(x) = x^6 - 12x^3 + 27 = (x^3 - 3)(x^3 - 9)$.



Il polinomio $x^3 - 3$ è irriducibile in $\mathbb{Z}[x]$ per il Criterio di Eisenstein applicato con primo 3; quindi esso è irriducibile anche in $\mathbb{Q}[x]$ per il Lemma di Gauss. Chiamando $\mathbb{K}$ il campo di spezzamento di $x^3 - 3$, si ha $\mathbb{K} = \mathbb{Q}(\sqrt[3]{3}, \zeta)$, dove ζ è una radice terza primitiva di 1. Dall'irriducibilità di $x^3 - 3$ si ottiene $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$. Poiché inoltre $\mathbb{Q}(\sqrt[3]{3}) \subseteq \mathbb{R}$ mentre ζ non è reale, il grado di $\mathbb{K}$ su $\mathbb{Q}$ è maggiore di 3. Infine, dovendo questo grado essere minore o uguale a $3! = 6$, esso è 6.

Analogamente, il campo di spezzamento $\mathbb{F}$ del polinomio $x^3 - 9$ è $\mathbb{Q}(\sqrt[3]{9}, \zeta)$. Ma $\sqrt[3]{9} = \sqrt[3]{3}^2 \in \mathbb{K}$, $\zeta \in \mathbb{K}$ e pertanto $\mathbb{F} \subseteq \mathbb{K}$. Concludiamo che il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ è uguale a $\mathbb{K}$ e ha quindi grado 6 su $\mathbb{Q}$.

In $\mathbb{F}_5[x]$ si ha $f(x) = (x^3 - 3)(x^3 - 9) = (x - 2)(x^2 + 2x - 1)(x + 1)(x^2 - x + 1)$ visto che $2^3 \equiv 3$ e $(-1)^3 \equiv 9 \pmod 5$. Inoltre $x^2 + 2x - 1$ e $x^2 - x + 1$ sono irriducibili non avendo radici in $\mathbb{F}_5$.

Pertanto il grado del campo di spezzamento di $f(x)$ su $\mathbb{F}_5$ è 2, ossia il minimo comune multiplo dei gradi dei suoi fattori irriducibili.

204. Elevando al quadrato $\alpha = \sqrt{2+\sqrt{3}}$ si ottiene $\alpha^2 = 2+\sqrt{3}$, da cui $\alpha^2 - 2 = \sqrt{3}$ e, elevando ancora al quadrato, $\alpha^4 - 4\alpha^2 + 4 = 3$. Ne segue che α è radice del polinomio $f(x) = x^4 - 4x^2 + 1$.

Si osservi che partendo da $\beta = \sqrt{2-\sqrt{3}}$ e ripetendo lo stesso procedimento seguito per α, si giunge ancora ad $f(x)$. Quindi $f(x)$ ha per radici $\pm\alpha$ e $\pm\beta$.

La fattorizzazione di $f(x)$ in $\mathbb{C}[x]$ è dunque $(x-\alpha)(x+\alpha)(x-\beta)(x+\beta)$. Visto che i quadrati di $\pm\alpha$ e $\pm\beta$ sono evidentemente irrazionali, allora lo sono anche $\pm\alpha$ e $\pm\beta$; quindi $f(x)$ non ha fattori di primo grado in $\mathbb{Q}[x]$.

Se esso si scomponesse nel prodotto di due polinomi di secondo grado, quello dei due che ha per radice α dovrebbe essere uno dei seguenti: $(x-\alpha)(x+\alpha)$, $(x-\alpha)(x-\beta)$, $(x-\alpha)(x+\beta)$.

Il primo di tali polinomi non ha coefficienti razionali in quanto, come già osservato, α^2 non è razionale. Analogamente il secondo non è a coefficienti razionali in quanto $(\alpha+\beta)^2 = (\sqrt{2+\sqrt{3}} + \sqrt{2-\sqrt{3}})^2 = 6$ e quindi $\alpha+\beta \notin \mathbb{Q}$. Infine, neanche il terzo polinomio ha coefficienti razionali visto che $(\alpha-\beta)^2 = (\sqrt{2+\sqrt{3}} - \sqrt{2-\sqrt{3}})^2 = 2$.

Il campo di spezzamento di $f(x)$ è $\mathbb{K} = \mathbb{Q}(\alpha, \beta)$, perché evidentemente $-\alpha, -\beta \in \mathbb{K}$. Si osservi però che $\alpha\beta = 1$, e quindi $\beta = 1/\alpha \in \mathbb{Q}(\alpha)$. Pertanto $\mathbb{K} = \mathbb{Q}(\alpha)$, ed essendo il polinomio minimo di α su $\mathbb{Q}$ di grado 4, si ha $[\mathbb{K} : \mathbb{Q}] = 4$.

205. (i) È facile controllare che il polinomio $x^3 - 7$ è irriducibile in $\mathbb{Q}[x]$, infatti esso è di terzo grado e, visto che ± 1 e ± 7 non sono radici, non ha radici razionali. Inoltre le sue radici sono $\sqrt[3]{7}$, $\sqrt[3]{7}\zeta$, $\sqrt[3]{7}\zeta^2$, dove $\zeta = (-1+\sqrt{-3})/2$ è una radice terza primitiva di 1.

$$\begin{array}{c} \mathbb{K} = \mathbb{Q}(\sqrt[3]{7}, \zeta) \\ | \\ \mathbb{Q}(\sqrt[3]{7}) \subseteq \mathbb{R} \\ {\scriptstyle 3}\ | \\ \mathbb{Q} \end{array}$$

Se $\mathbb{K}$ è il campo di spezzamento di $x^3 - 7$; avendo tale polinomio grado 3 si ha $[\mathbb{K} : \mathbb{Q}] \leq 3! = 6$ ed essendo un polinomio irriducibile $[\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}] = 3$. Ma $\mathbb{Q}(\sqrt[3]{7}) \subseteq \mathbb{K}$ e non ci può essere uguaglianza, in quanto $\mathbb{Q}(\sqrt[3]{7}) \subseteq \mathbb{R}$ e $\mathbb{K}$ contiene anche le radici non reali del polinomio. Allora necessariamente $[\mathbb{K} : \mathbb{Q}] = 6$. Il polinomio $x^2 + 3$ è anch'esso irriducibile in $\mathbb{Q}[x]$ e il suo campo di spezzamento è evidentemente $\mathbb{Q}(\sqrt{-3})$. Ora, da $\sqrt{-3} = \zeta - \zeta^2$, si vede che $\sqrt{-3} \in \mathbb{K}$ e quindi $\mathbb{Q}(\sqrt{-3}) \subseteq \mathbb{K}$.

Concludiamo che il campo di spezzamento di $f(x)$ coincide con $\mathbb{K}$ ed ha grado 6 su $\mathbb{Q}$.

(ii) Sappiamo che ogni elemento di $A = \mathbb{F}_5[x]/(f(x))$ è la classe di un polinomio di grado minore o uguale a 4, inoltre la classe di $g(x)$ è un divisore di zero in A se e solo se $g(x)$ non è primo con $f(x)$. Controllando le possibili radici, troviamo che la fattorizzazione di $f(x)$ in $\mathbb{F}_5[x]$ è $f(x) = (x-3)(x^2+3x-1)(x^2+3)$.

Osserviamo che le classi multiple di un fissato polinomio $h(x)$ di grado d sono del tipo $h(x)k(x)$, dove $k(x)$ è un qualsiasi polinomio di grado $4-d$; il loro numero

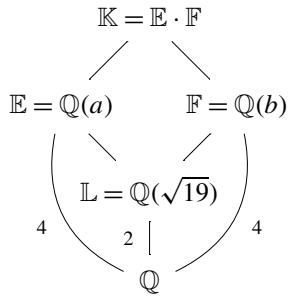
è quindi 5^{5-d}. Usando questa osservazione per calcolare i multipli dei vari prodotti dei fattori irriducibili di $f(x)$ e il Principio di Inclusione Esclusione, contiamo i multipli di $x-3$, i multipli di x^2+3x-1 e i multipli di x^2+3, poi sottraiamo i multipli di $(x-3)(x^2+3x-1)$, i multipli di $(x-3)(x^2+3)$ e di $(x^2+3x-1)(x^2+3)$ e sommiamo infine i multipli di $(x-3)(x^2+3x-1)(x^2+3)$. Troviamo che il numero di divisori di zero in A è

$$5^4+5^3+5^3-(5^2+5^2+5)+1=821.$$

206. Facciamo innanzitutto vedere che $f(x)=2x^4+6x^2-5$ è irriducibile in $\mathbb{Q}[x]$.

In $\mathbb{C}[x]$ si ha $f(x)=2(x^2-\alpha)(x^2-\beta)=2(x-a)(x+a)(x-b)(x-b)$ dove $\alpha=(-3+\sqrt{19})/2$ e $\beta=(-3-\sqrt{19})/2$ sono le due radici dell'equazione $2y^2+6y-5=0$, $a^2=\alpha$, $b^2=\beta$. Visto che α e β non sono razionali, non lo sono neanche a e b, pertanto $f(x)$ non ha fattori irriducibili di primo grado.

Inoltre b non è reale, quindi ogni polinomio a coefficienti razionali che abbia per radice b deve avere per radice il coniugato $\overline{b}=-b$. Ne segue che l'unica eventuale scomposizione di $f(x)$ come prodotto di due polinomi di secondo grado a coefficienti razionali è $2(x^2-\alpha)(x^2-\beta)$. Ma questa non è una scomposizione in $\mathbb{Q}[x]$, in quanto α e β non sono razionali.



Usiamo le seguenti notazioni: $\mathbb{L}=\mathbb{Q}(\alpha)=\mathbb{Q}(\beta)=\mathbb{Q}(\sqrt{19})$, $\mathbb{E}=\mathbb{Q}(a)$, $\mathbb{F}=\mathbb{Q}(b)$, $\mathbb{K}=\mathbb{E}\mathbb{F}=\mathbb{Q}(a,b)$.

Evidentemente $\mathbb{K}$ è il campo di spezzamento del polinomio. Per l'irriducibilità di $f(x)$ si ha $[\mathbb{E}:\mathbb{Q}]=[\mathbb{F}:\mathbb{Q}]=4$, da cui $[\mathbb{E}:\mathbb{L}]=[\mathbb{F}:\mathbb{L}]=2$. Poiché $\mathbb{E}\mathbb{F}=\mathbb{E}(b)$ e b ha grado 2 su $\mathbb{L}$, allora il grado di b su $\mathbb{E}$ è minore o uguale a 2, e, in particolare, è uguale a 1 se $b\in\mathbb{E}$, cioè se $\mathbb{E}=\mathbb{F}$, e uguale a 2 altrimenti.

Ma $\mathbb{E}=\mathbb{L}(\sqrt{\alpha})$, $\mathbb{F}=\mathbb{L}(\sqrt{\beta})$, e quindi $\mathbb{E}=\mathbb{F}$ se e solo se $\alpha\beta=-5/2$ è un quadrato in $\mathbb{L}$. Ciò è chiaramente impossibile in quanto $\mathbb{L}\subseteq\mathbb{R}$ e un quadrato in $\mathbb{R}$ è non negativo.

Concludendo, $\mathbb{E}\neq\mathbb{F}$, $[\mathbb{E}\mathbb{F}:\mathbb{E}]=2$ e quindi $[\mathbb{K}:\mathbb{Q}]=[\mathbb{E}\mathbb{F}:\mathbb{E}][\mathbb{E}:\mathbb{Q}]=2\cdot 4=8$.

⟦In modo equivalente, possiamo provare che $[\mathbb{E}(b):\mathbb{E}]>1$ anche osservando che $E=\mathbb{Q}(a)=\mathbb{Q}(\sqrt{(-3+\sqrt{19})/2})\subseteq\mathbb{R}$, mentre $b=\sqrt{(3-\sqrt{19})/2}\notin\mathbb{R}$.⟧

Il calcolo di α e β dice che, in $\mathbb{F}_{19}[x]$, si ha $f(x)=2(x^2+3\cdot 2^{-1})^2=2(x^2-8)^2$. Per controllo diretto, si vede poi che x^2-8 non ha radici in $\mathbb{F}_{19}$ e quindi $f(x)$ si fattorizza come un prodotto di fattori di secondo grado in $\mathbb{F}_{19}[x]$. Pertanto il grado del campo di spezzamento di $f(x)$ su $\mathbb{F}_{19}$ è 2.

207. Il polinomio $f(x)$ è irriducibile in $\mathbb{Q}[x]$ per il Criterio di Eisenstein rispetto al primo 3. Dunque $[\mathbb{Q}(\alpha):\mathbb{Q}]=5$. Poiché $\alpha^7\in\mathbb{Q}(\alpha)$, abbiamo $\mathbb{Q}\subseteq\mathbb{Q}(\alpha^7)\subseteq\mathbb{Q}(\alpha)$ e dunque $[\mathbb{Q}(\alpha^7):\mathbb{Q}]\mid 5$. Se $[\mathbb{Q}(\alpha^7):\mathbb{Q}]$ fosse 1, allora α^7 sarebbe razionale. Ma da

$\alpha^5 + 3\alpha + 3 = 0$ segue che $\alpha^7 = -3\alpha^3 - 3\alpha^2$, e questo numero non è razionale in quanto gli elementi $1, \alpha^2, \alpha^3$ sono linearmente indipendenti su $\mathbb{Q}$ visto che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$. Pertanto si ha anche $[\mathbb{Q}(\alpha^7) : \mathbb{Q}] = 5$.

Fattorizziamo $f(x)$ in $\mathbb{F}_2[x]$. È chiaro che $f(x)$ non ha radici; d'altra parte è divisibile per l'unico polinomio irriducibile di secondo grado $x^2 + x + 1$, da cui la fattorizzazione $f(x) = (x^2 + x + 1)(x^3 + x^2 + 1)$. Ne segue che $[\mathbb{F}_2(\alpha) : \mathbb{F}_2]$ è uguale a 2 o a 3, a seconda che α sia radice del primo o del secondo fattore.

Notiamo poi che, nel primo caso, $\alpha \in \mathbb{F}_4^*$, che è un gruppo ciclico di 3 elementi: pertanto $\alpha^7 = \alpha$ e $[\mathbb{F}_2(\alpha^7) : \mathbb{F}_2] = 2$. Nel secondo caso, invece, $\alpha \in \mathbb{F}_8^*$, che è un gruppo ciclico di 7 elementi: pertanto $\alpha^7 = 1$ e $[\mathbb{F}_2(\alpha^7) : \mathbb{F}_2] = 1$.

208. È noto che un elemento $\overline{g(x)} \in A$ è un divisore di zero se e solo se $(g(x), f(x)) \neq 1$. In altre parole, un elemento $\overline{g(x)}$ è un divisore di zero se e solo se $g(x)$ è divisibile per *almeno uno* dei fattori irriducibili di $f(x)$.

Sappiamo inoltre che $\overline{g(x)}$ è nilpotente se e solo se $g(x)$ è divisibile per *tutti* i fattori irriducibili di $f(x)$.

Riassumendo: se $f(x) = p(x)^k$ è una potenza di un polinomio irriducibile, allora ogni divisore di zero è rappresentato da un polinomio $g(x)$ multiplo di $p(x)$, e quindi nilpotente. Se invece $f(x)$ è divisibile per almeno due irriducibili distinti $p(x), q(x)$, allora l'elemento $\overline{p(x)}$ è un divisore di zero ma non è nilpotente.

