1 Gruppo moltiplicativo dei gruppi ciclici finiti

Osservazione 1. Abbiamo osservato nel corso di Aritmetica che

$$(\mathbb{Z}_p)^\star \cong \mathbb{Z}_{p-1}$$

Mostreremo adesso che

$$(Z_{p^\alpha})^\star \cong \mathbb{Z}_{\phi(p)}$$

ovvero che tale gruppo è ciclico se e solo se p è un primo dispari

Lemma 1.1. *Sia p un primo dispari e k un intero non nullo*

$$(1+p)^{p^k} = 1 + \lambda p^{k+1} \text{ con } \lambda \in \mathbb{N} - \{0\} \text{ e } M.C.D(\lambda, k) = 1$$

Dimostrazione. Induzione su k.
Se $k = 1$

$$(1+p)^p = 1 + \binom{p}{1}p + \binom{p}{2}p^2 + \cdots + \binom{p}{i}p^i + \cdots + p^p$$

Osserviamo che p^2 divide tutti i termini della sommatoria ad esclusione del primo, mentre p^3 divide tutti i termini tranne i primi 2 da cui

$$(1+p)^p = 1 + p^2\,(1 + \lambda' p)$$

infatti $\binom{p}{1} = p$.
Ponendo $1 + \lambda' p = \lambda$ osserviamo che $M.C.D(\lambda, p) = 1$ dunque abbiamo la tesi.
Supponiamo, per induzione che

$$(1+p)^{p^k} = 1 + \lambda p^{k+1} \text{ con } M.C.D(\lambda, p) = 1$$

Dalla propietà delle potenze osserviamo che

$$(1+p)^{p^{k+1}} = \left(1 + \lambda p^{k+1}\right)^p = 1 + \sum_{i=1}^{p} \binom{p}{i} \lambda^i p^{(k+1)i}$$

Ora p^{k+2} divide tutti i termini della sommatoria dunque

$$(1+p)^{p^{k+1}} = 1 + p^{k+2}\,(\lambda + up)$$

dunque poichè per ipotesi induttiva λ è primo con p posto $\lambda' = \lambda + up$ otteniamo la tesi

□

Proposizione 1.2. *Sia p un primo dispari a $\alpha \in \mathbb{N}$ con $\alpha \geq 2$ allora $(\mathbb{Z}_{p^\alpha})\star$ è ciclico*

Dimostrazione. Poichè la cardinalità del gruppo è $p^{\alpha-1}(p-1)$, per mostrare che il gruppoi è ciclico basta trovare un elemento con ordine $p^{\alpha-1}(p-1)$.
Osserviamo che $(1+p)$ ha ordine $p^{\alpha-1}$ infatti per il lemma precedente

$$(1+p)^{p^{\alpha-1}} = 1 + \lambda p^\alpha \equiv 1 \mod p^\alpha$$

dunque l'ordine di $1+p$ divide $p^{\alpha-1}$.
Se l'ordine di $1+p$ fosse un divisore proprio di $p^{\alpha-1}$ allora

$$(1+p)^{p^{\alpha-2}} \equiv= 0 \mod p^\alpha$$

ma ciò è assurdo in quanto

$$(1+p)^{p^{\alpha-2}} = 1 + p^{\alpha-1}\lambda \equiv 1 \mod p^{\alpha} \quad \Leftrightarrow \quad \lambda \equiv 0 \mod p^{\alpha} \quad \Rightarrow \quad \lambda \equiv 0 \mod p$$

Ma ciò è assurdo infatti per il lemma λ è primo con p e non è nullo.
Per concludere la dimostrazione basta trovare un elemento di ordine $p-1$ infatti se α e β commutano, hanno ordine primi tra loro allora l'ordine di $\alpha\beta$ è il prodotto degli ordini.
Consideriamo adesso l'omomorfismo

$$\psi : (\mathbb{Z}_{p^\alpha})^\star \to (\mathbb{Z}_p)^\star \quad [a]_{p^\alpha} \to [a]_p$$

Osserviamo che tale omomorfismo è ben definito (se a è inverti bile modulo p^α lo è anche modulo p) è suriettivo.
Sia x un generatore di $(\mathbb{Z}_p)^\star$.
Essendo l'omomorfismo suriettivo, esiste un $\beta \in (\mathbb{Z}_{p^\alpha})^\star$ tale che $\psi(\beta) = x$ dunque l'ordine di β deve essere un multiplo dell'ordine di x ($p-1$).
Ora esiste un $\beta' \in \langle\beta\rangle$ tale che $o(\beta') = p-1$.
$\beta'(p+1) \in (\mathbb{Z}_{p^\alpha})^\star$ inoltre tale elemento ha ordine uguale alla cardinalità del gruppo moltiplicativo, che è dunque ciclico □

Studiamo ora cosa succede quando $p = 2$, andremo a dimostrate che in questo caso (tranne nel caso 4) il gruppo moltiplicativo non è ciclico.

