Elenco teoremi e dimostrazioni di aritmetica

Matteo Del Vecchio

Anno Accademico 2019-2020

Introduzione

Questo documento è una lista di argomenti da studiare per sostenere l'esame di aritmetica nell'anno accademico 2019/2020 (il corso è stato tenuto dalla prof. Ilaria Del Corso e dal prof. Davide Lombardo). È stata scritta da me con lo scopo di mantenere un registro di "cosa dovevo sapere" mentre studiavo per l'esame, quindi potrebbe contenere errori/omissioni che si prega di segnalare (delvecchio@mail.dm.unipi.it). Essendo basata sugli argomenti trattati in classe, potrebbe non essere adatta ai corsi di anni accademici successivi, specialmente se tenuti da altri insegnanti. A meno che non sia specificato, bisogna idealmente essere in grado di dimostrare ogni lemma o teorema nella lista. Le sezioni "esercizi standard" contengono categorie "classiche" di esercizi oppure esercizi particolarmente significativi visti in classe, i cui risultati potrebbero risultare utili come fatti generali. Gli argomenti indicati come (Bonus) sono stati effettivamente trattati in classe, ma non credo vengano chiesti in sede d'esame (ma ciò ovviamente non esclude a priori che vengano chiesti).

1 Numeri e induzione

- Insiemi numerici: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
- Numeri naturali: Assiomi di Peano. Principio del minimo, induzione debole, induzione forte. Equivalenza dei tre principi.
- Successioni: numeri di Fibonacci. Risoluzione di ricorrenze lineari omogenee (di ordine 2)

1.1 Esercizi standard

- Trovare e dimostrare per induzione le formule per la somma dei primi n numeri naturali, dei primi n quadrati, dei primi n cubi, dei primi n numeri pari o dispari
- Dimostrare varie proprietà dei numeri di Fibonacci
- Dire per quali $n \in \mathbb{N}$ vale $n! \geq 2^n$ e problemi simili
- Problemi in cui è più facile dimostrare per induzione una proprietà più forte

- Problemi in cui intuire una formula chiusa da dimostrare per induzione (es. modi di tassellare un pavimento)
- Trovare formule chiuse per successioni generiche definite da ricorrenze lineari omogenee di ordine 2

2 Calcolo Combinatorio

- Principio dei cassetti
- Cardinalità di insiemi e legami con iniettività e surgettività di funzioni
- Numero di funzioni tra due insiemi di cardinalità finita
- Numero di funzioni iniettive tra due insiemi di cardinalità finita
- Cardinalità dell'insieme delle parti
- Sottoinsiemi di cardinalità n (coefficienti binomiali)
- Proprietà dei binomiali: $\binom{n}{i} = \binom{n}{n-i}$, $\binom{n}{i} + \binom{n}{i+1} = \binom{n+1}{i+1}$. Dimostrazioni "algebriche", dimostrazioni "insiemistiche" (anche in double counting)
- Sviluppo del binomio: formula di Newton. Dimostrazione per induzione
- $\sum_{i=0}^{n} \binom{n}{i}$: dimostrazione "algebrica", dimostrazione "insiemistica"
- Triangolo di Pascal (sapere cos'è)

Teoria e tecniche utili per gli esercizi

- Contare: scelte disgiunte, scelte indipendenti
- Principio di inclusione-esclusione
- Double counting
- Anagrammi e multinomiali
- Stars and bars (due varianti)

2.1 Esercizi standard

- Contare le funzioni surgettive tra due insiemi di cardinalità finita
- Determinare il numero di sottoinsiemi di cardinalità pari e di cardinalità dispari di un insieme di cardinalità n. Spoiler: sono metà e metà. Nota: si può risolvere in almeno 3 modi diversi: induzione, binomiali, bigezione
- Dato un insieme X di cardinalità finita, contare il numero di coppie (A, B) di suoi sottoinsiemi tali che $|A \cap B| = n$ e simili