209. La fattorizzazione di $f(x)$ in $\mathbb{F}_5[x]$ è

$$x^3 - 2x + 1 = (x - 1)(x - 2)^2.$$

I divisori di zero in $\mathbb{F}_5[x]/(x^3 - 2x + 1)$ sono l'unione delle classi dei polinomi multipli di $x - 1$ e dei polinomi multipli di $x - 2$. Le classi dei polinomi multipli di $x - 1$ sono del tipo $(x - 1)(ax + b)$ con $a, b \in \mathbb{F}_5$ e sono pertanto 25, cioè tante quante le possibili scelte della coppia ordinata (a, b). Analogamente, le classi dei polinomi multipli di $x - 2$ sono 25. L'intersezione delle classi multiple di $x - 1$ e di $x - 2$ sono le classi dei polinomi multipli di $(x - 1)(x - 2)$, cioè le classi del tipo $c(x - 1)(x - 2)$ con $c \in \mathbb{F}_5$ e sono quindi 5. Per il Principio di Inclusione Esclusione, i divisori di zero sono $25 + 25 - 5 = 45$.

Gli elementi nilpotenti sono esattamente le classi multiple di tutti i fattori primi di $f(x)$, ossia le classi dei polinomi multipli di $(x - 1)(x - 2)$, che abbiamo visto essere 5. Pertanto la risposta al problema è $45 - 5 = 40$.

210. (i) Sia α la radice quarta positiva di a. In $\mathbb{C}[x]$ il polinomio $f(x) = x^4 - a$ si fattorizza come $f(x) = (x - \alpha)(x + \alpha)(x - i\alpha)(x + i\alpha)$. Sappiamo che $f(x)$ è riducibile in $\mathbb{Z}[x]$; abbiamo quindi due possibilità: $f(x)$ ha una radice in $\mathbb{Z}$ oppure $f(x)$ si spezza come prodotto di due polinomi di secondo grado in $\mathbb{Z}[x]$.

Nel primo caso, visto che $\pm i\alpha$ non sono reali, le possibili radici sono solo $\pm\alpha$; e di fatto, se una delle due è intera, lo è anche l'altra. Ma se $\alpha = k \in \mathbb{N}$ allora $a = \alpha^4 = k^4$ e dunque si ottiene $a = b^2$ con $b = k^2 \in \mathbb{N}$.

Nel secondo caso, i due fattori di secondo grado devono essere necessariamente $x^2 - \alpha^2$ e $x^2 + \alpha^2$, perché il polinomio di secondo grado che ha una radice non reale

deve avere necessariamente come radice anche il numero complesso coniugato. Ne segue che $\alpha^2 = b \in \mathbb{N}$, e di nuovo $a = \alpha^4 = b^2$.

(ii) Sia α la radice quarta positiva di $-a$. La fattorizzazione di $f(x)$ in $\mathbb{C}[x]$ è $f(x) = (x - \zeta\alpha)(x - \overline{\zeta}\alpha)(x - \zeta^3\alpha)(x - \overline{\zeta}^3\alpha)$, dove $\zeta = (1+i)/\sqrt{2}$ è una radice ottava primitiva di 1. In questo caso non ci sono radici reali, e l'unica fattorizzazione a coefficienti interi può venire dal raccogliere insieme i fattori complessi coniugati $(x - \zeta\alpha)(x - \overline{\zeta}\alpha) = x^2 - \sqrt{2}\alpha x + \alpha^2$ e $(x - \zeta^3\alpha)(x - \overline{\zeta}^3\alpha) = x^2 + \sqrt{2}\alpha x + \alpha^2$. Poiché anche in questo caso $\alpha^2 = c$ deve essere un numero naturale, si deve avere $-a = \alpha^4 = c^2$. Inoltre la condizione che $\sqrt{2}\alpha$ sia un numero intero ci dice che $\alpha = d'/\sqrt{2}$ con $d' \in \mathbb{N}$. Elevando al quadrato si ha $c = d'^2/2$, da cui d' è pari, diciamo $d' = 2d$ con $d \in \mathbb{N}$, e $c = 2d^2$.

211. Osserviamo innanzitutto che il polinomio $f(x) = x^4 + 5x^2 + 5$ è irriducibile in $\mathbb{Q}[x]$, per il Lemma di Gauss e il Criterio di Eisenstein con primo 5. Per la stessa ragione, il polinomio $g(y) = y^2 + 5y + 5$ è irriducibile; le sue radici sono $\alpha_1, \alpha_2 = (-5 \pm \sqrt{5})/2$, ed il suo campo di spezzamento è $\mathbb{F} = \mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\sqrt{5})$ di grado 2 su $\mathbb{Q}$.

Il campo di spezzamento di $f(x)$ è allora $\mathbb{K} = \mathbb{F}(\sqrt{\alpha_1}, \sqrt{\alpha_2})$. Osserviamo anche che $\alpha_1\alpha_2$, essendo il prodotto delle due radici di $g(x)$, è uguale a 5, che evidentemente è un quadrato in $\mathbb{F}$. Quindi le due estensioni $\mathbb{F}(\sqrt{\alpha_1})/\mathbb{F}$ e $\mathbb{F}(\sqrt{\alpha_2})/\mathbb{F}$ coincidono e il grado del campo di spezzamento è minore o uguale a 4.

D'altra parte, poiché il polinomio $f(x)$ è irriducibile in $\mathbb{Q}[x]$, il grado del campo di spezzamento è multiplo di 4, cioè il grado che si otterrebbe aggiungendo una sola radice di $f(x)$. Pertanto $[\mathbb{K} : \mathbb{Q}] = 4$.

Su $\mathbb{F}_{11}$ il polinomio $f(x)$ si può riscrivere come $x^4 - 6x^2 + 5 = (x^2 - 1)(x^2 - 5) = (x + 1)(x - 1)(x^2 - 5)$. Notando che $5 \equiv 4^2 \pmod{11}$, si vede che $x^2 - 5 = (x + 4)(x - 4)$, così $f(x) = (x + 1)(x - 1)(x + 4)(x - 4)$ e dunque il grado del campo di spezzamento è uguale a 1.

212. (i) Poiché α è una radice di $f(x) = x^3 - x^2 - 2x - 1$ abbiamo $\alpha^3 = \alpha^2 + 2\alpha + 1$. Moltiplicando per α otteniamo

$$\begin{aligned}\beta &= \alpha^4 - 3\alpha^2 \\ &= \alpha^3 + 2\alpha^2 + \alpha - 3\alpha^2 \\ &= \alpha^3 - \alpha^2 + \alpha \\ &= \alpha^2 + 2\alpha + 1 - \alpha^2 + \alpha \\ &= 3\alpha + 1.\end{aligned}$$

Osserviamo ora che il polinomio $f(x)$ non ha radici razionali visto che 1 e -1 non sono radici. Allora esso è irriducibile in $\mathbb{Q}[x]$ essendo di terzo grado. Ne segue che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.

Ora ovviamente $\beta \in \mathbb{Q}(\alpha)$ e $\alpha = (\beta - 1)/3 \in \mathbb{Q}(\beta)$. Quindi $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$ e pertanto anche il grado del polinomio minimo di β su $\mathbb{Q}$ è 3.

Ponendo ora $x = (y-1)/3$ nel polinomio $f(x)$ si ha che

$$\left(\frac{y-1}{3}\right)^3 - \left(\frac{y-1}{3}\right)^2 - \frac{y-1}{3} - 1 = \frac{1}{27}y^3 - \frac{2}{9}y^2 - \frac{1}{3}y - \frac{13}{27}$$

si annulla in β, da cui troviamo che $y^3 - 6y^2 - 9y - 13$ è il polinomio minimo di β su $\mathbb{Q}$.

(ii) Dal polinomio minimo di β si ha $\beta^3 - 6\beta^2 - 9\beta = 13$. Dividendo per 13 si ottiene

$$\beta\,\frac{\beta^2 - 6\beta - 9}{13} = 1$$

e sostituendo poi $\beta = 3\alpha + 1$ si ha

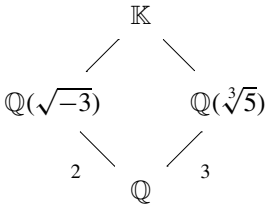
$$\frac{\beta^2 - 6\beta - 9}{13} = \frac{9\alpha^2 - 12\alpha - 14}{13}.$$

Ne segue che $g(x) = (9x^2 - 12x - 14)/13$ risponde ai requisiti del problema.

⟦La seconda parte si può anche risolvere nel seguente modo. Ogni elemento di $\mathbb{Q}(\alpha)$ si può scrivere come $u_2\alpha^2 + u_1\alpha + u_0$ con $u_0, u_1, u_2 \in \mathbb{Q}$. Allora per trovare $g(x)$ con $\beta g(\alpha) = 1$ basta svolgere i calcoli in $h = (3\alpha + 1)(u_2\alpha^2 + u_1\alpha + u_0) - 1$ e risolvere il sistema lineare in u_0, u_1, u_2 che risulta dall'equazione $h = 0$.⟧

213. Le radici di x^2+3 sono $\pm\sqrt{-3}$ mentre le radici di x^3-5 sono $\sqrt[3]{5}$, $\sqrt[3]{5}\zeta$, $\sqrt[3]{5}\zeta^2$ con $\zeta = (-1+\sqrt{-3})/2$. Il campo di spezzamento è quindi $\mathbb{K} \doteq \mathbb{Q}(\sqrt{-3}, \sqrt[3]{5}, \zeta)$.

Osserviamo che $\mathbb{K} = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{5})$; infatti, è chiaro che $\mathbb{Q}(\sqrt{-3}, \sqrt[3]{5}) \subseteq \mathbb{K}$ e, inoltre, $\zeta = (-1+\sqrt{-3})/2 \in \mathbb{Q}(\sqrt{-3})$ e quindi abbiamo anche $\sqrt[3]{5}\zeta, \sqrt[3]{5}\zeta^2 \in \mathbb{Q}(\sqrt{-3}, \sqrt[3]{5})$.



Il campo $\mathbb{K}$ contiene le due sottoestensioni $\mathbb{Q}(\sqrt{-3})$ e $\mathbb{Q}(\sqrt[3]{5})$, che hanno grado su $\mathbb{Q}$ rispettivamente 2 e 3 in quanto i polinomi minimi dei loro generatori sono rispettivamente x^2+3 e x^3-5, polinomi entrambi irriducibili su $\mathbb{Q}$ perché non hanno radici e hanno grado minore o uguale a 3. Da questo si ottiene che $2 \mid [\mathbb{K}:\mathbb{Q}]$ e $3 \mid [\mathbb{K}:\mathbb{Q}]$ e quindi $6 \mid [\mathbb{K}:\mathbb{Q}]$. D'altra parte $[\mathbb{K}:\mathbb{Q}] = [\mathbb{K}:\mathbb{Q}(\sqrt[3]{5})][\mathbb{Q}(\sqrt[3]{5}):\mathbb{Q}] \le 2\cdot 3 = 6$ e quindi $[\mathbb{K}:\mathbb{Q}] = 6$.

214. (i) Per $p = 3$ si ha $x^{15} - 1 = (x^5 - 1)^3$ e quindi, spezzare $f(x)$ è equivalente a spezzare $x^5 - 1$. Essendo 5 primo con 3, il campo di spezzamento di $x^5 - 1$ è $\mathbb{F}_{3^d}$ dove d è l'ordine moltiplicativo di 3 modulo 5. Quindi $d = 4$ e $(x-1)^5(x^4 + x^3 + x^2 + x + 1)^5$ è la fattorizzazione di $f(x)$ in irriducibili.

Per $p = 5$ procediamo in modo analogo: $f(x) = (x^3 - 1)^5$ e il campo di spezzamento è $\mathbb{F}_{5^2}$ visto che 5 ha ordine 2 in $\mathbb{F}_3^*$. La fattorizzazione è ora $f(x) = (x-1)^5(x^2 + x + 1)^5$.

(ii) Se p non è 3 né 5 allora 15 è primo con p e possiamo applicare lo stesso ragionamento del punto precedente per trovare il campo di spezzamento di $f(x)$.

Esso sarà $\mathbb{F}_{p^d}$ con d ordine moltiplicativo di p modulo 15. Poiché $(\mathbb{Z}/15\mathbb{Z})^* \simeq (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ l'ordine di p in questo gruppo è un divisore di 4.

(iii) Per $p = 31$ si ha $d = 1$ in quanto $31 \equiv 1 \pmod{15}$, per $p = 11$ si ha $d = 2$ in quanto $11^2 = 121 \equiv 1 \pmod{15}$ e, infine, per $p = 2$ si ha $d = 4$ visto che 2 ha ordine moltiplicativo 4 modulo 15.

215. Consideriamo il caso in cui il campo base sia $\mathbb{F}_7$. Per verifica diretta si vede che il polinomio $x^2 + 2$ non ha radici e quindi è irriducibile; inoltre $x^4 - 2 = (x^2 - 3)(x^2 + 3)$. Quindi, indipendentemente dalla riducibilità o irriducibilità di $x^2 - 3$ e $x^2 + 3$, il minimo comune multiplo dei gradi dei fattori irriducibili di $(x^2 + 2)(x^4 - 2)$ è 2. Il campo di spezzamento su $\mathbb{F}_7$ ha pertanto grado 2.

Le radici in $\mathbb{C}$ del polinomio $(x^2 + 2)(x^4 - 2)$ sono $\pm i\sqrt{2}$, $\pm\sqrt[4]{2}$ e $\pm i\sqrt[4]{2}$, quindi il campo di spezzamento di tale polinomio su $\mathbb{Q}$ è $\mathbb{K} = \mathbb{Q}(i\sqrt{2}, \sqrt[4]{2}, i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$.

$$\begin{array}{c} \mathbb{K} = \mathbb{Q}(\sqrt[4]{2}, i) \\ | \\ \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R} \\ 4 \; | \\ \mathbb{Q} \end{array}$$

Per calcolarne il grado, consideriamo la torre di estensioni $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})(i) = \mathbb{K}$. La prima estensione ha grado 4 perché il polinomio minimo di $\sqrt[4]{2}$ su $\mathbb{Q}$ è $x^4 - 2$, infatti questo polinomio è irriducibile su $\mathbb{Z}$ per il Criterio di Eisenstein con primo 2 e quindi, per il Lemma di Gauss, esso è irriducibile anche su $\mathbb{Q}$. La seconda ha grado 2 perché $x^2 - 1$ si annulla in i e l'estensione non è banale visto che $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$ mentre $i \notin \mathbb{R}$. Si ha quindi $[\mathbb{K} : \mathbb{Q}] = 8$.

216. (i)

$$\begin{array}{c} \mathbb{F} = \mathbb{Q}(\sqrt{5}, \sqrt{-5}) \\ | \\ \mathbb{Q}(\sqrt{5}) \subseteq \mathbb{R} \\ 2 \; | \\ \mathbb{Q} \end{array}$$

Sia $\mathbb{F} = \mathbb{Q}(\sqrt{5}, \sqrt{-5}) = \mathbb{Q}(\alpha, \beta)$. Consideriamo le estensioni $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{5}) \subseteq \mathbb{F}$. La prima ha grado 2 su $\mathbb{Q}$ ed è reale, la seconda ha grado al più 2 visto che si ottiene aggiungendo $\sqrt{-5}$ a $\mathbb{Q}(\sqrt{5})$ e $\sqrt{-5}$ ha grado 2 su $\mathbb{Q}$ e, quindi, grado al più 2 su $\mathbb{Q}(\sqrt{5})$. Ma il grado della seconda estensione non può essere uno in quanto allora si avrebbe $\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\sqrt{5}, \sqrt{-5})$, ma ciò è impossibile perché il secondo campo non è reale.

