In questa nota mostriamo il seguente

Teorema: Sia n un numero primo.

Allora $\left(\mathcal{U}(\mathbb{Z}/_{n}\mathbb{Z}), \cdot\right) \simeq \left(\mathbb{Z}/_{(n-1)}\mathbb{Z}\,; +\right)$

In altre parole, esiste $a \in \mathcal{U}(\mathbb{Z}/_{n}\mathbb{Z}) = \mathbb{Z}/_{n\mathbb{Z}} - \{0\}$ di ordine $n-1$ $\left(= |\mathcal{U}(\mathbb{Z}/_{n}\mathbb{Z})|\right)$.

Per la dimostrazione avremo bisogno del seguente fatto:

Fatto: Sia G un gruppo commutativo. Se G contiene $a, b \in G$ di ordine $o(a) = n$ e $o(b) = m$ allora contiene anche $c \in G$ di ordine $o(c) = \text{mcm}(o(a), o(b))$.

Pf. del fatto.

L'idea e' considerare l'elemento ab e cercare di calcolare il suo ordine.

Osserviamo subito che $(ab)^{nm} \underset{\text{perche' } G \text{ e' commutativo}}{=} (a^n)^m \cdot (b^m)^n \underset{\substack{\text{perche'} \\ n = o(a) \\ m = o(b).}}{=} 1$

$\Rightarrow$ $o(ab)$ divide nm.

Tuttavia non e' detto che $o(ab) = nm$,

infatti osserviamo anche che nel caso $a=x$, $b=x^{-1}$ abbiamo $ab=1$ e $1=o(1) < o(a)=o(b)=n$.

In generale, se $(ab)^t=1$ allora

$$1=(ab)^t=a^tb^t \implies a^t=b^{-t}$$
$$\implies o(a^t)=o(b^{-t})$$

il LHS divide $o(a)$, mentre il RHS divide $o(b)$.

Questo suggerisce il seguente:

Claim: Se $n=o(a)$, $m=o(b)$ sono coprimi allora $o(ab)=nm=\mathrm{mcm}(n,m)$.

Pf. del claim.

Per quanto detto sopra

$$a^{o(ab)}=b^{-o(ab)}$$
$$\implies 1=\left(a^{o(ab)}\right)^n=\left(b^{-o(ab)}\right)^n=b^{-n\,o(ab)}$$

$\implies$ $m=o(b)$ divide $n\cdot o(ab)$
siccome n e m sono coprimi, necessariamente m divide $o(ab)$.

Similmente, $1=\left(b^{-o(ab)}\right)^m=\left(a^{o(ab)}\right)^m=a^{m\cdot o(ab)}$ implica che n divide $o(ab)$. Di conseguenza nm divide $o(ab)$ come volevamo dimostrare.

Questo conclude la dimostrazione del claim. $\varnothing$

Continuiamo con il Fatto.
Ci rimane da considerare il caso in cui n, m hanno fattori comuni. Lo riconduciamo al caso precedente in questo modo:
Fattorizziamo in primi

$$\text{mcm}(n,m) = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

e osserviamo che ogni fattore $p_j^{\alpha_j}$ divide n oppure m. Come visto a lezione, se G contiene un elemento g di ordine s e d divide s allora G contiene anche un elemento di ordine d (basta prendere $g^{s/d}$). Questo ci permette di costruire per ogni $j = 1, \dots, k$ un elemento c_j di ordine $p_j^{\alpha_j}$.

Consideriamo $c := c_1 \cdots c_k$

Claim: $o(c) = p_1^{\alpha_1} \cdots p_k^{\alpha_k} = \text{mcm}(n,m)$

Pf. del claim.

Formalmente possiamo procedere per induzione sul numero k di fattori: supponiamo di sapere che

$o(c_1 \dots c_j) = p_1^{\alpha_1} \dots p_j^{\alpha_j}$ e calcoliamo

$o(c_1 \dots c_{j+1})$: siccome $o(c_1 \dots c_j) = p_1^{\alpha_1} \dots p_j^{\alpha_j}$

e $o(c_{j+1}) = p_{j+1}^{\alpha_{j+1}}$ sono coprimi possiamo applicare il primo claim e troviamo

$o((c_1 \dots c_j) c_{j+1}) = o(c_1 \dots c_j) o(c_{j+1})$

come volevamo dimostrare.

