Estensioni quadratiche di $\mathbb{F}_p$.

$\mathbb{F}$ campo finito di caratteristica $p \geq 3$.

Problema: per quali $\Delta \in \mathbb{F}^*$ l'eq. $z^2 - \Delta = 0$ ha soluzioni in $\mathbb{F}$?

I Δ per cui $z^2 - \Delta = 0$ ha soluzioni si dicono residui quadratici. Nota che:

$$(\mathbb{F}^*)^2 = \{\alpha^2 \mid \alpha \in \mathbb{F}^*\} = \left\{\begin{matrix}\text{Residui} \\ \text{quadratici}\end{matrix}\right\}$$

Dunque i residui quadratici formano un sotto-gruppo di $\mathbb{F}^*$.

Fatto:

$$\#\left\{\begin{matrix}\text{residui} \\ \text{quadratici}\end{matrix}\right\} = \frac{|\mathbb{F}| - 1}{2}.$$

Dim.

$\mathbb{F}^*$ ciclico $\Rightarrow$ $G = \mathbb{F}^*/(\mathbb{F}^*)^2$ è ciclico

Siccome

$$[\alpha]^2 = [\alpha^2] = 1 \qquad \forall\, [\alpha] \in G$$

ho che $G \simeq \mathbb{Z}/2\mathbb{Z}$ appena banale.

D'altra parte se G non può essere banale altrimenti si avrebbe che

$$\mathbb{F}^\times = (\mathbb{F}^\times)^2 \Rightarrow \phi : \mathbb{F}^\times \to (\mathbb{F}^\times)^2, \quad x \mapsto x^2$$

omo. suriettivo $\Rightarrow$ isom

$$\Rightarrow \quad \ker(\phi) = (1)$$

$\Rightarrow$ no elementi di ordine 2

$\ker(\phi) = \{x^2 = 1\}$

che è assurdo dato che $|\mathbb{F}^\times| = |\mathbb{F}| - 1$ che è pari.

(teo. di Cauchy!)

$$\Rightarrow \quad \mathbb{F}^\times / (\mathbb{F}^\times)^2 \simeq \mathbb{Z}/2\mathbb{Z}$$

$$\Rightarrow \quad 2 = \left| \mathbb{F}^\times / (\mathbb{F}^\times)^2 \right| = \frac{|\mathbb{F}^\times|}{|(\mathbb{F}^\times)^2|} = \frac{|\mathbb{F}| - 1}{|(\mathbb{F}^\times)^2|}$$

$$\Rightarrow \quad 2 = \frac{|\mathbb{F}| - 1}{\#\text{residui quadratici}} \qquad \text{QED.}$$

Nota: se $\pi : \mathbb{F}^\times \to \mathbb{F}^\times / (\mathbb{F}^\times)^2$ è la proiezione al quoziente ho che

$$\boxed{a \text{ residuo quadratico} \iff \pi(a) = 1}$$

Di conseguenza ho che

$$\begin{pmatrix}\text{residuo}\\ \text{quadratico}\end{pmatrix}\cdot\begin{pmatrix}\text{residuo}\\ \text{quadratico}\end{pmatrix}=\begin{pmatrix}\text{residuo}\\ \text{quadratico}\end{pmatrix}.$$

$$\begin{pmatrix}\text{non residuo}\\ \text{quadratico}\end{pmatrix}\cdot\begin{pmatrix}\text{non residuo}\\ \text{quadratico}\end{pmatrix}=\begin{pmatrix}\text{residuo}\\ \text{quadratico}\end{pmatrix}.$$

$$\begin{pmatrix}\text{non residuo}\\ \text{quadratico}\end{pmatrix}\cdot\begin{pmatrix}\text{residuo}\\ \text{quadratico}\end{pmatrix}=\begin{pmatrix}\text{non residuo}\\ \text{quadratico}\end{pmatrix}.$$

Nota: se $\alpha\in\overline{\mathbb{F}}$ è una radice di $z^2-\Delta$ ho che

$$[\mathbb{F}(\alpha):\mathbb{F}]=2 \iff \Delta \text{ non è residuo quadratico}$$

e che se Δ è residuo quadratico $\alpha\in\mathbb{F}$ e di conseguenza $\mathbb{F}(\alpha)=\mathbb{F}$ $(\Rightarrow [\mathbb{F}(\alpha):\mathbb{F}]=1)$.