Abbiamo quindi provato che $\mathbb{F}$ ha grado 4 su $\mathbb{Q}$. Chiaramente $\alpha + \beta \in \mathbb{F}$. Vogliamo provare che in realtà $\mathbb{Q}(\alpha + \beta) = \mathbb{F}$, facendo così vedere che il grado del polinomio minimo di $\alpha + \beta$ su $\mathbb{Q}$ è 4.

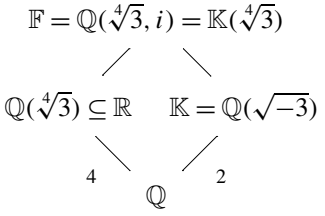
Osserviamo che $i = (\alpha + \beta)^2/10 \in \mathbb{Q}(\alpha + \beta)$ e quindi anche $-\alpha + \beta = i(\alpha + \beta)$ appartiene a $\mathbb{Q}(\alpha + \beta)$. È allora chiaro che $\alpha, \beta \in \mathbb{Q}(\alpha + \beta)$, cioè $\mathbb{Q}(\alpha + \beta) = \mathbb{Q}(\alpha, \beta) = \mathbb{F}$.

(ii) Il grado di $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ è al più 2, come quello di $\mathbb{F}_p(\beta)/\mathbb{F}_p$, quindi sia $\mathbb{F}_p(\alpha)$ che $\mathbb{F}_p(\beta)$ sono contenute in $\mathbb{F}_{p^2}$ in quanto esiste un'unica estensione di grado 2 di $\mathbb{F}_p$ in una fissata chiusura algebrica. Quindi $\alpha + \beta \in \mathbb{F}_{p^2}$ e il polinomio minimo di $\alpha + \beta$ ha grado al più 2 su $\mathbb{F}_p$.

Ad esempio se $p = 5$ allora $\alpha = \beta = 0$ e $\alpha + \beta$ ha grado ovviamente 1 su $\mathbb{F}_5$. Se invece $p = 3$ allora $\alpha = \pm\sqrt{2} \in \mathbb{F}_{3^2} \setminus \mathbb{F}_3$, mentre $\beta = \pm 1$, e quindi $\alpha + \beta \in \mathbb{F}_{3^2} \setminus \mathbb{F}_3$, cioè $\alpha + \beta$ ha grado 2 su $\mathbb{F}_3$.

(iii) Visto che 2011 è congruo a 3 modulo 4, abbiamo che -1 non è un quadrato in $\mathbb{F}_{2011}$. Allora uno e uno solo tra 5 e -5 è un quadrato in $\mathbb{F}_{2011}$, quindi delle due estensioni $\mathbb{F}_{2011}(\alpha)$ e $\mathbb{F}_{2011}(\beta)$ una ha grado 1 e l'altra ha grado 2. In ogni caso il grado cercato è 2.

217. Il polinomio $f(x)$ è irriducibile su $\mathbb{Q}$ per il criterio di Eisenstein, quindi è il polinomio minimo di ognuna delle sue radici. Ne segue che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Le radici del polinomio $f(x)$ in una chiusura algebrica di $\mathbb{Q}$ sono $\pm\sqrt[4]{3}, \pm i\sqrt[4]{3}$, quindi il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ è $\mathbb{F} = \mathbb{Q}(\sqrt[4]{3}, i\sqrt[4]{3}) = \mathbb{Q}(\sqrt[4]{3}, i)$.



Usando la moltiplicatività dei gradi nelle torri di estensioni si calcola $[\mathbb{F} : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{3})(i) : \mathbb{Q}(\sqrt[4]{3})][\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 2 \cdot 4 = 8$, infatti il grado di $\mathbb{Q}(\sqrt[4]{3})/\mathbb{Q}$ è stato già calcolato, e l'altro vale 2 in quanto è minore o uguale a 2, perché i annulla il polinomio $x^2 + 1 \in \mathbb{Q}(\sqrt[4]{3})[x]$, ed è maggiore di 1 visto che $i \notin \mathbb{Q}(\sqrt[4]{3}) \subseteq \mathbb{R}$.

Sia ora $\mathbb{K} = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(i\sqrt{3})$. Poiché $i\sqrt{3}$ non è reale abbiamo che $[\mathbb{Q}(\sqrt[4]{3}, i\sqrt{3}) : \mathbb{Q}] = 8$, quindi $[\mathbb{K}(\sqrt[4]{3}) : \mathbb{K}] = [\mathbb{Q}(\sqrt[4]{3}, i\sqrt{3}) : \mathbb{Q}]/[\mathbb{K} : \mathbb{Q}] = 8/2 = 4$. Da questo segue che il polinomio $f(x)$ è irriducibile anche su $\mathbb{K}$, quindi ogni sua radice α ha grado 4 su $\mathbb{K}$. Ragionando come nel caso precedente si ha che il campo di spezzamento di $f(x)$ su $\mathbb{K}$ è $\mathbb{K}(\sqrt[4]{3}, i)$. D'altra parte $\mathbb{K}(\sqrt[4]{3}) = \mathbb{K}(\sqrt[4]{3}, i) = \mathbb{Q}(i\sqrt{3}, \sqrt[4]{3}, i) = \mathbb{Q}(\sqrt[4]{3}, i) = \mathbb{F}$ in quanto $i\sqrt{3} = i(\sqrt[4]{3})^2 \in \mathbb{F}$, e il suo grado su $\mathbb{K}$ è $[\mathbb{F} : \mathbb{K}] = [\mathbb{K}(\sqrt[4]{3}) : \mathbb{K}] = 4$.

218. (i) Ricordiamo che il grado del campo di spezzamento di un polinomio su un campo finito $\mathbb{F}_{p^n}$ è $\mathbb{F}_{p^{nd}}$ dove d è il minimo comune multiplo dei gradi dei fattori irriducibili del polinomio su $\mathbb{F}_{p^n}$.

Su $\mathbb{F}_2$ otteniamo facilmente $f(x) = x(x^4 + x + 1)$; inoltre il polinomio $x^4 + x + 1$ è irriducibile in quanto non ha radici e non è il quadrato di $x^2 + x + 1$ che è l'unico polinomio irriducibile di secondo grado di $\mathbb{F}_2[x]$. Il campo di spezzamento di $f(x)$ su $\mathbb{F}_2$ è quindi $\mathbb{F}_{2^4}$.

In $\mathbb{F}_3[x]$ abbiamo $f(x) = (x^2 + 1)(x^3 - x + 1)$ e questi due fattori sono irriducibili visto che non hanno radici. Il campo di spezzamento di $f(x)$ su $\mathbb{F}_3$ è quindi $\mathbb{F}_{3^6}$.

(ii) Occorre vedere se $x^2 + 1$ e $x^3 - x + 1$ si spezzano o meno su $\mathbb{F}_{3^k}$. Le radici del polinomio $x^2 + 1$ generano $\mathbb{F}_{3^2}$ e quindi il polinomio si spezza su $\mathbb{F}_{3^k}$ se e solo se $\mathbb{F}_{3^2} \subseteq \mathbb{F}_{3^k}$ cioè se e solo se $2 \mid k$. Analogamente $x^3 - x + 1$ si spezza in $\mathbb{F}_{3^k}$ se e solo se $3 \mid k$.

In conclusione, se $k \equiv 0 \pmod 6$, in $\mathbb{F}_{3^k}$ il polinomio $f(x)$ si spezza in fattori lineari. Se, invece, $k \equiv 2, 4 \pmod 6$, $f(x)$ ha due radici e un fattore irriducibile di terzo grado. Se $k \equiv 3 \pmod 6$ allora $f(x)$ ha tre radici e un fattore di secondo

grado. Infine se $k \equiv 1, 5 \pmod 6$ il polinomio $f(x)$ ha un fattore di grado 2 e uno di grado 3, come su $\mathbb{F}_3$.

219. Riducendo il polinomio $f(x) = x^4 + 2x^3 + 2x^2 + x + 3$ modulo 2 otteniamo $x^4 + x^2 + 1$; tale polinomio è irriducibile visto che non ha radici in $\mathbb{F}_2$ e non è il quadrato di $x^2 + x + 1$, l'unico polinomio irriducibile di secondo grado in $\mathbb{F}_2[x]$. Allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$ e, quindi, per il Lemma di Gauss, anche in $\mathbb{Q}[x]$.

Da ciò otteniamo che $f(x)$ è il polinomio minimo di α su $\mathbb{Q}$ e quindi $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Essendo $\mathbb{Q}(\alpha + 1) = \mathbb{Q}(\alpha)$ anche il polinomio minimo di $\alpha + 1$ su $\mathbb{Q}$ ha grado 4. Chiaramente il polinomio $f(x - 1) = x^4 - 2x^3 + 2x^2 - x + 3$ si annulla in $\alpha + 1$, quindi esso deve essere un multiplo del polinomio minimo di $\alpha + 1$, ma poiché è monico ed ha grado 4 è proprio il polinomio minimo.

Cerchiamo ora il polinomio minimo di $\alpha^2 + \alpha$ su $\mathbb{Q}$. Dato che $\mathbb{Q}(\alpha^2 + \alpha) \subseteq \mathbb{Q}(\alpha)$ il grado di $\alpha^2 + \alpha$ su $\mathbb{Q}$ è un divisore di 4. Possiamo escludere che sia 1 in quanto altrimenti $\alpha^2 + \alpha = q \in \mathbb{Q}$ e quindi $x^2 + x - q$ sarebbe un polinomio di grado 2 di $\mathbb{Q}[x]$ che si annulla in α, ma questo non è possibile perché abbiamo visto che il grado di α su $\mathbb{Q}$ è 4. Il grado cercato sarà quindi 2 o 4, e sarà 2 se e solo se $(\alpha^2 + \alpha)^2$, $\alpha^2 + \alpha$, 1 sono linearmente dipendenti su $\mathbb{Q}$. Dobbiamo quindi decidere se esistano o meno soluzioni in $a, b \in \mathbb{Q}$ di

$$(\alpha^2 + \alpha)^2 + a(\alpha^2 + \alpha) + b = 0.$$

Svolgendo i calcoli si ottiene $\alpha^4 + 2\alpha^3 + (a + 1)\alpha^2 + a\alpha + b = 0$, e ricavando α^4 dalla relazione $f(\alpha) = 0$ si ha

$$(a - 1)\alpha^2 + (a - 1)\alpha + b - 3 = 0$$

che ha soluzione $a = 1, b = 3$. Questo prova che il polinomio $h(x) = x^2 + x + 3$ si annulla in $\alpha^2 + \alpha$ e, avendo grado minimo possibile, ne è il polinomio minimo.

220. (i) Dimostriamo che il polinomio $f(x)$ è irriducibile in $\mathbb{Q}[x]$. Innanzitutto non ha radici razionali; basta, infatti, controllare che $f(1)$ e $f(-1)$ siano diversi da zero. Poi, per il Lemma di Gauss, è sufficiente provare che $f(x)$ non si fattorizzi in $\mathbb{Z}[x]$. Ora, se $f(x)$ si potesse scrivere come prodotto di due polinomi di secondo grado, che possiamo supporre monici, avremmo $f(x) = (x^2 + ax + b)(x^2 + cx + d)$ per opportuni $a, b, c, d \in \mathbb{Z}$. Uguagliando il termine di terzo grado si ha $a + c = 0$, mentre per il termine noto si ha $bd = 1$, da cui $c = -a$ e $d = b = \pm 1$. Quindi

$$f(x) = (x^2 + ax + b)(x^2 - ax + b) = (x^2 + b)^2 - (ax)^2 = x^4 + (2b - a^2)x^2 + 1.$$

Infine, uguagliando il termine di secondo grado si dovrebbe avere $2b - a^2 = 3$, ossia $2b - 3 = a^2$. Ma, se $b \in \{1, -1\}$ allora $2b - 3 \in \{-1, -5\}$ e quindi tale numero non è il quadrato di un intero. Perciò $f(x)$ è irriducibile, ed essendo anche monico è il polinomio minimo di α su $\mathbb{Q}$. Ne segue che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

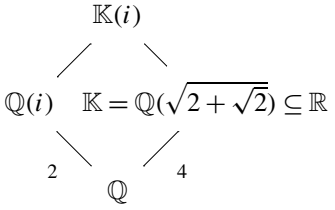
(ii) Siano β_1, β_2 le radici del polinomio di secondo grado $y^2 + 3y + 1$. Allora $\mathbb{E} = \mathbb{Q}(\beta_1) = \mathbb{Q}(\beta_2)$ ha grado 2 su $\mathbb{Q}$, infatti abbiamo già controllato che questo polinomio non ha radici razionali. Detto $\mathbb{K}$ il campo di spezzamento di $f(x)$ si

ha $\mathbb{K} = \mathbb{E}(\sqrt{\beta_1}, \sqrt{\beta_2})$. Però i due campi $\mathbb{E}(\sqrt{\beta_1})$ ed $\mathbb{E}(\sqrt{\beta_2})$ coincidono, perché $\beta_1\beta_2 = 1$ è un quadrato in $\mathbb{E}$. Pertanto $\mathbb{K} = \mathbb{E}(\sqrt{\beta_1})$. Senza perdita di generalità, possiamo supporre che $\mathbb{K} = \mathbb{Q}(\alpha)$ e quindi otteniamo $[\mathbb{K} : \mathbb{Q}] = 4$.

(iii) Il polinomio $f(x-1) = (x-1)^4 + 3(x-1)^2 + 1 = x^4 - 4x^3 + 9x^2 - 10x + 5$ si annulla in $\alpha + 1$. Il suo polinomio reciproco, ossia $g(x) = 5x^4 - 10x^3 + 9x^2 - 4x + 1$, si annulla in $1/(\alpha + 1)$. Inoltre, è chiaro che $\mathbb{Q}(\alpha) = \mathbb{Q}(1/(\alpha + 1))$, quindi il polinomio minimo di $1/(\alpha + 1)$ su $\mathbb{Q}$ ha grado 4. Ne segue che tale polinomio è uguale a $g(x)/5$.

221. Il polinomio $f(x) = x^4 - 4x^2 + 2$ è irriducibile in $\mathbb{Q}[x]$ per il Lemma di Gauss e per il Criterio di Eisenstein rispetto al primo 2, quindi ogni sua radice ha grado 4 su $\mathbb{Q}$.

Le soluzioni complesse dell'equazione $y^2 - 4y + 2 = 0$ sono $2 \pm \sqrt{2}$, quindi le radici complesse di $f(x)$ sono $\pm\alpha, \pm\beta$ dove $\alpha^2 = 2 + \sqrt{2}$ e $\beta^2 = 2 - \sqrt{2}$. È chiaro che sia $\mathbb{Q}(\alpha)$ che $\mathbb{Q}(\beta)$ sono estensioni di grado 2 su $\mathbb{Q}(\sqrt{2})$. Inoltre esse sono la stessa estensione se e solo se $(2 + \sqrt{2})(2 - \sqrt{2}) = 2$ è un quadrato in $\mathbb{Q}(\sqrt{2})$, cosa banalmente vera. Quindi, poiché il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ è $\mathbb{K} = \mathbb{Q}(\pm\alpha, \pm\beta)$, si ha $[\mathbb{K} : \mathbb{Q}] = 4$.