Questo finisce la dimostrazione del claim e del fatto. $\boxtimes$

Vediamo come applicare il fatto per dimostrare il teorema

Pf. del Teorema:

Vogliamo far vedere che esiste $a \in U(\mathbb{Z}/n\mathbb{Z})$ di ordine $n-1$. Quello che possiamo fare è prendere un elemento di ordine massimo (siccome $U(\mathbb{Z}/n\mathbb{Z})$ è finito, ogni elemento ha ordine finito), diciamo $a \in \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ di ordine m. Chiaramente $m \leq n-1$, ma a priori non sappiamo se vale l'uguaglianza. Mostriamo la seguente cosa

Claim: Ogni $b \in \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ ha ordine che divide $m = o(a)$.

Pf. del claim.

Qui è dove usiamo il Fatto.

Se esistesse b di ordine che non divide $m = o(a)$ allora, siccome $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ è commutativo, esisterebbe anche un elemento $c \in \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ di ordine $o(c) = \text{mcm}\big(o(a), o(b)\big) > o(a)$ (perché $o(b)$ non divide $o(a)$). Tuttavia a era stato scelto di ordine massimo, questo produce una contraddizione e conclude la dimostrazione del claim. $\boxtimes$

Dunque ogni $b \in \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ soddisfa $b^m = 1$ dove $m = o(a)$. In altre parole, ogni $b \in \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ e' una radice del polinomio $X^m - 1$ (a coefficienti nel campo $\mathbb{Z}/n\mathbb{Z}$).

perche' n e' primo

Siccome un polinomio a coeff. in un campo ha grado $\geq$ numero di radici (perche' se $\beta_1, \dots, \beta_k$ sono radici di $X^m - 1$ allora $X^m - 1 = (X - \beta_1) \cdots (X - \beta_k) q(X)$ con $\deg q(X) = m - k$) ne deduciamo che $m \geq |\mathcal{U}(\mathbb{Z}/n\mathbb{Z})| = n - 1$ e, di conseguenza, $m = n - 1$ come volevamo dimostrare.

Questo finisce la dimostrazione del teorema. $\boxtimes$

Facciamo qualche esempio

- $\mathcal{U}(\mathbb{Z}/5\mathbb{Z}) = \{1, 2, 3, 4\}$

un generatore è 2: infatti

$2^1 = 2 \quad 2^2 = 4 \quad 2^3 = 8 = 3 \quad 2^4 = 1 \quad \mathrm{mod}\ 5$
$ \overset{\|}{-1}$

- $\mathcal{U}(\mathbb{Z}/7\mathbb{Z}) = \{1,2,3,4,5,6\}$

in questo caso 2 non genera (perché $2^3 = 8 = 1 \ \mathrm{mod}\ 7 \Rightarrow o(2) \leq 3$),

ma 3 sí: infatti

$3^1 = 3 \quad 3^2 = 9 = 2 \quad 3^3 = 6 \quad 3^4 = 18 = 4 \quad 3^5 = 12 = 5 \quad 3^6 = 1 \quad \mathrm{mod}\ 7$
$ \overset{\|}{-1}$

⚠ • Non è vero che $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ è sempre ciclico! Neanche nel caso $n = p^\alpha$ con p un numero primo. Un esempio è $\mathcal{U}(\mathbb{Z}/8\mathbb{Z}) = \{1,3,5,7\}$

in questo caso $1^2 = 3^2 = 5^2 = 7^2 = 1$, tutti gli elementi hanno ordine ≤ 2.

Infatti, un facile calcolo mostra che

$$\mathcal{U}(\mathbb{Z}/8\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

tramite l'isomorfismo

$$\varphi : \begin{cases} 1 \to (0,0) \\ 3 \to (1,0) \end{cases} \quad \begin{cases} 5 \to (0,1) \\ 7 \to (1,1) \end{cases}.$$