3 Divisione euclidea

- Teorema di divisione euclidea in $\mathbb{Z}$
- Relazioni. Relazioni di equivalenza, di ordine, di ordine totale. Maggioranti, minoranti, massimali, minimali, sup, inf. Relazione di divisibilità
- Minimo comune multiplo, massimo comun divisore. Definizioni, esistenza, "unicità"
- Identità di Bézout, algoritmo di Euclide. Dimostrazioni
- (Bonus) Considerazioni sulla complessità computazionale di Euclide
- Numeri primi, numeri irriducibili. Definizione ed equivalenza in $\mathbb{Z}$. Relazioni varie tra massimo comun divisore, coprimalità e divisibilità.
- Equazioni diofantee lineari del primo ordine: esistenza di soluzioni (con dimostrazione), ricerca delle soluzioni
- Teorema fondamentale dell'aritmetica

Utili per esercizi

- Valutazione p-adica
- (Bonus) Primi di Fermat, primi di Mersenne
- (Bonus) Frazioni di Farey

3.1 Esercizi standard

- Applicare l'algoritmo di Euclide a numeri o espressioni parametriche
- Risolvere equazioni diofantee lineari del primo ordine
- (Bonus) Dimostrare che esistono infiniti numeri primi
- Ricavare la formula del numero di divisori di un intero
- Trovare tutte le soluzioni di una diofantea che rispettano condizioni specifiche (es. $x \leq 100$, $y \leq 100$)
- Fattorizzazione di $n!$ (valutazione p-adica per ogni primo $\leq n$)

4 Congruenze

- Congruenze: varie definizioni e loro equivalenza. Definizione tramite relazione di equivalenza e classi di congruenza. Buona definizione delle operazioni. Strutture di gruppo, anello e campo di $\mathbb{Z}/n\mathbb{Z}$
- Proprietà delle congruenze, viste sia come uguaglianze sia come classi
- Equazioni lineari $ax \equiv b$. Sistemi di congruenze. Prima forma del Teorema Cinese del Resto

- Funzione ϕ di Eulero. Calcolo con dimostrazioni. Teorema del "binomio ingenuo". Piccolo teorema di Fermat. Teorema di Eulero. Ordine moltiplicativo e congruenze esponenziali
- Cenni sulla crittografia e sul metodo RSA.

Utili per esercizi

- Congruenze e criteri di divisibilità per 2, 3, 4, 5, 9, 10, 11
- Tecniche per risolvere una congruenza quadratica. Ricondursi al caso modulo p. Numero di soluzioni. Esempi particolari. Idempotenti e nilpotenti in $\mathbb{Z}/n\mathbb{Z}$
- Tecniche per risolvere congruenze esponenziali
- Ricordarsi che se p è primo e $p \equiv 2(mod\ 3)$ allora $f : x \mapsto\ x^3$ è bigettiva

4.1 Esercizi standard

- Saper risolvere equazioni e sistemi di congruenze di più o meno qualsiasi tipo (quadratiche, esponenziali, con parametro, polinomiali con esponenti grandi)
- (Bonus) Dimostrare che esistono n numeri non primi consecutivi e n non potenze perfette consecutive per ogni n (e simili)
- Esercizi vari su funzioni aritmetiche: ϕ, numero di divisori, numero di divisori primi e relazioni. Contare quanti numeri hanno $\phi(n) = a$ con a fissato