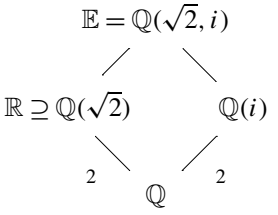


Osserviamo che le radici di $f(x)$ sono tutte reali, in quanto radici quadrate di elementi reali positivi, quindi $i \notin \mathbb{K}$. Ne segue che $[\mathbb{K}(i) : \mathbb{K}] = 2$ e, per la formula del prodotto dei gradi $[\mathbb{K}(i) : \mathbb{Q}] = 8$. D'altra parte, $\mathbb{K}(i) = \mathbb{Q}(i, \alpha, \beta)$ è il campo di spezzamento di $f(x)$ su $\mathbb{Q}(i)$. Sempre per la formula dei gradi, si ha inoltre $[\mathbb{K}(i) : \mathbb{Q}(i)] = [\mathbb{K}(i) : \mathbb{Q}]/[\mathbb{Q}(i) : \mathbb{Q}] = 8/2 = 4$.

In $\mathbb{F}_7$ vale $(\pm 3)^2 = 2$, quindi le radici di $y^2 - 4y + 2 = 0$ sono $2 \pm 3 = -1, 5$. Ne segue che $y^2 - 4y + 2 = (y + 1)(y - 5)$ e $x^4 - 4x^2 + 2 = (x^2 + 1)(x^2 - 5)$. Per verifica diretta, cioè controllando che non ci siano radici, si trova che sia $x^2 + 1$ che $x^2 - 5$ sono irriducibili in $\mathbb{F}_7[x]$, e quindi il grado del campo di spezzamento di $f(x)$ su $\mathbb{F}_7$ è 2.

222. (i) Proviamo che $\mathbb{EF} \subseteq \mathbb{K}$. Ogni radice di $x^8 - 1$ e di $x^3 - 1$ è anche una radice di $x^{24} - 1$, quindi i generatori di $\mathbb{E}$ e di $\mathbb{F}$ sono contenuti in $\mathbb{K}$.

Siano $\zeta_8 = e^{2\pi i/8}$ e $\zeta_3 = e^{2\pi i/3}$, rispettivamente, radici ottave e terze primitive dell'unità in $\mathbb{C}$. Allora $\zeta_8 \cdot \zeta_3$ è una radice 24–esima primitiva dell'unità, quindi vale anche $\mathbb{K} \subseteq \mathbb{EF}$.



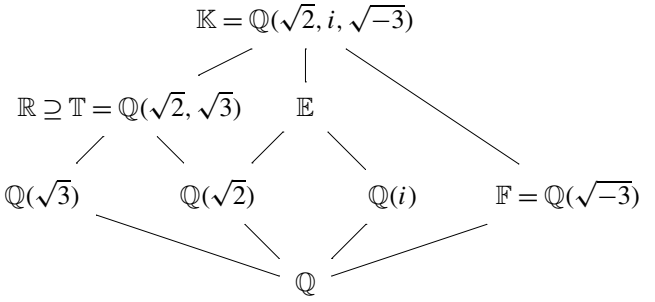
Le radici ottave di 1 sono $\pm 1, \pm i, (\pm 1 \pm i)/\sqrt{2}$, quindi $\mathbb{E}$ è contenuto in $\mathbb{Q}(\sqrt{2}, i)$. D'altra parte, $\mathbb{E}$ deve contenere la radice i ed anche $\sqrt{2} = (1 + i)\sqrt{2}/(1 + i)$, quindi $\mathbb{E}$ è uguale a $\mathbb{Q}(\sqrt{2}, i)$. Notiamo che $\mathbb{Q}(\sqrt{2})$ e $Q(i)$ sono due estensioni distinte di $\mathbb{Q}$ di grado 2, infatti una è reale e l'altra no, abbiamo allora $[\mathbb{E} : \mathbb{Q}] = 4$.

Le radici terze di 1 sono $(-1 \pm \sqrt{-3})/2$, quindi $\mathbb{F} = \mathbb{Q}(\sqrt{-3})$ ed $[\mathbb{F} : \mathbb{Q}] = 2$. Ne segue che $\mathbb{K} = \mathbb{Q}(\sqrt{2}, i, \sqrt{-3})$.

Osservando poi che sia $\sqrt{2}$ che $\sqrt{3} = i \cdot \sqrt{-3} \in \mathbb{K}$, si ha che $\mathbb{K} = \mathbb{T}(i)$, dove $\mathbb{T} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ è un campo contenuto nei numeri reali. Poiché $2 \cdot 3 = 6$ non è un quadrato in $\mathbb{Q}$, si ha $[\mathbb{T} : \mathbb{Q}] = 4$, mentre $\mathbb{K}$ è un'estensione di grado 2 di $\mathbb{T}$, quindi $[\mathbb{K} : \mathbb{Q}] = 8$.

Infine $\mathbb{T} \subseteq \mathbb{K} \cap \mathbb{R} \subseteq \mathbb{K}$ e, dato che $[\mathbb{T} : \mathbb{Q}] = 4$ e $[\mathbb{K} : \mathbb{Q}] = 8$, abbiamo $\mathbb{K} \cap \mathbb{R} = \mathbb{T}$ oppure $\mathbb{K} \cap \mathbb{R} = \mathbb{K}$. Siccome $\mathbb{K} \cap \mathbb{R} \subseteq \mathbb{R}$ mentre $\mathbb{K} \not\subseteq \mathbb{R}$, si ha necessariamente $\mathbb{K} \cap \mathbb{R} = \mathbb{T}$.

Una base di $\mathbb{K} \cap \mathbb{R}$ si può trovare facendo i prodotti degli elementi di due basi di $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{3})$, ad esempio $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$.



223. (i) Il polinomio $x^2 + x + 1$ ha come radici ζ, ζ^2, dove $\zeta \in \mathbb{C}$ è una radice terza primitiva di 1. Per avere la divisibilità dei polinomi, bisogna che queste siano anche radici di $f(x) = x^{2n} + x^n + 1$. In realtà, basta verificare che solo una sia radice, in quanto esse sono complesse coniugate; se una è radice lo è anche l'altra. Calcoliamo il valore del polinomio $f(x)$ in ζ. Abbiamo

$$f(\zeta) = \begin{cases} 1 + 1 + 1 = 3 & \text{se } n \equiv 0 \pmod 3; \\ \zeta^2 + \zeta + 1 = 0 & \text{se } n \equiv 1 \pmod 3; \\ \zeta + \zeta^2 + 1 = 0 & \text{se } n \equiv 2 \pmod 3. \end{cases}$$

Quindi i valori cercati sono tutti e soli i numeri naturali $n \not\equiv 0 \pmod 3$.

(ii) Dall'uguaglianza

$$\frac{x^{12} - 1}{x^4 - 1} = x^8 + x^4 + 1$$

segue che il campo di spezzamento del polinomio, sia su $\mathbb{Q}$ che su $\mathbb{F}_7$ è generato da una radice 12–esima primitiva dell'unità. Infatti le radici del polinomio $x^{12} - 1$ sono un gruppo ciclico di ordine 12, e quelle del denominatore sono un gruppo ciclico, sottogruppo del precedente, di ordine 4. D'altra parte, aggiungendo al campo di base una qualsiasi radice primitiva 12–esima dell'unità, vengono aggiunte automaticamente tutte le altre, in quanto potenze della prima.

Per quanto riguarda $\mathbb{Q}$, calcolando le radici del polinomio

$$\frac{\pm 1 \pm \sqrt{3}i}{2}, \frac{\pm\sqrt{3} \pm i}{2}$$

troviamo che il campo di spezzamento è uguale a $\mathbb{Q}(\sqrt{3}, i)$. Infatti il campo di spezzamento è sicuramente contenuto in $\mathbb{Q}(\sqrt{3}, i)$ vista l'espressione esplicita delle radici. Inoltre il contenimento opposto si ottiene dal fatto che sommando le due radici coniugate $(\sqrt{3} \pm i)/2$ si ottiene $\sqrt{3}$ e quindi anche i per differenza.

Per quanto riguarda $\mathbb{F}_7$ il grado del campo di spezzamento è il più piccolo intero k per il quale $\mathbb{F}_{7^k}$ contiene le radici 12–esime di 1; altrimenti detto, il più piccolo intero positivo k per il quale $12 \mid 7^k - 1$, ossia $k = 2$.

224. Dimostriamo innanzitutto che $f(x) = x^4 - x^3 + x^2 - x + 1$ è irriducibile in $\mathbb{Q}[x]$. Per verifica diretta, $f(x)$ non ha radici razionali: basta infatti controllare che ± 1 non siano radici. Inoltre, per il Lemma di Gauss, è sufficiente verificare che $f(x)$ non si fattorizzi in $\mathbb{Z}[x]$. Supponiamo quindi, per assurdo, che

$$f(x) = (x^2 + ax + b)(x^2 + cx + d)$$

sia il prodotto di due polinomi di secondo grado. Svolgendo il prodotto, si ottiene

$$\begin{cases} a + c = -1 \\ b + d + ac = 1 \\ ad + bc = -1 \\ bd = 1. \end{cases}$$

L'ultima equazione dice che $b = d = \pm 1$. Sostituendo nella terza equazione, si vede che l'unica possibilità è $b = d = 1$, perché altrimenti si contraddice la prima equazione. D'altra parte le soluzioni delle prime due equazioni $a + c = -1$ e $ac = -1$ sono soluzioni di $t^2 + t - 1 = 0$ ma, evidentemente, tale polinomio in t non ha radici intere.

⟦È possibile provare che $f(x)$ è irriducibile in $\mathbb{Z}[x]$ anche riducendo i coefficienti modulo 2. Si ottiene così il polinomio $x^4 + x^3 + x^2 + x + 1$ che non ha chiaramente radici; inoltre, esso non è il quadrato di $x^2 + x + 1$, l'unico polinomio irriducibile di grado 2 in $\mathbb{F}_2[x]$.⟧

Il grado $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ è dunque 4, e il grado $d = [\mathbb{Q}(\alpha + c\alpha^{-1}) : \mathbb{Q}]$ è un divisore di 4 visto che $\alpha + c\alpha^{-1} \in \mathbb{Q}(\alpha)$. Notiamo subito che $d \neq 1$, in quanto se fosse $d = 1$ avremmo che $\alpha + c\alpha^{-1} = q \in \mathbb{Q}$, ossia $\alpha^2 - q\alpha + c = 0$ e quindi α soddisferebbe un'equazione di grado 2 a coefficienti razionali, cosa impossibile in quanto $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Quindi $d = 2$ o $d = 4$.

Affinché $d = 2$, è necessario e sufficiente che $(\alpha + c\alpha^{-1})^2$, $\alpha + c\alpha^{-1}$, 1 siano linearmente dipendenti su $\mathbb{Q}$. Moltiplicando per α^2, la condizione diventa che $(\alpha^2 + c)^2, \alpha^3 + c\alpha, \alpha^2$ siano linearmente dipendenti su $\mathbb{Q}$.

Scriviamo tutti i termini come combinazione lineare dei vettori della base 1, α, α^2, α^3. I vettori $\alpha^3 + c\alpha, \alpha^2$ sono già scritti in questa base, mentre $(\alpha^2 + c)^2 = \alpha^4 + 2c\alpha^2 + c^2 = \alpha^3 + (2c - 1)\alpha^2 + \alpha + (c^2 - 1)$. Confrontando i coefficienti di α^3, si vede che una combinazione lineare $r(\alpha^3 + (2c - 1)\alpha^2 + \alpha + (c^2 - 1)) +$

$s(\alpha^3 + c\alpha) + t\alpha^2 = 0$ si può ottenere solo se $r = -s$. Se $r = -s = 0$ otteniamo che anche $t = 0$, quindi la combinazione lineare è banale. Se $r = -s \neq 0$, il confronto dei coefficienti di α dà $c = 1$ e inoltre $t = -r$, che è effettivamente una soluzione.

Concludendo, $d = 2$ se $c = 1$ e $d = 4$ se $c \neq 1$.

225. (i) Visto che $f(x)$ ha grado 3, esso è irriducibile in $\mathbb{Q}[x]$ se e sono se non ha radici razionali; inoltre, le uniche possibili radici sono ± 1. Poiché né 1 né -1 sono radici, $f(x)$ è irriducibile in $\mathbb{Q}[x]$. Sia α una radice reale di $f(x)$, abbiamo dunque $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Un polinomio irriducibile di grado 3 ha un campo di spezzamento $\mathbb{K}$ su $\mathbb{Q}$ di grado un divisore di $3! = 6$. Ma abbiamo scelto $\alpha \in \mathbb{R}$ e, visto che la derivata $f'(x) = 3x^2 + 3$ è sempre positiva, c'è una sola radice reale di $f(x)$, abbiamo che $\mathbb{K}$ è più grande di $\mathbb{R}$, ossia $[\mathbb{K} : \mathbb{Q}] = 6$.

(ii) Per il Criterio della Derivata, un polinomio $f(x) \in \mathbb{F}_p[x]$ ha radici multiple in $\mathbb{F}_p$ se e solo se $(f(x), f'(x)) \neq 1$. Se $p = 3$, $f(x) = x^3 + 1 = (x + 1)^3$ ha 1 come radice tripla. Se $p \neq 3$, poiché $f'(x) = 3x^2 + 3 = 3(x^2 + 1)$ e 3 è invertibile modulo p, possiamo fare il massimo comune divisore fra $f(x)$ e $x^2 + 1$. Eseguendo la prima divisione otteniamo $x^3 + 3x + 1 = x(x^2 + 1) + (2x + 1)$.

Ora osserviamo che per $p = 2$ il polinomio $f(x)$ è irriducibile, in quanto è di grado 3 e non ha radici. Possiamo quindi supporre $p \neq 2$ e, per semplicità, moltiplicare $x^2 + 1$ per la costante invertibile 4, ottenendo la divisione euclidea $4x^2 + 4 = (2x - 1)(2x + 1) + 5$. Ne segue che il massimo comune divisore fra $f(x)$ e $f'(x)$ è diverso da 1 se e solo se $p = 3$ o $p = 5$. Per $p = 5$ si ha, in effetti, $f(x) = (x - 1)(x - 2)^2$.

Concludiamo, quindi, che $f(x)$ ha una radice multipla in $\mathbb{F}_p$ se e solo se $p = 3$ o $p = 5$.

226. (i) Il polinomio si fattorizza in $\mathbb{Z}[x]$ come $f(x) = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1)$, dobbiamo quindi mostrare che $h(x) = x^6 + x^3 + 1$ è irriducibile su $\mathbb{F}_{11}$.

Per il Teorema sulle Estensioni Ciclotomiche, il grado del campo di spezzamento di $f(x)$ su $\mathbb{F}_{11}$ è $\mathbb{F}_{11^d}$ dove d è l'ordine moltiplicativo di 11 modulo 9; si calcola che $d = 6$. Ne segue che, detto C l'insieme delle radici di $f(x)$ in una fissata chiusura algebrica di $\mathbb{F}_{11}$, si ha $\mathbb{F}_{11}(C) = \mathbb{F}_{11^6}$. Sappiamo inoltre che C è un gruppo moltiplicativo finito, e quindi è ciclico; sia $C = \langle \alpha \rangle$, allora $\mathbb{F}_{11^6} = \mathbb{F}_{11}(\alpha)$. Da questo segue che il polinomio minimo di α, che è un divisore di $f(x)$, ha grado 6 e quindi è proprio $h(x)$ che è per questo irriducibile.