EX $\mathbb{F} = \mathbb{F}_p$, p primo ≥ 3.

Per quali $p \geq 3$, $\Delta = -1$ è un residuo quadratico in $\mathbb{F}_p$?

Risposta:

> -1 è un residuo quadratico in $\mathbb{F}_p$ $\Leftrightarrow$ $p \equiv 1 \pmod 4$.

Dim:

"$\Rightarrow$" $\exists\, \alpha \in \mathbb{F}_p$ t.c. $\alpha^2 = -1$. Ora

$$\alpha^2 = -1 \Rightarrow \alpha^4 = 1$$

$$\Rightarrow \operatorname{ord}(\alpha) = \cancel{1}, \cancel{2}, 4$$

perché se no $\alpha = 1$ $\Rightarrow 1 = \alpha^2 = -1$ assurdo

perché se no $1 = \alpha^2 = -1$ assurdo

$$\Rightarrow 4 = \operatorname{ord}(\alpha) \mid |\mathbb{F}_p^*| = p - 1$$

$$\Rightarrow p \equiv 1 \pmod 4$$

"$\Leftarrow$" Devo produrre $\alpha \in \mathbb{F}_p$ t.c. $\alpha^2 = -1$.

$p \equiv 1 \pmod 4 \Rightarrow p - 1 = 4 \cdot k$

Per Wilson: $(4k)! = (p-1)! = -1 \pmod p$.

$$\Rightarrow \quad (2k)! \cdot (2k+1)(2k+2)\cdots(2k+2k) = -1 \pmod p$$

$$2k+1 = 2k+1-p = 2k-4k = -2k$$

$$2k+2 = 2k+2-p = 2k+1-4k = -(2k-1)$$

$$\vdots$$

$$2k+2k = 2k+2k-p = 2k+2k-1-4k = -1$$

$$\Rightarrow (2k+1)(2k+2)\cdots(2k+2k) = (-2k)\cdot(-(2k-1))\cdot\ldots\cdot(-1)$$

$$= (-1)^{2k}\cdot(2k)\cdot(2k-1)\cdot\ldots\cdot 1$$

$$= (2k)!$$

$$\Rightarrow \quad (2k)!\cdot(2k)! = -1 \pmod p$$

$$\Rightarrow \quad \alpha^2 = -1 \pmod p \quad \text{dove } \alpha = (2k)!\,, \quad \uparrow \tfrac{1}{2}\cdot(p-1).$$

In altre parole se $p \equiv 1 \pmod 4$ esiste $\sqrt{-1} \in \mathbb{F}_p$ e vale la formula:

$$\boxed{\sqrt{-1} = \left(\frac{p-1}{2}\right)!}$$

Ex. $\mathbb{F} = \mathbb{F}_{2011}$. $\alpha, \beta \in \overline{\mathbb{F}_{2011}}$ $\alpha^2 = 5$ $\beta^2 = -5$

Calcolare $[\mathbb{F}(\alpha+\beta) : \mathbb{F}]$.

Sol.: 2011 è primo

$$2011 = 2 \cdot 10^3 + 11 = 11 = 3 = -1 \pmod 4$$

$\Rightarrow -1$ non è residuo quadratico.

1) 5 residuo quadratico $\Rightarrow$ $-5 = -1 \cdot 5$ non è residuo quadratico

$\Rightarrow$ $\mathbb{F}(\alpha+\beta) = \mathbb{F}(\beta)$

e $[\mathbb{F}(\alpha+\beta) : \mathbb{F}] = [\mathbb{F}(\beta) : \mathbb{F}] = 2$

2) 5 non è residuo quadratico $\Rightarrow$ $-5 = -1 \cdot 5$ è residuo quadratico

$\Rightarrow$ $\mathbb{F}(\alpha+\beta) = \mathbb{F}(\alpha)$

e $[\mathbb{F}(\alpha+\beta) : \mathbb{F}] = [\mathbb{F}(\alpha) : \mathbb{F}] = 2$