5 Gruppi

- Definizione di gruppo e gruppo abeliano. Esempi. Sottogruppi: definizione ed esempi. Centro di un gruppo e proprietà. Sottogruppo generato da un elemento e proprietà
- Proprietà dei gruppi: unicità di neutro e inverso, inverso dell'inverso, inverso di un "prodotto"(in notazione moltiplicativa), leggi di cancellazione.
- Ordine di un elemento, cardinalità ("ordine") del sottogruppo generato da un elemento. Definizione di gruppo ciclico. Ciclicità dei sottogruppi di un gruppo ciclico.
- $n\mathbb{Z}$ come sottogruppi di $\mathbb{Z}$ e ciclicità. Il gruppo $(\mathbb{Z}/n\mathbb{Z}, +)$: ciclicità, ordine di ogni elemento, ordini possibili, numero di elementi di ciascun ordine, numero di generatori (e chi sono). Corollario: $n = \sum_{d|n} \phi(d)$. Sottogruppi di ordine d.
- Omomorfismi di gruppi: definizione (basta una condizione!) e conseguenze: immagine dell'elemento neutro, dell'inverso, immagine e controimmagine di un sottogruppo, $\mathrm{Ker}\, f$ e $\mathrm{Im}\, f$ sono sottogruppi. Kernel e iniettività. Relazione tra ordine di un elemento e ordine della sua immagine nel caso generale e nel caso iniettivo. Definizione di isomorfismo

- Un gruppo ciclico di n elementi è isomorfo a $\mathbb{Z}/n\mathbb{Z}$. Un gruppo ciclico infinito è isomorfo a $\mathbb{Z}$. Conseguenze: valgono le cose dette su $\mathbb{Z}$ e $\mathbb{Z}/n\mathbb{Z}$.

- Prodotto diretto di gruppi. Il centro del prodotto è il prodotto dei centri e conseguenze sull'abelianità di $G_1 \times G_2$. Ordine di un elemento in un prodotto diretto.

- Teorema cinese del resto: "terza forma" (isomorfismo di gruppi). Conseguenza: isomorfismo tra i gruppi moltiplicativi.

- Teorema di Cauchy: dimostrazione per $p = 2$; dimostrazione per G abeliano.

- Relazione di equivalenza sinistra (e destra). Classi laterali sinistre (e destre). (Tenere a mente l'esempio di $\mathbb{Z}/n\mathbb{Z}$ in notazione additiva). Teorema di Lagrange e corollari: teorema di Eulero, un gruppo di ordine p primo è isomorfo a $\mathbb{Z}/p\mathbb{Z}$.

- Sottogruppi normali: due definizioni equivalenti. Normalità e abelianità. Esempi: il centro, l'intersezione di sottogruppi normali. Definizione di indice e normalità dei sottogruppi di indice 2. Gruppo quoziente modulo un sottogruppo normale. Buona definizione dell'operazione. $\mathbb{Z}/n\mathbb{Z}$.

- Omomorfismi $f : G \to G'$ e normalità: normalità del nucleo, elementi che hanno la stessa immagine sono nella stessa classe modulo il nucleo, la controimmagine di un elemento di G' è una classe laterale di G. La proiezione modulo N è un omomorfismo di gruppi e il suo nucleo è N. Corollario: sottogruppi normali e nuclei degli omomorfismi.

- Primo teorema di omomorfismo. Enunciato completo e dimostrazioni. Corollari e "varianti" spesso utili: $G/\operatorname{Ker} f \cong \operatorname{Im} f$, $\frac{G/K}{H/K} \cong G/H$ (secondo teorema di omomorfismo/isomorfismo), $H/(H \cap K) \cong HK/K$ (terzo teorema di omomorfismo/isomorfismo). Teorema di corrispondenza tra sottogruppi.

Utili per esercizi e "slogan" da ricordare (ma ovviamente bisogna saperli dimostrare)

- Dimostrare che $(G, \cdot)$ è un gruppo: $\cdot$ è un'operazione binaria su G - $\cdot$ è associativa - $\cdot$ ha un elemento neutro - ogni elemento di G ha un inverso.