(ii) Usando quanto dimostrato nel punto precedente, $x^2 + x + 1$ non ha radici in $\mathbb{F}_{11}$ e quindi la fattorizzazione $f(x) = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1)$ è in irriducibili anche in $\mathbb{Z}[x]$ perché i fattori sono irriducibili modulo 11. Inoltre, per il Lemma di Gauss questi fattori sono irriducibili anche in $\mathbb{Q}[x]$. Sia $\eta \in \mathbb{C}$ una radice nona primitiva di 1, le radici di $f(x)$ sono quindi $1, \eta, \eta^2, \ldots, \eta^8$. Il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ è quindi $\mathbb{Q}(\eta)$ e il suo grado è il grado del polinomio minimo $\mu(x)$ di η su $\mathbb{Q}$. Sappiamo che $\mu(x) \mid f(x)$, inoltre $\eta^3 \neq 1$, quindi $\mu(x) \mid f(x)/(x^3 - 1) = x^6 + x^3 + 1$. Essendo quest'ultimo polinomio irriducibile si ha $\mu(x) = x^6 + x^3 + 1$ e quindi il grado del campo di spezzamento di $f(x)$ su $\mathbb{Q}$ è 6.

Sia $\mathbb{K} = \mathbb{Q}(\zeta)$, allora il campo di spezzamento di $f(x)$ su $\mathbb{K}$ è $\mathbb{K}(\eta) = \mathbb{Q}(\eta)$. Visto che il polinomio minimo di ζ su $\mathbb{Q}$ è $x^2 + x + 1$ si ha $[\mathbb{K} : \mathbb{Q}] = 2$ e quindi $[\mathbb{Q}(\eta) : \mathbb{K}] = 3$.

227. (i) Mostriamo che il polinomio $f(x)$ è irriducibile modulo 2. Per prima cosa, infatti, è banale verificare che 0 e 1 non sono radici modulo 2, quindi il polinomio non ha fattori di primo grado. Se non fosse irriducibile dovrebbe essere prodotto di due polinomi irriducibili di grado 2. Ma l'unico polinomio irriducibile di grado 2 di $\mathbb{F}_2[x]$ è $x^2 + x + 1$ e si ha $(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq f(x)$, quindi $f(x)$ è irriducibile.

Allora, essendo irriducibile modulo 2, il polinomio $f(x)$ è irriducibile in $\mathbb{Z}[x]$ e quindi, per il Lemma di Gauss, anche in $\mathbb{Q}[x]$. Da ciò ricaviamo che $f(x)$ è il polinomio minimo di α, quindi $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$; poiché $\mathbb{Q}(1/(\alpha + 1)) = \mathbb{Q}(\alpha)$ anche il polinomio minimo di $1/(\alpha + 1)$ avrà grado 4. Il polinomio minimo di $\alpha + 1$ è $f(x - 1) = (x - 1)^4 + (x - 1) + 1 = x^4 - 4x^3 + 6x^2 - 3x + 1$, e quindi il polinomio minimo di $1/(\alpha + 1)$ è il suo reciproco $x^4 - 3x^3 + 6x^2 - 4x + 1$.

Osserviamo che $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^2)$ infatti, chiaramente $\mathbb{Q}(\alpha^2) \subseteq \mathbb{Q}(\alpha)$, inoltre dall'equazione $f(\alpha) = 0$ si ricava $\alpha = -\alpha^4 - 1 \in \mathbb{Q}(\alpha^2)$ che dà l'altro contenimento.

Abbiamo quindi che il polinomio minimo di α^2 su $\mathbb{Q}$ ha grado 4. Possiamo ora procedere in vari modi per calcolare questo polinomio minimo. Osservando, ad esempio, che $\alpha^4 + 1 = -\alpha$ da cui, elevando al quadrato ambo i membri, si ottiene $\alpha^8 + 2\alpha^4 + 1 = \alpha^2$, quindi il polinomio $x^4 + 2x^2 - x + 1$ si annulla in α^2 e ne è il polinomio minimo perché di grado minimo.

⟦Calcoliamo il polinomio minimo di α^2 anche in un altro modo. Sappiamo che è del tipo $\mu(x) = x^4 + ax^3 + bx^2 + cx + d$, dobbiamo ricavare $a, b, c, d \in \mathbb{Q}$ in modo tale che $\mu(\alpha^2) = \alpha^8 + a\alpha^6 + b\alpha^4 + c\alpha^2 + d = 0$. Usando la relazione data dal polinomio minimo di α si calcola che $\alpha^4 = -\alpha - 1$, $\alpha^6 = -\alpha^3 - \alpha^2$ e $\alpha^8 = \alpha^2 + 2\alpha + 1$. Quindi si ha $\mu(\alpha^2) = -a\alpha^3 + (1 - a + c)\alpha^2 + (2 - b)\alpha + 1 - b + d = 0$. Poiché $1, \alpha, \alpha^2, \alpha^3$ sono linearmente indipendenti l'equazione è verificata se e solo se $a = 0, b = 2, c = -1$ e $d = 1$.⟧

(ii) Il campo di spezzamento di $f(x)$ su $\mathbb{F}_5$ è $\mathbb{F}_{5^d}$ dove d è il minimo comune multiplo dei gradi dei fattori irriducibili di $f(x)$ in $\mathbb{F}_5[x]$. Valutando il polinomio in $0, \pm 1, \pm 2$, troviamo che l'unica radice è -2. Per il Teorema di Ruffini $x + 2 \mid f(x)$ e si calcola subito $f(x) = (x + 2)(x^3 + 3x^2 - x + 3)$. Le possibili radici del fattore di terzo grado sono da ricercarsi tra quelle di $f(x)$, quindi l'unica possibile radice è ancora -2; ma si ha $(-2)^3 + 3(-2)^2 - (-2) + 3 \neq 0$ e quindi $x^3 + 3x^2 - x + 3$ non ha radici. Ma un polinomio di grado 3 che non ha radici è irriducibile, quindi $f(x) = (x + 2)(x^3 + 3x^2 - x + 3)$ è la fattorizzazione di $f(x)$. Abbiamo quindi che il campo di spezzamento di $f(x)$ su $\mathbb{F}_5$ è $\mathbb{F}_{5^3}$.

228. (i) Sia α una radice di $f(x)$ in una chiusura algebrica di $\mathbb{F}_p$, allora $\alpha^4 = \pm a \in \mathbb{F}_p^*$, quindi $\mathrm{ord}(\alpha) \mid 4(p - 1) \mid p^2 - 1$, dove l'ultima relazione segue dall'ipotesi $p \equiv 3 \pmod 4$. Allora ogni radice α di $f(x)$ appartiene a $\mathbb{F}_{p^2}$. Resta quindi da mostrare che $f(x)$ non ha tutte le radici in $\mathbb{F}_p$. Infatti, $x^4 - a$ ha una radice in $\mathbb{F}_p$ se e solo se $a = b^4$ con $b \in \mathbb{F}_p$ in tal caso però $-a$ non è una quarta potenza in $\mathbb{F}_p$ in quanto non è neppure un quadrato visto che -1 non è un quadrato in $\mathbb{F}_p$ per $p \equiv 3 \pmod 4$.

Un discorso analogo vale cambiando a con $-a$, quindi il campo di spezzamento cercato è $\mathbb{F}_{p^2}$.

(ii) Sia $a = 1$, allora $f(x) = x^8 - 1$ e il suo campo di spezzamento su $\mathbb{F}_p$ è $\mathbb{F}_{p^k}$ dove k è l'ordine di p in $(\mathbb{Z}/8\mathbb{Z})^*$. Ne segue che, per $p \equiv 1 \pmod 8$, ad esempio $p = 17$, si ha $k = 1$ e per $p \equiv 5 \pmod 8$, ad esempio $p = 5$, si ha $k = 2$.

Resta da mostrare che possiamo realizzare un campo di spezzamento di grado 4. Consideriamo $a = 2$ e $p = 5$; si ha $f(x) = (x^4 - 2)(x^4 + 2)$. Poiché né 2 né -2 sono quadrati modulo 5, non sono neanche quarte potenze e quindi $f(x)$ non ha radici in $\mathbb{F}_5$. Rimane da escludere la possibilità che entrambi i polinomi $x^4 - 2$ e $x^4 + 2$ si fattorizzino come prodotto di due polinomi, necessariamente irriducibili, di grado 2. In realtà, nessuno dei due polinomi si fattorizza in questo modo, come si può mostrare con il calcolo diretto.

Supponiamo infatti che $x^4 \pm 2 = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (b + ac + d)x^2 + (ad + bc)x + bd$ con $a, b, c, d \in \mathbb{F}_5$. Uguagliando i coefficienti si ha

$$\begin{cases} a + c = 0 \\ b + ac + d = 0 \\ ad + bc = 0 \\ bd = \pm 2 \end{cases}$$

e, svolgendo i calcoli, si vede che questi sistemi non hanno soluzione in $\mathbb{F}_5$.

⟦Un altro modo per vedere l'irriducibilità di $x^4 - 2$ e di $x^4 + 2$ è osservare che se $\alpha \in \mathbb{F}_{5^k}$ è una radice di $f(x)$, allora $\alpha^4 = \pm 2$, da cui $\operatorname{ord}(\alpha^4) = 4$ e quindi $\operatorname{ord}(\alpha) = 4r$. Dalla formula $\operatorname{ord}(\alpha^4) = \operatorname{ord}(\alpha)/(4, \operatorname{ord}(\alpha))$ si ottiene $r = 4$, cioè $\operatorname{ord}(\alpha) = 16$. Ne segue che $16 \mid 5^k - 1$ e quindi $k = 4$.⟧

229. (i) Siano $\Delta = a - 4b^2$, $\alpha = (-a + \sqrt{\Delta})/2$ e $\beta = (-a - \sqrt{\Delta})/2$; si ha $\mathbb{F}_p(\sqrt{\Delta}) \subseteq \mathbb{F}_{p^2}$ e quindi $f(x) = (x^3 - \alpha)(x^3 - \beta)$ in $\mathbb{F}_{p^2}[x]$. Ora osserviamo che ogni binomio del tipo $x^3 - \gamma$ di $\mathbb{F}_{p^2}[x]$ è irriducibile o è prodotto di tre fattori di grado 1. Infatti, se $p = 3$ si ha $x^3 - \gamma = (x - \gamma^3)^3$; se invece $p > 3$ si ha $3 \mid p^2 - 1$ e quindi l'omomorfismo $\mathbb{F}_{p^2}^* \ni z \longmapsto z^3 \in \mathbb{F}_{p^2}^*$, è un'applicazione 3 a 1, cioè elementi che sono cubi hanno 3 radici cubiche distinte in $\mathbb{F}_{p^2}$. Possiamo quindi concludere che il grado del campo di spezzamento di $f(x)$ su $\mathbb{F}_{p^2}$ è 1 se sia α che β sono cubi, altrimenti è 3.

(ii) Sia $\mathbb{F}_{p^k}$ il campo di spezzamento di $f(x)$ su $\mathbb{F}_p$. Da quanto dimostrato al punto precedente segue che il campo di spezzamento di $f(x)$ su $\mathbb{F}_{p^2}$, e quindi anche quello su $\mathbb{F}_p$, è contenuto in $\mathbb{F}_{p^6}$. La relazione $\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^6}$ implica $k \mid 6$. In particolare $k \neq 4, 5$.

(iii) Come prima sia $\mathbb{F}_{p^k}$ il campo di spezzamento di $f(x)$ su $\mathbb{F}_p$. Nel primo punto abbiamo visto che $\mathbb{F}_p(\sqrt{\Delta}) \subseteq \mathbb{F}_{p^k}$, quindi se fosse $k = 3$ si avrebbe $\sqrt{\Delta} \in \mathbb{F}_p$, e $f(x) = (x^3 - \alpha)(x^3 - \beta)$ in $\mathbb{F}_p[x]$. Per $p \equiv 2 \pmod 3$, l'applicazione $z \longmapsto z^3$ è un isomorfismo di $\mathbb{F}_p^*$, quindi sia $x^3 - \alpha$ che $x^3 - \beta$ sono prodotto di un fattore lineare e di uno irriducibile di grado 2, quindi in questo caso il campo di spezzamento non può avere grado 3.

230. Ricordiamo che, per il Teorema sulle Estensioni Ciclotomiche, se $(n, p) = 1$ il grado del campo di spezzamento su $\mathbb{F}_p$ del polinomio $x^n - 1$ coincide con l'ordine moltiplicativo di p modulo n. Ne segue che se $p \neq 2, 3, 5$ il grado cercato è il minimo comune multiplo tra l'ordine moltiplicativo di p modulo 15 e l'ordine moltiplicativo di p modulo 12, o, equivalentemente, la minima soluzione positiva del seguente sistema

$$\begin{cases} p^x \equiv 1 \pmod{15} \\ p^x \equiv 1 \pmod{12}. \end{cases}$$

Usando il Teorema Cinese dei Resti il sistema diventa

$$\begin{cases} p^x \equiv 1 \pmod{3} \\ p^x \equiv 1 \pmod{4} \\ p^x \equiv 1 \pmod{5}. \end{cases}$$

È immediato verificare che $x = 4$ risolve il sistema quindi la minima soluzione positiva sarà un divisore di 4. Vediamo, nel seguito, che tutti i divisori di 4 sono gradi possibili.

Per $p = 7$ applicando quanto sopra, si verifica subito che il grado del campo di spezzamento è 4.

Il grado del campo di spezzamento su $\mathbb{F}_p$ è 2 se $p \equiv -1 \pmod{5}$, infatti $p^2 \equiv 1 \pmod{3}$ e $p^2 \equiv 1 \pmod{4}$ per ogni primo maggiore di 3, e possiamo ad esempio scegliere $p = 19$.

Il grado del campo di spezzamento sarà invece 1 se e solo se $3 \mid p - 1$, $4 \mid p - 1$ e $5 \mid p - 1$ cioè se e solo se $60 \mid p - 1$. Poiché, ad esempio, 61 è primo, il campo di spezzamento di $f(x)$ sul campo $\mathbb{F}_{61}$ ha grado 1.

Resta da considerare il caso $p = 2$. In $\mathbb{F}_2[x]$ si ha $f(x) = (x^{15} - 1)(x^3 - 1)^4$ e, poiché $3 \mid 15$ allora $x^3 - 1 \mid x^{15} - 1$, quindi il grado del campo di spezzamento di $f(x)$ coincide con l'ordine di 2 in $(\mathbb{Z}/15\mathbb{Z})^*$, che si vede facilmente essere 4.

⟦Per completare la casistica rimangono da considerare i primi 3 e 5. Per $p = 3$ si ha $f(x) = (x^5 - 1)^3(x^4 - 1)^3$ e, visto che l'ordine moltiplicativo di 3 modulo 5 è 4 e modulo 4 è 2, il grado del campo di spezzamento è 4. Infine, per $p = 5$ si ha $f(x) = (x^3 - 1)^5(x^{12} - 1)$ e con lo stesso ragionamento si ottiene che il grado del campo di spezzamento è 2.⟧

231. La decomposizione in fattori primi di 1635 è $3 \cdot 5 \cdot 109$, quindi $\mathbb{Z}/1635\mathbb{Z}$ non è un campo e l'equazione può avere più di quattro soluzioni. Dal Teorema Cinese dei Resti $\mathbb{Z}/1635\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/109\mathbb{Z}$.

Cerchiamo una decomposizione di $f(x) = 2x^4 - 41x^3 + 201x^2 - 71x - 91$ in $\mathbb{Z}[x]$. Avendo questa, avremo tre decomposizioni in $\mathbb{Z}/3\mathbb{Z}[x]$, $\mathbb{Z}/5\mathbb{Z}[x]$, $\mathbb{Z}/109\mathbb{Z}[x]$ per passaggio al quoziente.

