Sia p un primo e $n \geq 1$. Allora il gruppo moltiplicativo $\mathbb{F}_{p^n}^*$ è ciclico.

DIMOSTRAZIONE 1

- Lemma: Sia G un gruppo abeliano; $\alpha, \beta \in G$ con $o(\alpha)=a$, $o(\beta)=b$. e

$$MCD(a,b)=1 \Rightarrow o(\alpha\beta)=ab.$$

DIM $(\alpha\beta)^{ab} = \alpha^{ab}\beta^{ab} = 1^b 1^a = 1$ quindi $o(\alpha\beta) \mid ab$

Viceversa: supponiamo $(\alpha\beta)^c = \alpha^c\beta^c = 1$ per $1 \leq c < ab$

$\Rightarrow \alpha^c = \beta^{-c}$. In particolare $o(\alpha^c) = o(\beta^{-c})$ e $o(\alpha^c) \mid a$, $o(\beta^{-c}) \mid b$

dunque $o(\alpha^c) = o(\beta^{-c}) \mid MCD(a,b)=1 \Rightarrow o(\alpha^c)=1=o(\beta^{-c}) \Rightarrow$

$\Rightarrow \alpha^c = 1 \Rightarrow a \mid c$; $b^{-c}=1 \Rightarrow b \mid c \Rightarrow ab \mid o(\alpha\beta)$.

Ne segue $o(\alpha\beta)=ab$. □

- Sia $\alpha \in \mathbb{F}_{p^n}^*$ un elemento di ordine $o(\alpha)=n$ MASSIMO $\Rightarrow n \mid (p^n-1)$.

$\forall \beta \in \mathbb{F}_{p^n}^*$ $o(\beta) \mid n$. Altrimenti esisterebbe un i tale che $o(\beta^i)=t \neq 1$

e $MCD(t,r)=1$ e dunque β^t avrebbe per il lemma ordine $t \cdot r > r$. /

In particolare $\beta^r = 1 \Rightarrow (x^r - 1)$ ha come radice β.

Poiché siamo in un campo questo vuol dire $(x-\beta) \mid (x^r - 1)$

$$\forall \beta \in \mathbb{F}_{p^n}^* \Rightarrow f(x) = \prod_{\beta \in \mathbb{F}_{p^n}^*} (x-\beta) \mid (x^r - 1)$$

$f(x)$ è un polinomio di grado $|\mathbb{F}_{p^n}^*| = p^n - 1 \Rightarrow r \geq p^n - 1$

Ne segue $r = p^n - 1$ ed esiste dunque un elemento in $\mathbb{F}_{p^n}^*$ di ordine $p^n - 1 \Rightarrow \mathbb{F}_{p^n}^*$ è ciclico

□

DIMOSTRAZIONE 2

- Lemma: $\forall n$: $\boxed{\sum_{d \mid n} \varphi(d) = n}$

DIM:

Sia $S_d = \{ m \in \mathbb{Z} : 1 \leq m \leq n, MCD(m,n) = d \}$ e $\delta_d = |S_d|$

poiché ogni numero $\leq n$ ha un MCD con n che è un

divisore di n abbiamo

$$\sum_{d|n} \delta_d = n$$

D'altro canto $S_d = \{ m \in \mathbb{Z} : 1 \leq m \leq \frac{n}{d} \mid MCD\left(m, \frac{n}{d}\right) = 1 \} \Rightarrow$

$$\Rightarrow |S_d| = \varphi\left(\frac{n}{d}\right)$$

Ne segue $$\sum_{d|n} \delta_d = n = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d)$$

↑ riarrangiando la somma

□

DIM (teorema).

Sia $\psi_d := \{ x \in \mathbb{F}_{p^n}^* \mid o(x) = d \}$ e $\psi(d) := |\psi_d|$.

Chiaramente ogni elemento di $\mathbb{F}_{p^n}^*$ appartiene ad esattamente un insieme $\psi_d \Rightarrow \sum_{1 \leq d \leq p^n} \psi(d) = p^n - 1$

Inoltre se $d \nmid p^n - 1$ si ha $\psi(d) = 0$, $\Rightarrow \sum_{d|p^n-1} \psi(d) = p^n - 1$

D'altro canto se $d \mid p^n - 1 \Rightarrow H_d := \{ x \mid x^d - 1 = 0 \} \leq \mathbb{F}_{p^n}^*$

che contiene al più d elementi (perché $x^d - 1 = 0$ ha al più d radici). Osserviamo che in H_d il numero di elementi di ordine esattamente d è al più $\varphi(d)$.

Se c'è un elemento di ordine $d \Rightarrow o_t\ |H_d| = \varphi(d)$
se non c'è $0 = |H_d| \leq \varphi(d)$

Dunque $\psi(d) \leq \varphi(d) \quad \forall d,\ d \mid n$

Ne segue $\sum_{d \mid p^n-1} \psi(d) = p^n - 1 = \sum_{d \mid p^n-1} \varphi(d) \qquad \psi(d) \leq \varphi(d)$

Da cui $\forall d : d \mid p^n - 1$ si ha $\varphi(d) = \psi(d)$.

In particolare $0 \neq \varphi(p^n - 1) = \psi(p^n - 1)$

e dunque esiste almeno un elemento di ordine $p^n - 1$ in $\mathbb{F}_{p^n}^*$

□