- Verificare se un sottoinsieme è un sottogruppo: è chiuso per operazione - contiene il neutro - contiene l'inverso di ogni elemento

- Se un sottoinsieme è finito, contiene l'elemento neutro ed è chiuso per operazione, allora contiene anche l'inverso di ogni elemento, quindi è un sottogruppo

- L'intersezione di sottogruppi è un sottogruppo

- L'ordine del sottogruppo generato da un elemento è uguale all'ordine dell'elemento

- Ogni sottogruppo di un gruppo ciclico è ciclico

- Un gruppo ciclico di n elementi è isomorfo a $\mathbb{Z}/n\mathbb{Z}$. Un gruppo ciclico infinito è isomorfo a $\mathbb{Z}$.
- Verificare che una funzione è un omomorfismo: è ben definita - $f(ab) = f(a)f(b)\ \forall a, b \in G$
- Verificare che una funzione è isomorfismo: è omomorfismo - è bigettiva
- Sapere dell'esistenza del gruppo infinito delle radici complesse di 1, i cui elementi hanno tutti ordine finito.
- Classificazione di ("sapere chi sono") tutti i gruppi "di ordine basso" (2, 3, 4, 6) e di ordine primo.
- (Lagrange) L'ordine di un sottogruppo divide l'ordine del gruppo. L'ordine di un elemento divide l'ordine del gruppo.
- (Cauchy) Sia G finito e p primo che divide $|G|$. Allora $\exists g \in G :\ ord_G(g) = p$.
- L'unico omomorfismo $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$ è quello banale. Al contrario, esistono n omomorfismi distinti tra $\mathbb{Z}$ e $\mathbb{Z}/n\mathbb{Z}$. Esistono $\gcd(n, m)$ omomorfismi tra $\mathbb{Z}/n\mathbb{Z}$ e $\mathbb{Z}/m\mathbb{Z}$. Per contare gli omomorfismi che rispettano date condizioni è spesso utile caratterizzarli con le immagini di un sistema di generatori del gruppo di partenza. Gli omomorfismi iniettivi da un gruppo ciclico mandano un generatore in un elemento della sua stessa cardinalità. L'omomorfismo verso un prodotto diretto può essere scomposto come prodotto diretto di due omomorfismi.
- Sapere dell'esistenza del gruppo $Aut(G) := \{f : G \to G|\ f \text{ isomorfismo}\}$ e sapere a cosa è isomorfo nei casi $G = \mathbb{Z},\ G = \mathbb{Z}/n\mathbb{Z}$.
- Relazione tra sottogruppi ciclici di ordine n ed elementi di ordine n di un gruppo
- Sottogruppo generato da un insieme
- Ciclicità di $(\mathbb{Z}/p\mathbb{Z})^*$ per p primo e di $(\mathbb{Z}/p^k\mathbb{Z})^*$ per p primo diverso da 2. Applicazione: numero di soluzioni della congruenza $x^k \equiv 1 \pmod{p^e}$
- Sottogruppi normali di G: sono tutti e soli i sottogruppi H tali che $gH = Hg\ \forall g \in G$; tutti e soli i sottogruppi H per cui $gHg^{-1} \subseteq H$ (in realtà questo è equivalente a $gHg^{-1} = H$), tutti e soli i nuclei degli omomorfismi su G.
- $G/Z(G)$ ciclico $\implies G$ abeliano
- Il gruppo $(\mathbb{Z}/p\mathbb{Z})^k$. Considerazioni "vettoriali"
- Sia G gruppo abeliano e $a.b \in G$. Sia $ord_G(a) = n,\ ord_G(b) = m$. $\gcd(m, n) = 1 \implies ord_G(ab) = mn$.

5.1 Esercizi Standard

- Dimostrare proprietà più o meno esoteriche di gruppi, ad esempio una di quelle che seguono o una di quelle della sezione precedente.
- G gruppo. H, K sottogruppi. Dimostrare che HK è sottogruppo $\Leftrightarrow HK = KH$.
- Dimostrare che l'intersezione tra due sottogruppi normali è un sottogruppo normale.
- Dimostrare che $f: G \to G, g \longmapsto g^2$ è omomorfismo $\Leftrightarrow$ G è abeliano.
- Contare elementi di ordine prestabilito in un gruppo (solitamente ottenuto da prodotti diretti). Contare sottogruppi di ordine prestabilito nello stesso gruppo. Contare omomorfismi e omomorfismi iniettivi tra due gruppi.