Dato che $91 = 13 \cdot 7$, le possibili radici razionali di f sono a/b con a un divisore di 91 e b un divisore di 2. Controllando si ha che $f(1) = f(7) = f(13) = 0$ e quindi $(x - 1)(x - 7)(x - 13)$ divide $f(x)$; eseguendo la divisione abbiamo $f(x) = (x - 1)(x - 7)(x - 13)(2x + 1)$ in $\mathbb{Z}[x]$, e quindi anche $-1/2$ è una radice. Da questa fattorizzazione ricaviamo: $f(x) = -(x - 1)^4$ in $\mathbb{Z}/3\mathbb{Z}[x]$, $f(x) = (x - 1)(x - 2)^2(x - 3)$ in $\mathbb{Z}/5\mathbb{Z}[5]$ e $(x - 1)(x - 7)(x - 13)(2x + 1)$ in $\mathbb{Z}/109\mathbb{Z}[x]$.

Dato che $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ e $\mathbb{Z}/109\mathbb{Z}$ sono campi, dalle fattorizzazioni abbiamo immediatamente le radici che sono, rispettivamente: $x = 1$, di molteplicità 4, in $\mathbb{Z}/3\mathbb{Z}[x]$; $x = 1, -2, 2$, con 2 di molteplicità 2, in $\mathbb{Z}/5\mathbb{Z}[x]$ e, infine, $x = -1/2, 1, 7, 13$, in $\mathbb{Z}/109\mathbb{Z}[x]$. È, inoltre, facile verificare che le radici sono distinte in $\mathbb{Z}/109\mathbb{Z}[x]$. Abbiamo quindi $1 \cdot 3 \cdot 4 = 12$ soluzioni distinte in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/109\mathbb{Z}$ e, quindi, anche in $\mathbb{Z}/1635\mathbb{Z}$.

Dato che la decomposizione in $\mathbb{Z}[x]$ rimane valida anche nell'anello quoziente $\mathbb{Z}/1635\mathbb{Z}[x]$, tre radici di $f(x)$ sono immediate: $x \equiv 1, 7, 13 \pmod{1635}$. Osserviamo poi che $(2, 1635) = 1$, e quindi in $\mathbb{Z}/1635\mathbb{Z}$ l'elemento 2 è invertibile e abbiamo la soluzione $x = -1/2 \equiv 817 \in \mathbb{Z}/1635\mathbb{Z}$, ovviamente distinta dalle precedenti.

Rimangono da costruire altre due soluzioni, che troviamo usando il Teorema Cinese dei Resti, ad esempio dalle triple di soluzioni $(1, 1, 7)$ e $(1, 2, 13)$ in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/109\mathbb{Z}$. Con facili calcoli si trova che 661 e 667 sono le corrispondenti classi modulo 1635 radici di $f(x)$.

⟦ Per completezza, osservando che $-1/2 \equiv 54 \pmod{109}$, la corrispondenza tra le triple di soluzioni in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/109\mathbb{Z}$ e le soluzioni in $\mathbb{Z}/1635\mathbb{Z}$ è

$$\begin{array}{llll} (1,1,1) & \longleftrightarrow 1 & (1,1,7) & \longleftrightarrow 661 \\ (1,1,13) & \longleftrightarrow 1321 & (1,1,54) & \longleftrightarrow 1471 \\ (1,2,1) & \longleftrightarrow 982 & (1,2,7) & \longleftrightarrow 7 \\ (1,2,13) & \longleftrightarrow 667 & (1,2,54) & \longleftrightarrow 817 \\ (1,3,1) & \longleftrightarrow 328 & (1,3,7) & \longleftrightarrow 988 \\ (1,3,13) & \longleftrightarrow 13 & (1,3,54) & \longleftrightarrow 163. \end{array}$$ ⟧

232. (i) Dimostriamo innanzitutto che $f(x)$ è irriducibile in $\mathbb{Q}[x]$. Poiché $\deg(f) = 3$, è sufficiente far vedere che $f(x)$ non ha radici razionali. Le possibili radici razionali devono avere numeratore divisore del termine noto, cioè -1, e denominatore divisore del coefficiente direttore, cioè 1; si tratta quindi solo di controllare che ± 1 non siano radici. Ora $f(1) = f(-1) = -1$, quindi non esistono radici razionali e il polinomio è irriducibile.

È allora chiaro che il campo $\mathbb{Q}(\alpha)$ ha grado 3 sui razionali e, quindi, ogni suo elemento si può scrivere come combinazione lineare a coefficienti razionali della base 1, α e α^2. Scriviamo $1/(\alpha + 2) = a\alpha^2 + b\alpha + c$, con a, b, c numeri razionali da determinare. Otteniamo

$$\begin{aligned} 1 &= (a\alpha^2 + b\alpha + c)(\alpha + 2) = a\alpha^3 + b\alpha^2 + c\alpha + 2a\alpha^2 + 2b\alpha + 2c \\ &= (b + 2a)\alpha^2 + (a + c + 2b)\alpha + (a + 2c) \end{aligned}$$

dove, nell'ultima uguaglianza, abbiamo usato $\alpha^3 = \alpha + 1$. Uguagliando i coefficienti nella base dei vettori a sinistra e a destra dell'uguaglianza, otteniamo il sistema

$$\begin{cases} b + 2a = 0 \\ a + c + 2b = 0 \\ a + 2c = 1 \end{cases}$$

da cui $a = 1/7$, $b = -2/7$, $c = 3/7$ e, in conclusione, $1/(\alpha + 2) = (\alpha^2 - 2\alpha + 3)/7$.

⟦In alternativa, si può dividere il polinomio $x^3 - x - 1$ per $x + 2$, ottenendo $x^3 - x - 1 = (x^2 - 2x + 3)(x + 2) - 7$. Sostituendo α al posto di x, si ha $(\alpha^2 - 2\alpha + 3)(\alpha + 2) - 7 = 0$, da cui, dividendo per $7(\alpha + 2)$, l'espressione cercata.⟧

(ii) Abbiamo le inclusioni ovvie $\mathbb{Q}(\alpha^2) \subseteq \mathbb{Q}(\alpha)$ e $\mathbb{Q}(\alpha^3) \subseteq \mathbb{Q}(\alpha)$, per cui i gradi cercati sono minori o uguali a 3. Usando, inoltre, la formula del prodotto dei gradi, essi sono divisori di 3, quindi uguali a 1 o a 3.

Se fosse $[\mathbb{Q}(\alpha^2) : \mathbb{Q}] = 1$, avremmo che $\alpha^2 = c \in \mathbb{Q}$, quindi α sarebbe radice del polinomio $x^2 - c \in \mathbb{Q}[x]$ di grado 2, contraddicendo il fatto che il polinomio minimo di α è $x^3 - x - 1$ ed ha grado 3. Pertanto $[\mathbb{Q}(\alpha^2) : \mathbb{Q}] = 3$.

Dall'equazione $\alpha^3 = \alpha + 1$ abbiamo che $\alpha = \alpha^3 - 1 \in \mathbb{Q}(\alpha^3)$, pertanto $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^3)$ e $[\mathbb{Q}(\alpha^3) : \mathbb{Q}] = 3$.

233. (i) Riducendo modulo 2 il polinomio $f(x)$ otteniamo $x^4 + x + 1$ che non ha evidentemente radici e non è il quadrato dell'unico polinomio irriducibile di secondo grado in $\mathbb{F}_2[x]$, cioè $x^2 + x + 1$. Allora il polinomio è irriducibile modulo 2 e quindi è irriducibile in $\mathbb{Z}[x]$. Ma allora è irriducibile anche in $\mathbb{Q}[x]$ per il Lemma di Gauss.

(ii) Dal punto precedente abbiamo che $f(x)$ è il polinomio minimo di α su $\mathbb{Q}$, e quindi $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. È ovvio che $2\alpha - 3 \in \mathbb{Q}(\alpha)$; d'altra parte, $\alpha = (2\alpha - 3)/2 + 3/2 \in \mathbb{Q}(2\alpha - 3)$ da cui $\mathbb{Q}(2\alpha - 3) = \mathbb{Q}(\alpha)$ e $[\mathbb{Q}(2\alpha - 3) : \mathbb{Q}] = 4$. Il polinomio minimo di $2\alpha - 3$ su $\mathbb{Q}$ ha, quindi, grado 4, ed è l'unico polinomio monico di grado 4 in $\mathbb{Q}[x]$ che si annulla su $2\alpha - 3$. Il polinomio

$$g(x) = f\left(\frac{x+3}{2}\right) = \frac{1}{16}(x^4 + 12x^3 + 54x^2 + 84x - 71)$$

ha grado 4 e, chiaramente, si annulla in $2\alpha - 3$. Il polinomio minimo di $2\alpha - 3$ su $\mathbb{Q}$ è allora $16g(x) = x^4 + 12x^3 + 54x^2 + 84x - 71$.

(iii) Ovviamente $\alpha^2 \in \mathbb{Q}(\alpha)$. D'altra parte, dall'equazione $\alpha^4 - 3\alpha - 5 = 0$ troviamo $\alpha = (\alpha^4 - 5)/3 = ((\alpha^2)^2 - 5)/3 \in \mathbb{Q}(\alpha^2)$.

Quindi, anche per α^2, si ha $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\alpha)$, $[\mathbb{Q}(\alpha^2) : \mathbb{Q}] = 4$, e il polinomio minimo di α^2 è caratterizzato dalle proprietà di essere monico, di grado 4 e di annullarsi in α^2. Elevando al quadrato $\alpha^4 - 5 = 3\alpha$ otteniamo subito che $x^4 - 10x^2 - 9x + 25$ si annulla in α^2, esso è quindi il polinomio minimo cercato per quanto appena osservato.

234. Risulta $5 = 2x^2 + 17 - 2(x^2 + 6)$ e quindi si ha $5 \in I = (2x^2 + 17, x^2 + 6)$, anzi $I = (5, x^2 + 1)$.

L'applicazione $\mathbb{F}_5 \ni \overline{a} \longmapsto \overline{a} + I \in A = \mathbb{Z}[x]/I$ è ben definita visto che l'ideale generato da 5 in $\mathbb{Z}[x]$ è contenuto in I, ed è, inoltre, un omomorfismo di anelli. Per provare che essa è anche iniettiva osserviamo che $I \cap \mathbb{Z}$ è un ideale di $\mathbb{Z}$ che contiene $5\mathbb{Z}$, esso può quindi essere uguale a $5\mathbb{Z}$ o a $\mathbb{Z}$. Ma se fosse $I \cap \mathbb{Z} = \mathbb{Z}$ si avrebbe $1 \in I$, cioè $\overline{1} \in (x^2 + 1)$ in $\mathbb{F}_5[x]$, che è invece impossibile. Allora da $\overline{a} + I = \overline{a}' + I$ troviamo $a - a' \in I \cap \mathbb{Z} = 5\mathbb{Z}$ e quindi $\overline{a} = \overline{a}'$.

Avendo provato che $\mathbb{F}_5 \subseteq A$, concludiamo che A è uno spazio vettoriale su $\mathbb{F}_5$. Dimostriamo ora che $1, x$ sono una base di A come spazio vettoriale su $\mathbb{F}_5$. È chiaro che essi sono dei generatori visto che ogni classe di A ha un rappresentante del

tipo $\overline{a}x + \overline{b}$ con $a, b \in \mathbb{Z}$. Per dimostrare la lineare indipendenza assumiamo che $\overline{a}x + \overline{b} = 0$ in $A = \mathbb{Z}[x]/(5, x^2 + 1)$. Allora $ax + b \in (5, x^2 + 1)$ in $\mathbb{Z}[x]$, e quindi $\overline{a}x + \overline{b} \in (x^2 + 1)$ in $\mathbb{F}_5[x]$ da cui $\overline{a} = \overline{b} = 0$ in $\mathbb{F}_5$.

Avendo una base con due elementi A è isomorfo ad $\mathbb{F}_5^2$ come ogni spazio vettoriale di dimensione 2 su tale campo.

235. (i)

$$\begin{array}{c} \mathbb{Q}(\sqrt[3]{2}, i) \\ | \\ \mathbb{Q}(\sqrt[3]{2}) \\ {\scriptstyle 3}\ | \\ \mathbb{Q} \end{array}$$

Per la formula dei gradi abbiamo che $[\mathbb{K} : \mathbb{Q}] = [\mathbb{K} : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$. Ora $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$; infatti il polinomio a coefficienti razionali $x^3 - 2$ è irriducibile per il Criterio di Eisenstein ed ammette $\sqrt[3]{2}$ come radice, ed è quindi il polinomio minimo di $\sqrt[3]{2}$ su $\mathbb{Q}$. Per determinare $[\mathbb{K} : \mathbb{Q}(\sqrt[3]{2})]$, calcoliamo il polinomio minimo di i su $\mathbb{Q}(\sqrt[3]{2})$. Dato che conosciamo la fattorizzazione del polinomio $x^2 + 1$ su $\mathbb{C}[x]$ possiamo vedere immediatamente che questo polinomio è irriducibile in $\mathbb{R}[x]$ e quindi in $\mathbb{Q}(\sqrt[3]{2})[x] \subseteq \mathbb{R}[x]$.

Visto che i annulla il polinomio irriducibile $x^2 + 1 \in \mathbb{Q}(\sqrt[3]{2})[x]$, questo è il suo polinomio minimo su $\mathbb{Q}(\sqrt[3]{2})$. Quindi $[\mathbb{K} : \mathbb{Q}(\sqrt[3]{2})] = 2$.

In conclusione, $[\mathbb{K} : \mathbb{Q}] = 2 \cdot 3 = 6$.

(ii) Proviamo che $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2}, i) = \mathbb{Q}(\sqrt[3]{2} + i)$. Dato che $\sqrt[3]{2} + i \in \mathbb{Q}(\sqrt[3]{2}, i)$ è ovvio che $\mathbb{Q}(\sqrt[3]{2} + i) \subseteq \mathbb{Q}(\sqrt[3]{2}, i)$.

Sia $u = \sqrt[3]{2} + i$. Allora elevando al cubo entrambi i membri di $u - i = \sqrt[3]{2}$ otteniamo

$$i = \frac{u^3 - 3u - 2}{3u^2 - 1} \in \mathbb{Q}(u) = \mathbb{Q}(\sqrt[3]{2} + i).$$

Inoltre $\sqrt[3]{2} = u - i \in \mathbb{Q}(\sqrt[3]{2} + i)$ e quindi $\mathbb{Q}(\sqrt[3]{2}, i) \subseteq \mathbb{Q}(\sqrt[3]{2} + i)$.

(iii) Dobbiamo trovare il polinomio minimo di $\sqrt[3]{2} + i$ su $\mathbb{Q}$. Per quanto dimostrato nei due punti precedenti, abbiamo che il suo grado deve essere 6. Ci basterà quindi trovare un polinomio monico a coefficienti razionali di grado 6 che si annulli su $\sqrt[3]{2} + i$.

Sia come prima $u = \sqrt[3]{2} + i$. Elevando al quadrato l'espressione di i in termini di u, abbiamo subito che $u^6 + 3u^4 - 4u^3 + 3u^2 + 12u + 5 = 0$. Quindi, il polinomio $x^6 + 3x^4 - 4x^3 + 3x^2 + 12x + 5 \in \mathbb{Q}(x)$ è monico, di grado 6 e si annulla in $\sqrt[3]{2} + i$. Esso è il polinomio minimo di $\sqrt[3]{2} + i$ su $\mathbb{Q}$.