Lemma 1.3. *Sia $k \in \mathbb{N}$ con $k \neq 0$ allora*

$$5^{2^k} = 1 + \lambda 2^{k+2} \text{ con } \lambda \text{ dispari}$$

Dimostrazione. Induzione su k.
Per $k = 1$ osserviamo che $5^2 = 1 + 3 \cdot 2^3$.
Supponiamo che la tesi sia vera per k, mostriamo che è vera anche per $k+1$

$$5^{2^{k+1}} = \left(5^{2^k}\right)^2 = \left(1 + \lambda 2^{k+2}\right)^2 = 1 + \lambda^2 2^{2k+4} + \lambda 2^{k+3} = 1 + \lambda(1 + 2^\alpha\lambda)2^{k+3}$$

Osserviamo ora che $\lambda(1 + 2^\alpha\lambda)$ è dispari dunque otteniamo la tesi.

Proposizione 1.4. *Il gruppo $(\mathbb{Z}_{2^\alpha})^\star$ non è ciclico.*
In particolare

$$(\mathbb{Z}_{2^\alpha})^\star \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$$

Dimostrazione. Consideriamo l'omomorfismo

$$\psi : (\mathbb{Z}_{2^\alpha})^\star \to (\mathbb{Z}_4)^\star \quad [a]_{2^\alpha} \to [a]_4$$

Tale omomorfismo è ben definito e suriettivo.
Osserviamo che il $\ker\psi$ ha esattamente $2^{\alpha-2}$ elementi (l'omomorfismo è suriettivo).
Per il lemma precedente, possiamo concludere che il nucleo è ciclico, 5 appartiene al nucleo e ha ordine $2^{\alpha-2}$.
Osserviamo inoltre che $\ker\psi \lhd (\mathbb{Z}_{2^\alpha})^\star$ $\{1,-1\} \lhd (\mathbb{Z}_{2^\alpha})^\star$, inoltre $\ker\psi \cap \{1,-1\} = \{1\}$.
Per ragioni di cardinalità segue che $(\mathbb{Z}_{2^\alpha})^\star = \ker\psi\{1,-1\}$ e dato che sono entrambi normali

$$(\mathbb{Z}_{2^\alpha})^\star = \{1,-1\} \times \ker\psi \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^\alpha-2}$$

□

Possiamo adesso studiare $(\mathbb{Z}_n)^\star$.
Supponiamo infatti

$$n = p_1^{\alpha_1} \dots p_n^{\alpha_n}$$

allora come sappiamo

$$\mathbb{Z}_n \cong \prod_{i=1}^{n} \mathbb{Z}_{p_i^{\alpha_i}}$$

ed inoltre

$$(\mathbb{Z}_n) \star \cong \prod_{i=1}^{n} \left(\mathbb{Z}_{p_i^{\alpha_i}}\right)^\star$$

infatti se un elemento è invertibile in $\mathbb{Z}_n$ allora deve essere invertibile in ogni componente $\mathbb{Z}_{p^\alpha}$ e viceversa.

Proposizione 1.5. *$(\mathbb{Z}_n)^\star$ è ciclico solamente nei seguenti casi*

- $n = 2$
- $n = 4$
- $n = 2p^\alpha$ *con p primo dispari e $\alpha \in \mathbb{N}$ non nullo*
- $n = p^q$ *con p primo dispari e $\alpha \in \mathbb{N}$*

Dimostrazione. Da quanto visto precedentemente, in questi casi il gruppo moltiplicativo è ciclico.
Supponiamo adesso $n = p_1^{\alpha_1} \cdot p_n^{\alpha^n}$ con p_s, p_t primi dispari distinti.
Allora per il ragionamento precedentemente fatto

$$(Z_n)^\star \cong \left(\mathbb{Z}_{p_1^{\alpha_1}}\right)^\star \times \dots \times \left(\mathbb{Z}_{p_s^{\alpha_s}}\right)^\star \times \dots \times \left(\mathbb{Z}_{p_t^{\alpha_t}}\right)^\star \times \dots \times \left(\mathbb{Z}_{p_n^{\alpha_n}}\right)^\star$$

Ora $\left(\mathbb{Z}_{p_t^{\alpha_t}}\right)^\star \times$ e $\left(\mathbb{Z}_{p_s^{\alpha_s}}\right)^\star \times$ sono ciclici di ordine pari dunque entrambi contengono una copia isomorfa a $\mathbb{Z}_2$.
$(\mathbb{Z}_n)^\star$ dunque contiene una copia isomorfa a $\mathbb{Z}_2 \times \mathbb{Z}_2$ dunque non può essere ciclica.
Con un ragionamento analogo si mostra che $n \neq 2^\alpha p^\beta$ con $\alpha > 1$