6 Anelli, campi, polinomi

- Definizioni: anello, anello commutativo, anello con identità
- Definizioni: elemento invertibile, divisore di zero. Dominio di integrità. Campo. Proposizioni: $a \cdot 0 = 0$, $(A^*, \cdot)$ gruppo, legge di annullamento del prodotto nei domini di integrità (oss: può essere usata per definirli), intersezione tra divisori di zero e invertibili. Corollari: ogni campo è dominio di integrità. Ogni dominio di integrità finito è un campo. Definizione: omomorfismo di anelli.
- Polinomi: definizione, anello di polinomi a coefficienti in un anello commutativo con identità. Grado di un polinomio: operazioni e grado per A anello generico e in un dominio di integrità. Corollari: A dominio $\implies$ $A[x]$ dominio. $(A[x])^* = A^*$.
- Polinomi a coefficienti in un campo: teorema di divisione euclidea, conseguenze (vedi sezione "Divisione Euclidea" e cerca di adattare più cose possibili traducendo "valore assoluto" in "grado"). Teorema di Ruffini. Massimo comun divisore: definizione, esistenza e "unicità"(dimostrarlo costruttivamente applicando Euclide).
- Definzione di polinomio irriducibile e di polinomio primo. Equivalenza delle sue definizioni in un campo. Teorema di fattorizzazione unica. Corollario: un polinomio in $K[x]$ di grado n ha al più n radici in K contate con molteplicità.
- Teorema fondamentale dell'algebra (no dimostrazione) e conseguenze: fattorizzazione e irriducibili in $\mathbb{C}$ e $\mathbb{R}$ (radice coniugata). Fattorizzazione in $\mathbb{Q}[x]$ e $\mathbb{Z}[x]$: polinomio primitivo, criterio delle radici razionali, lemma di Gauss (non dimostrato in classe), criterio di riduzione modulo p, criterio di Eisenstein. Corollario: infiniti irriducibili di grado $n > 2$ in $\mathbb{Z}[x]$.
- Ideali: definizione, ideale generato da un polinomio. Quozienti modulo $(f(x))$. L'anello $K[x]/(f(x))$: operazioni, rappresentanti (resti modulo f), base e dimensione come spazio vettoriale su K. Invertibili, divisori di zero, nilpotenti. Corollario:$K[x]/(f(x))$ campo $\Leftrightarrow$ f irriducibile.

- Elementi algebrici e trascendenti. Estensioni di campi. Estensioni algebriche. L'anello $K[\alpha]$ con $\alpha \in F \subseteq K$: omomorfismo di valutazione e isomorfismo con $K[x]/\operatorname{Ker}(\phi_\alpha)$. Chi è $\operatorname{Ker}(\phi_\alpha)$ per α algebrico? L'ideale generato dal polinomio minimo. Polinomio minimo: definizione e proprietà. $K[\alpha]$ è un campo isomorfo a $K(\alpha)$ per α algebrico. Grado di un'estensione. Corollario: ogni estensione finita è algebrica.

- Estensioni algebriche semplici. Teorema dei gradi delle torri di estensioni. Definizione e proprietà di $K[\alpha_1, ..., \alpha_r]$ con $\alpha_1, ..., \alpha_r \in F/K$ algebrici su K.

- Campi algebricamente chiusi. Chiusura algebrica. Teorema non dimostrato: esistenza e "unicità"(a meno di isomorfismo) della chiusura algebrica. Campi di spezzamento. Caratteristica di un campo. Definizione e possibili valori. "Immersione" di $\mathbb{F}_p$ in un campo finito e di $\mathbb{Q}$ in un campo infinito. Considerazioni sul grado del campo di spezzamento ($\leq (deg(p))!$).