236. (i)

$$\begin{array}{c} \mathbb{Q}(\sqrt{3}, \sqrt{5}) \\ | \\ \mathbb{Q}(\sqrt{3}) \\ {\scriptstyle 2}\ | \\ \mathbb{Q} \end{array}$$

Consideriamo le estensioni $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Poiché $x^2 - 3$ e $x^2 - 5$ sono i polinomi minimi di $\sqrt{3}$ e $\sqrt{5}$ su $\mathbb{Q}$, la prima estensione ha grado 2, mentre la seconda ha grado al più 2. Se per assurdo si avesse $\sqrt{5} \in \mathbb{Q}(\sqrt{3})$, allora $\sqrt{5} = a + b\sqrt{3}$ con a e b razionali non nulli; elevando al quadrato, si otterrebbe $5 = a^2 + 2ab\sqrt{3} + 3b^2$, cioè $\sqrt{3} = (5 - a^2 - 3b^2)/2ab \in \mathbb{Q}$, il che è assurdo.

⟦Si può provare che $\sqrt{5} \notin \mathbb{Q}(\sqrt{3})$ anche come segue. Se fosse $\sqrt{5} \in \mathbb{Q}(\sqrt{3})$ allora le due estensioni quadratiche $\mathbb{Q}(\sqrt{3})$ e $\mathbb{Q}(\sqrt{5})$ sarebbe uguali; ma questo è impossibile in quanto $3 \cdot 5 = 15$ non è un quadrato in $\mathbb{Q}$.⟧

Questo ci dice che anche la seconda estensione ha grado 2 e quindi

$$[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 4.$$

Consideriamo adesso le estensioni $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3} - \sqrt{5}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Poiché $\sqrt{3} - \sqrt{5}$ è irrazionale, in quanto il suo quadrato è un numero irrazionale, la prima estensione ha grado almeno 2 e quindi può avere grado 2 oppure 4 perché deve dividere $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 4$.

Supponiamo per assurdo che abbia grado 2, cioè che esista un polinomio $f(x) = x^2 + ax + b \in \mathbb{Q}[x]$ tale che $f(\sqrt{3} - \sqrt{5}) = 0$. Questo significa che $(\sqrt{3} - \sqrt{5})^2 + a(\sqrt{3} - \sqrt{5}) + b = 0$ da cui $3 + 5 - 2\sqrt{15} + a\sqrt{3} - a\sqrt{5} + b = 0$, cioè $8 + b + a\sqrt{3} = (a + 2\sqrt{3})\sqrt{5}$. Elevando entrambi i membri al quadrato si ottiene $64 + b^2 + 3a^2 + 16b + 16a\sqrt{3} + 2ab\sqrt{3} = 5a^2 + 60 + 20a\sqrt{3}$, da cui $b^2 + 16b - 2a^2 + 4 + (2ab - 4a)\sqrt{3} = 0$; poiché $\sqrt{3}$ è irrazionale, si deve avere $2ab - 4a = 0$, cioè $a = 0$ oppure $b = 2$. Nel primo caso si ottiene $b^2 + 16b + 4 = 0$ e nel secondo $a^2 = 20$, ma nessuna delle due equazioni ha soluzioni razionali. Questo implica che un tale polinomio non può esistere e di conseguenza $[\mathbb{Q}(\sqrt{3} - \sqrt{5}) : \mathbb{Q}] = 4$.

(ii) Poniamo $\alpha = \sqrt{3} - \sqrt{5}$. Elevando al quadrato si ottiene $\alpha^2 = 3 + 5 - 2\sqrt{15}$, cioè $\alpha^2 - 8 = -2\sqrt{15}$. Elevando nuovamente al quadrato si ha $\alpha^4 - 16\alpha^2 + 4 = 0$ e di conseguenza $\sqrt{3} - \sqrt{5}$ è radice del polinomio $x^4 - 16x^2 + 4 \in \mathbb{Q}[x]$. Poiché $[\mathbb{Q}(\sqrt{3} - \sqrt{5}) : \mathbb{Q}] = 4$, questo polinomio è irriducibile ed è il polinomio minimo di $\sqrt{3} - \sqrt{5}$ su $\mathbb{Q}$.

Consideriamo ora il secondo elemento. Posto $f(x) = x^8 - 16x^4 + 4 \in \mathbb{Q}[x]$, è facile vedere che $f(\sqrt{\sqrt{3} - \sqrt{5}}) = 0$ e quindi il polinomio $g(x) = f(x + 1) = (x + 1)^8 - 16(x + 1)^4 + 4 \in \mathbb{Q}[x]$ è monico e si annulla in $\sqrt{\sqrt{3} - \sqrt{5}} - 1$. Per dimostrare che $g(x)$ è il polinomio minimo di $\sqrt{\sqrt{3} - \sqrt{5}} - 1$ su $\mathbb{Q}$, resta da far vedere che $g(x)$ è irriducibile o, equivalentemente, che l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{\sqrt{3} - \sqrt{5}} - 1) = \mathbb{Q}(\sqrt{\sqrt{3} - \sqrt{5}})$ ha grado 8.

$$\begin{array}{c} \mathbb{Q}(\beta) \\ | \\ \mathbb{Q}(\sqrt{3} - \sqrt{5}) \subseteq \mathbb{R} \\ 4 \ | \\ \mathbb{Q} \end{array}$$

Poniamo $\beta = \sqrt{\sqrt{3} - \sqrt{5}}$. Poiché sappiamo che $[\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}(\sqrt{3} - \sqrt{5})] \cdot [\mathbb{Q}(\sqrt{3} - \sqrt{5}) : \mathbb{Q}]$ e che $[\mathbb{Q}(\sqrt{3} - \sqrt{5}) : Q] = 4$, abbiamo che $[\mathbb{Q}(\beta) : \mathbb{Q}] = 8$ è equivalente a $\mathbb{Q}(\sqrt{3} - \sqrt{5}) \neq \mathbb{Q}(\beta)$. Questo segue subito dal fatto che $\mathbb{Q}(\sqrt{3} - \sqrt{5})$ è una sottoestensione di $\mathbb{R}$, mentre $\mathbb{Q}(\beta)$ non lo è, in quanto $\beta = \sqrt{\sqrt{3} - \sqrt{5}}$ è la radice quadrata di un numero negativo.

237. Sia $f(x) = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ e osserviamo che $(x - 1) f(x) = x^8 - 1$. È allora chiaro che in $\mathbb{C}[x]$ il polinomio $f(x)$ ha per radici tutte le radici

ottave dell'unità tranne 1, cioè

$$f(x) = \left(x - \frac{1+i}{\sqrt{2}}\right)(x-i)\left(x - \frac{-1+i}{\sqrt{2}}\right)(x+1)$$
$$\cdot \left(x - \frac{-1-i}{\sqrt{2}}\right)(x+i)\left(x - \frac{1-i}{\sqrt{2}}\right).$$

Inoltre una scomposizione in $\mathbb{Z}[x]$, non necessariamente in irriducibili, di $x^8 - 1$ è data da $(x-1)(x+1)(x^2+1)(x^4+1)$ come si trova subito usando ripetutamente la fattorizzazione di una differenza di quadrati. Questa scomposizione continua a valere in $\mathbb{F}_5[x]$ e $\mathbb{F}_{13}[x]$ dato che entrambi questi due anelli sono quozienti di $\mathbb{Z}[x]$.

Osserviamo ora che x^2+1 è irriducibile in $\mathbb{Z}[x]$ in quanto non ha radici reali ed è monico. Poi $(x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$ è irriducibile per il Criterio di Eisenstein con primo 2, e quindi anche x^4+1 è irriducibile. La fattorizzazione in irriducibili in $\mathbb{Z}[x]$ è quindi

$$f(x) = (x+1)(x^2+1)(x^4+1).$$

In $\mathbb{F}_5$ abbiamo $\overline{2}^2 = -\overline{1}$, mentre $\pm\overline{2}$ non sono quadrati. Allora $x^2+1 = (x-2)(x+2)$, $x^4+1 = (x^2-2)(x^2+2)$ e questi ultimi due polinomi sono irriducibili non avendo radici. La fattorizzazione in $\mathbb{F}_5[x]$ è quindi

$$f(x) = (x+1)(x-2)(x+2)(x^2-2)(x^2+2).$$

In $\mathbb{F}_{17}$ si ha $\overline{4}^2 = -\overline{1}$ e quindi $x^2+1 = (x-4)(x+4)$, $x^4+1 = (x^2-4)(x^2+4) = (x-2)(x+2)(x-8)(x+8)$. Il polinomio si spezza quindi completamente

$$f(x) = (x+1)(x-4)(x+4)(x-2)(x+2)(x-8)(x+8).$$

238. (i) Osserviamo che 1 è radice di $f(x)$ su $\mathbb{F}_7$, possiamo quindi dividere per $x-1$; otteniamo $f(x) = (x-1)(x^3 - x^2 - 3x + 3)$. Visto che 1 è radice anche di $x^3 - x^2 - 3x + 3$, dividiamo ancora e abbiamo $f(x) = (x-1)^2(x^2-3)$.

Per studiare la riducibilità di x^2-3 calcoliamo i quadrati degli elementi di $\mathbb{F}_7^*$: $(\pm 1)^2 = 1$, $(\pm 2)^2 = -3$, $(\pm 3)^2 = 2$, quindi 3 non è un quadrato e x^2-3 è irriducibile. La fattorizzazione in irriducibili di $f(x)$ è $(x-1)^2(x^2-3)$.

(ii) Dato che $\mathbb{F}_7[x]/(f(x))$ è un anello finito, gli elementi sono invertibili o divisori di zero; basta quindi contare i divisori di zero. Sappiamo che questi sono rappresentati da polinomi di grado minore di 4 non coprimi con $f(x)$. L'insieme dei divisori di zero è cioè dato dai polinomi di grado minore o uguale a 3 che sono multipli di $x-1$ o di x^2-3. Per contarli usiamo il Principio di Inclusione Esclusione

$$|\{\text{divisori di zero}\}| = |\{\text{multipli di } (x-1)\}| + |\{\text{multipli di } (x^2-3)\}|$$
$$- |\{\text{multipli di } (x-1)(x^2-3)\}|.$$

I multipli di $x-1$ sono rappresentati da polinomi della forma $(a_2x^2+a_1x+a_0)(x-1)$, senza condizioni su $a_0, a_1, a_2 \in \mathbb{F}_7$ e sono $7^3 = 343$. Per la stessa ragione, i multipli di x^2-3 sono $7^2 = 49$ e i multipli di $(x-1)(x^2-3)$ sono 7.

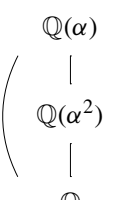
I divisori di zero sono quindi $7^3 + 7^2 - 7 = 385$ e gli invertibili

$$|\mathbb{F}_7[x]/(f(x))| - 385 = 7^4 - 385 = 2016.$$

239. Calcoliamo il polinomio minimo di α su $\mathbb{Q}$. Isolando ripetutamente le radici quadrate abbiamo

$$\begin{aligned}\alpha &= 2+\sqrt{5+\sqrt{-5}}\\ (\alpha-2)^2 &= 5+\sqrt{-5}\\ ((\alpha-2)^2-5)^2 &= -5\\ \alpha^4-8\alpha^3+14\alpha+8\alpha+6 &= 0,\end{aligned}$$

dunque α è radice del polinomio $f(x) = x^4-8x^3+14x^2+8x+6$. Ora $f(x) \in \mathbb{Z}[x]$ ed è irriducibile in $\mathbb{Z}[x]$ per il Criterio di Eisenstein con $p = 2$. Per il Lemma di Gauss $f(x)$ è irriducibile anche in $\mathbb{Q}[x]$ e, essendo monico, esso è il polinomio minimo di α su $\mathbb{Q}$. Ne segue che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 4$.



Consideriamo ora la torre di estensioni $\mathbb{Q} \subseteq \mathbb{Q}(\alpha^2) \subseteq \mathbb{Q}(\alpha)$. Sappiamo che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ e che $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^2)] \leq 2$, in quanto α è radice del polinomio $x^2-\alpha^2$ che ha grado 2 e coefficienti in $\mathbb{Q}(\alpha^2)$.

Dalla moltiplicatività del grado nelle torri di estensioni ricaviamo che $[\mathbb{Q}(\alpha^2) : \mathbb{Q}] = 2$ o 4. Se fosse $[\mathbb{Q}(\alpha^2) : \mathbb{Q}] = 2$ il polinomio minimo di α^2 su $\mathbb{Q}$ sarebbe del tipo x^2+ax+b, con a e b in $\mathbb{Q}$, e quindi α sarebbe radice del polinomio $g(x) = x^4+ax^2+b \in \mathbb{Q}[x]$.

Allora $g(x)$ dovrebbe essere un multiplo di $f(x)$. Ma poiché f e g sono entrambi polinomi monici dello stesso grado, dovrebbero coincidere: questo però non è possibile perché g è un polinomio biquadratico, mentre f non lo è. Concludiamo che $[\mathbb{Q}(\alpha^2) : \mathbb{Q}] = 4$.

240. (i) In $\mathbb{F}_2$ si ha

$$\begin{aligned}f(x) &= x^4+3x^3+x+1\\ &= x^4+x^3+x+1\\ &= (x+1)^2(x^2+x+1)\end{aligned}$$

e questa è una fattorizzazione in quanto il polinomio x^2+x+1 è irriducibile su $\mathbb{F}_2$, perché ha grado 2 e non ha radici.

Analogamente, in $\mathbb{F}_3[x]$ abbiamo $f(x) = (x-1)(x^3+x^2+x-1)$ e x^3+x^2+x-1 è un polinomio irriducibile su $\mathbb{F}_3$, in quanto di grado 3 e privo di radici in $\mathbb{F}_3$.

Segue che il campo di spezzamento di $f(x)$ su $\mathbb{F}_2$ è dato da $\mathbb{F}_{2^2}$ e il campo di spezzamento di $f(x)$ su $\mathbb{F}_3$ è dato da $\mathbb{F}_{3^3}$.

Il campo di spezzamento di $f(x)$ su $\mathbb{F}_{2^k}$ è, per definizione, la minima estensione di $\mathbb{F}_{2^k}$ che contenga le radici di $f(x)$. Ora, contenere le radici di $f(x)$ equivale a contenere l'estensione da loro generata su $\mathbb{F}_2$, quindi si tratta di determinare il grado della minima estensione di $\mathbb{F}_{2^k}$ che contenga $\mathbb{F}_{2^2}$. Da quanto sappiamo sui contenimenti tra estensioni finite si ha che il grado del campo di spezzamento cercato è $2/(k,2)$, cioè 1 se k è pari e 2 se k è dispari.

Analogamente, il campo di spezzamento di $f(x)$ su $\mathbb{F}_{3^k}$ è la minima estensione di $\mathbb{F}_{3^k}$ che contiene $\mathbb{F}_{3^3}$, che quindi ha grado $3/(k,3)$.

(ii) Si ha $[\mathbb{Q}(\alpha):\mathbb{Q}]=4$ in quanto $f(x)$ è un polinomio irriducibile su $\mathbb{Q}$. Infatti $f(x)$ non ha radici in $\mathbb{Q}$, perché gli unici candidati ad essere radici sono ± 1 e si verifica che $f(\pm 1)\neq 0$. Quindi se $f(x)$ fosse riducibile su $\mathbb{Q}$ dovrebbe potersi esprimere come prodotto di due polinomi irriducibili di grado 2. Ciò, tuttavia, è in contraddizione con la fattorizzazione trovata su $\mathbb{F}_3$.

⟦ In alternativa, è possibile osservare che se $f(x)$ si fattorizzasse su $\mathbb{Q}$ come prodotto di due irriducibili di grado 2, dovremmo avere

$$x^4+3x^3+x+1=(x^2+ax\pm 1)(x^2+bx\pm 1)$$

con $a,b\in\mathbb{Z}$. Confrontando i coefficienti dei monomi x e x^3 in ambo i membri risulterebbe $a+b=\pm 1$, e $a+b=3$, condizioni chiaramente incompatibili. ⟧

241. Per prima cosa osserviamo che il polinomio $f(x)$ è irriducibile su $\mathbb{Q}$ per il criterio di Eisenstein con primo 2. Le sue radici complesse sono i numeri $i^k\sqrt[4]{2}$, per $k=0,1,2,3$. Posto $\alpha=\sqrt[4]{2}$ si ha che il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ è dato da $\mathbb{Q}(i,\alpha)$.

$\mathbb{Q}(\alpha,i)$
$|$
$\mathbb{Q}(\alpha)$
$4\ |$
$\mathbb{Q}$

Consideriamo la seguente torre di estensioni $\mathbb{Q}\subseteq\mathbb{Q}(\alpha)\subseteq\mathbb{Q}(\alpha,i)$. La prima estensione ha grado 4 per l'irriducibilità di $f(x)$, e la seconda estensione ha grado 2: infatti, ha grado al più 2 perché il polinomio x^2+1 è un polinomio con coefficienti in $\mathbb{Q}(\alpha)$ che si annulla in i, e non ha grado 1 perché le due estensioni non coincidono in quanto $\mathbb{Q}(\alpha)$ è reale. In particolare, il grado del campo di spezzamento di $f(x)$ su $\mathbb{Q}$ è 8.

Su $\mathbb{F}_3$ vale la seguente identità

$$f(x)=x^2-2=x^4+4=\left(x^4+4x^2+4\right)-(2x)^2=\left(x^2-2x+2\right)\left(x^2+2x+2\right)$$

e i polinomi $x^2\pm 2x+2$ sono irriducibili su $\mathbb{F}_3$ in quanto il loro discriminante, -1, non è un quadrato in $\mathbb{F}_3$. In particolare il grado del campo di spezzamento di $f(x)$ su $\mathbb{F}_3$ è 2.

Su $\mathbb{F}_{17}$ vale

$$f(x)=x^4-2=x^4-36=\left(x^2-6\right)\left(x^2+6\right).$$

Inoltre i polinomi $x^2\pm 6$ sono irriducibili su $\mathbb{F}_{17}$ in quanto 6 e -6 non sono quadrati in $\mathbb{F}_{17}$ come si può verificare elencando esplicitamente i quadrati. In particolare, il grado del campo di spezzamento di $f(x)$ su $\mathbb{F}_{17}$ è 2.

⟦L'identità $a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$, che abbiamo usato sopra per $\mathbb{F}_3$ con $b = 1$, è detta Identità di Sophie Germain in onore della matematica francese.

Si poteva calcolare il grado su $\mathbb{F}_{17}$ anche osservando che, poiché 2 ha ordine 8 in $(\mathbb{Z}/17\mathbb{Z})^*$, ogni radice α nella chiusura algebrica di $\mathbb{F}_{17}$ è tale che $(\alpha^4)^8 = 2^8 = 1$, quindi si ha $\alpha^{32} = 1$ e $\alpha^{16} \neq 1$. Stiamo allora cercando il grado del campo generato dalle radici 32–esime dell'unità su $\mathbb{F}_{17}$: questo campo è $\mathbb{F}_{17^d}$ dove d è l'ordine di 17 in $(\mathbb{Z}/32\mathbb{Z})^*$. Poiché $17 \not\equiv 1 \pmod{32}$ e $17^2 \equiv 1 \pmod{32}$, si ha $d = 2$.⟧

Indice analitico

A
Abeliano
  gruppo, 24
Algebrico(a)
  elemento, 46
  estensione, 46
Algoritmo
  di Euclide, 15
  di Euclide per polinomi, 39
Anello(i), 33
  commutativo, 33
  con unità, 33
  di polinomi, 36
  generato, 35
  isomorfismo di, 35
  nullo, 33
  omomorfismo di, 35
  quoziente, 36
  unitario, 33
  uno di un, 33
  zero di un, 33
Applicazione(i), 3
  biiettiva, 4
  codominio di una, 3
  compatibile con una relazione, 5
  composizione di, 3
  diagramma commutativo di, 4
  dominio di una, 3
  identità, 4
  immagine di una, 3
  inclusione, 4
  iniettiva, 3
  inversa, 4
  invertibile, 4
  legge associativa per, 3
  punti fissi di una, 4
  restrizione di una, 4
  suriettiva, 4
Argomento
  di un numero complesso, 10
Aritmetica
  modulare, 20
  teorema fondamentale della, 16
Automorfismo
  di Frobenius, 45
  di un campo, 45
  di un gruppo, 31

B
Base, 43
Bezout
  identità di, 15
    per polinomi, 39
Binomio
  teorema del
    di Newton, 14, 35
    ingenuo, 18, 45

C
Campo(i), 34, 44
  algebricamente chiuso, 48
  automorfismo di un, 45
  caratteristica di un, 44
  chiusura algebrica di un, 48
  estensione di, 45
  finito, 49
Caratteristica
  di un campo, 44
  positiva, 44
  zero, 44
Cardinalità
  di un insieme, 11

R. Chirivì et al., *Esercizi scelti di Algebra, Volume 1*,
UNITEXT – La Matematica per il 3+2 107, DOI 10.1007/978-88-470-3961-2

Cauchy
teorema di, 32
Centro, 24
Chiuso
sottoinsieme, 8
Chiusura
algebrica di un campo, 48
Ciclico(i)
gruppo, 25
teorema di struttura dei gruppi, 31
Ciclo, 29
lunghezza di un, 29
Ciclotomico(a)
estensione
su $\mathbb{Q}$, 49
polinomio, 42
teorema delle Estensioni, 51
Cinese
teorema
dei resti, 19
Classe(i)
di equivalenza, 5
di resto invertibili, 20
laterali, 26
Codominio, 3
Coefficiente
binomiale, 13
direttore, 37
Combinatoria, 11
Combinazione lineare, 43
Commutativo
anello, 33
diagramma, 4
gruppo, 24
Complementare, 2
Complesso(i)
argomento di un numero, 10
forma algebrica di un numero, 10
forma polare di un numero, 10
modulo di un numero, 10
numeri, 9
numero
immaginario puro, 10
parte immaginaria di un numero, 9
parte reale di un numero, 9
piano, 10
Composizione, 8
di applicazioni, 3
Congruenza, 17
Congruo, 17, 26
Coniugato, 27
numero complesso, 10
Contenuto
di un polinomio, 41
Controimmagine, 3
Costante
polinomio, 37
Criterio
della derivata, 48
di Eisenstein, 42

D

De Morgan
legge di, 2
Derivata
criterio della, 48
di un polinomio, 48
Dimensione, 43
Diofantea
equazione
lineare, 16
Dipendenti
linearmente, 43
Divide esattamente, 17
Divisibilità
tra polinomi, 39
Divisione
euclidea, 15
euclidea tra polinomi, 39
Divisore, 15
dello zero, 34
Dominio, 3
d'integrità, 34

E

Eisenstein
criterio di, 42
Elemento
algebrico, 46
invertibile in un anello, 34
neutro
per un'operazione, 8
neutro di un gruppo, 23
nilpotente, 34
trascendente, 46
Equazione
diofantea lineare, 16
Equivalenza
classe di, 5
relazione di, 5
Estensione(i)
algebrica, 46
ciclotomica, 49
di campi, 45
finita, 46
grado di una, 46
torre di, 46

Euclide
algoritmo di, 15
per polinomi, 39
lemma di, 16
Eulero
formula di, 10
funzione di, 21
teorema di, 21

F
Fattoriale, 12
Fattorizzazione
di polinomi, 40
Fermat
teorema di, 19
Fibonacci
numeri di, 8
Finito
campo, 49
Forma
algebrica di un numero complesso, 10
polare di un numero complesso, 10
Formula
di Eulero, 10
Frobenius
automorfismo di, 45
Funzione
caratteristica, 12
di Eulero, 21
moltiplicativa, 21

G
Gauss
lemma di, 41
Generatore(i)
insieme di, 25
per uno spazio vettoriale, 43
Grado
di un polinomio, 37
di un'estensione, 46
Gruppo(i), 23
automorfismo di, 31
centro di un, 24
ciclico, 25
commutativo o abeliano, 24
delle unità dei quaternioni, 28
elemento neutro di un, 23
immagine omomorfa di un, 30
isomorfismo di, 30
moltiplicativo di un campo, 45
omomorfismo di, 29
ordine di un, 24
prodotto diretto di, 32
quoziente, 27
quoziente di, 26
simmetrico, 29
teorema di struttura dei
ciclici, 31

I
Ideale, 36
generato, 36
massimale, 36
Identità
applicazione, 4
di Bezout, 15
di Bezout per polinomi, 39
Immaginario(a)
puro, 10
unità, 9
Immagine
di un elemento, 3
di un insieme, 3
di un'applicazione, 3
omomorfa di un gruppo, 30
Indeterminata, 37
Indice
di un sottogruppo, 26
Indipendenti
linearmente, 43
Induzione
principio di, 7
Insieme(i), 1
cardinalità di un, 11
chiuso per un'operazione, 8
complementare, 2
controimmagine di un, 3
delle parti, 1
di generatori, 25
di rappresentanti, 6
disgiunti, 2
finito, 11
funzione caratteristica di un, 12
immagine di un, 3
infinito, 11
intersezione di, 2
quoziente, 5
unione di, 1
vuoto, 1
Integrità
dominio di, 34
Intero(i)
congruo, 17
numeri, 9
primi tra loro, 15
primo, 16
Intersezione, 2

Inverso
destro per un'operazione, 8
in un gruppo, 23
per un'operazione, 8
sinistro per un'operazione, 8
Invertibile
classe di resto, 20
elemento
in un anello, 34
Irriducibile
polinomio, 40
Isomorfismo
di anelli, 35
di gruppi, 30

L
Lagrange
teorema di, 27
Laterali
destri di un sottogruppo, 26
sinistri di un sottogruppo, 26
Legendre
simbolo di, 51
Legge(i)
associativa per applicazioni, 3
dell'annullamento del prodotto, 34
di cancellazione, 24
di de Morgan, 2
Leibniz
regola di, 48
Lemma
di Euclide, 16
di Gauss, 41
Linearmente
dipendenti, 43
indipendenti, 43
Lunghezza
di un ciclo, 29

M
Massimale
ideale, 36
Massimo comun divisore, 15
Minimo
polinomio, 47
Minimo comune multiplo, 17
Modulo
di un numero complesso, 10
Molteplicità
di una radice, 39
Moltiplicativa
funzione, 21
Monico
polinomio, 37
Multiplo, 15
di un polinomio, 39

N
Newton
teorema del binomio di, 14, 35
Nilpotente
elemento, 34
Normale
sottogruppo, 27
Nucleo
di un omomorfismo di anelli, 36
di un omomorfismo di gruppi, 30
Numero(i), 9
complessi, 9
complesso coniugato, 10
di Fibonacci, 8
interi, 9
naturali, 7
razionali, 9
reali, 9

O
Omomorfismo
di anelli, 35
di gruppi, 29
nucleo di un
di anelli, 36
di gruppi, 30
teorema di, 30
Operazione, 8
associativa, 8
commutativa, 8
del quoziente di gruppi, 27
distributiva, 9
elemento neutro per una, 8
inverso destro per una, 8
inverso per una, 8
inverso sinistro per una, 8
restrizione di una, 8
sottoinsieme chiuso per una, 8
Ordine
di un elemento, 24
di un gruppo, 24
relazione di, 6
parziale, 6
stretto, 6
totale, 6

P
Parte immaginaria
di un numero complesso, 9

Parte reale
di un numero complesso, 9
Partizione(i), 5
più fine, 6
Pascal
triangolo di, 14
Permutazione, 4
Piano
complesso, 10
Polinomio(i), 36, 37
associati, 40
ciclotomico, 42
coefficiente direttore di un, 37
contenuto di un, 41
costante, 37
derivata di un, 48
divisibilità tra, 39
divisione Euclidea tra, 39
fattorizzazione di, 40
grado di un, 37
indeterminata di un, 37
irriducibile, 40
minimo, 47
monico, 37
multiplo di un, 39
nullo, 37
primitivo, 41
quoziente della divisione tra, 39
quoziente di anelli di, 42
radice di un, 38
resto della divisione tra, 39
termine noto di un, 37
valutazione di un, 38
Primitivo
polinomio, 41
Primo(i)
interi
tra loro, 15
intero, 16
polinomi
tra loro, 40
Principio
dei cassetti, 12
del buon ordinamento, 7
del minimo, 7
di inclusione esclusione, 14
di induzione ricorsiva, 8
d'induzione, 7
Prodotto
cartesiano di insiemi, 2
di sottogruppi, 26
diretto di gruppi, 32
per scalare, 43
Proiezione al quoziente, 5
Proprietà
antisimmetrica, 6
irriflessiva, 6
riflessiva, 5, 6
simmetrica, 5
transitiva, 5, 6

Q

Quaternioni
gruppo delle unità dei, 28
Quoziente, 15
della divisione tra polinomi, 39
di anelli di polinomi, 42
di gruppi, 26, 27
insieme, 5
per anelli, 36

R

Radice
dell'unità, 49
di un polinomio, 38
molteplicità di una, 39
multipla, 39
primitiva dell'unità, 11, 49
semplice, 39
Rappresentanti
insieme di, 6
Razionali
numeri, 9
Reali
numeri, 9
Regola
di Leibniz, 48
Relazione(i), 5
classe di equivalenza per una, 5
di equivalenza, 5
d'ordine, 6
d'ordine parziale, 6
d'ordine stretto, 6
d'ordine totale, 6
quoziente per una, 5
Residuo(i), 17
quadratico, 51
Resto, 15
della divisione tra polinomi, 39
Restrizione
di un'operazione, 8
Ricorsione, 7
Ruffini
teorema di, 39

S
Scalare, 43
Simbolo
di Legendre, 51
Simmetrico
gruppo, 29
Sottoanello(i), 35
Sottogruppo(i), 24
classi laterali di un, 26
generato, 25
indice di un, 26
normale, 27
prodotto di, 26
Sottoinsieme, 1
Spazio
vettoriale, 43
Successione, 7

T
Tartaglia
triangolo di, 14
Teorema
cinese dei resti, 19
del binomio di Newton, 14, 35
del binomio ingenuo, 18, 45
delle Estensioni Ciclotomiche, 51
di Cauchy, 32
di Eulero, 21
di Fermat, 19
di Lagrange, 27
di omomorfismo, 30
di Ruffini, 39
di struttura dei gruppi ciclici, 31
fondamentale dell'algebra, 40
fondamentale dell'aritmetica, 16
Termine noto, 37
Torre
di estensioni, 46
Trascendente
elemento, 46
Trasposizione, 29
Triangolo di Tartaglia, 14

U
Unione, 1
disgiunta, 2
Unità
dei quaternioni, 28
di un anello, 33
immaginaria, 9
Unitario
anello, 33
Uno
di un anello, 33

V
Valutazione
di un polinomio, 38
Vettore, 43
colonna, 43
nullo, 43
Vettoriale
spazio, 43

Z
Zero
caratteristica, 44
di un anello, 33