- Campi finiti. $\mathbb{F}_p/(f(x))$ è campo finito di $p^{deg(f)}$ elementi. Se un campo è finito allora ha p^n elementi. Criterio della derivata. Esistenza e unicità di $\mathbb{F}_{p^n}$ fissata una chiusura algebrica. Ogni sottogruppo moltiplicativo finito di un campo è ciclico (quindi anche il gruppo moltiplicativo). $\mathbb{F}_{p^n}$ è estensione semplice. $\forall p$ primo, $\forall n \geq 1$ esiste un polinomio irriducibile di grado n e $\mathbb{F}_{p^n} = \mathbb{F}_p/(f(x))$. Sottocampi di $\mathbb{F}_{p^n}$. Campo di spezzamento di un polinomio su $\mathbb{F}_p$ (mcm dei gradi dei fattori irriducibili). Caso particolare: campo di spezzamento di $x^n - 1$, ($\mathbb{F}_{p^d}$ con $d = ord_m(p)$) (saper riprodurre tutto quello che porta a dimostrarlo).

Utili per esercizi

- Dimostrare che $(A, +, \cdot)$ è un anello: $(A, +)$ gruppo, $\cdot$ associativa, proprietà distributive. (ed eventuale identità e commutatività per $\cdot$)

- L'anello dei polinomi a coefficienti in un campo è euclideo (quindi a fattorizzazione unica). (non lo abbiamo detto in questi termini, ma è bene saperlo)

- Il polinomio minimo di α su K è l'unico che rispetta le proprietà: monico - irriducibile su K, si annulla in α.

- Conseguenze delle torri di estensioni: se conosco $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$, allora $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ sarà un suo divisore.

- Due estensioni quadratiche $K(\sqrt{a})$, $K(\sqrt{b})$ sono equivalenti $\Leftrightarrow \exists c \in K^*$ $b = a \cdot c^2$.

- Il campo finito con n elementi è unico a meno di isomorfismo. Tutti e soli gli n per cui esiste sono della forma p^k con p primo e $k \geq 1$. Si ottengono tutti come $\mathbb{F}_p[x]/(f(x))$ per un certo $f(x) \in \mathbb{F}_p[x]$ irriducibile.

- Il campo di spezzamento di $f(x)$ su $\mathbb{F}_p$ è $\mathbb{F}_{p^n}$ dove n è il minimo comune multiplo dei gradi dei suoi fattori irriducibili.

- Il campo di spezzamento di $x^n - 1$ su $\mathbb{F}_p$ è $\mathbb{F}_{p^n}$ con $n = ord_m(p)$.

- L'unico irriducibile di grado due in $\mathbb{F}_2[x]$ è $x^2 + x + 1$. Gli irriducibili di grado 3 sono $x^3 + x + 1$ e $x^3 + x^2 + 1$. Un polinomio di grado 4 senza radici è riducibile solo se è $(x^2 + x + 1)^2$.

6.1 Esercizi standard

- Contare le classi, gli invertibili, i nilpotenti e i divisori di zero dell'anello $\mathbb{F}_p[x]/(f(x))$. (A volte viene richiesto di calcolare l'inverso di un elemento specifico. Usare Euclide per determinare i coefficienti di Bézout, poi considerare le classi nell'anello e sparirà l'addendo con $f(x)$.)

- Determinare il polinomio minimo di α su $\mathbb{Q}$ e su $\mathbb{F}_p$ per qualche p primo, oppure su $\mathbb{Q}(\sqrt{2})$.

- Calcolare il campo di spezzamento di un polinomio su un campo: solitamente su $\mathbb{Q}$ e su $\mathbb{F}_p$ per qualche p primo.