TEOREMA CINESE DEI RESTI

m_1, m_2 interi (coprimi) $\qquad n = m_1 \cdot m_2$

$$\Gamma : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \qquad \Gamma \text{ biettiva}$$
$$[a]_n \longmapsto ([a]_{m_1}, [a]_{m_2})$$

m_1, m_2 interi coprimi $(n = m_1 \cdot m_2)$
Allora posso considerare il sistema di congruenze

$$\begin{cases} x \equiv a \pmod{m_1} & a \in \mathbb{Z} \\ x \equiv b \pmod{m_2} & b \in \mathbb{Z} \end{cases}$$

Questo sistema ha soluzioni per ogni $a, b \in \mathbb{Z}$.

$$\Gamma : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$$
$$[x]_n \longmapsto ([x]_{m_1}, [x]_{m_2}) = ([a], [b])$$

Per trovare x uso il fatto che $MCD(m_1, m_2) = 1$ e la formula di Bezout: $\exists\ \alpha, \beta$ t.c.

$$\boxed{1 = \alpha m_1 + \beta m_2}$$

$$a = a\alpha m_1 + a\beta m_2$$
$$a\beta m_2 = a - a\alpha m_1 \equiv a \pmod{m_1}$$

$$b = b\alpha m_1 + b\beta m_2$$
$$b\alpha m_1 = b - b\beta m_2 \equiv b \pmod{m_2}$$

$$c = a\beta m_2 + b\alpha m_1$$

es:
$$\begin{cases} x \equiv 4 \pmod 5 \\ x \equiv 3 \pmod 9 \end{cases}$$

$a=4$
$b=3$
$m_1=5$
$m_2=9$

$MCD(5,9) = 1$

$1 = \underset{\alpha}{\underset{\shortparallel}{2}} \cdot 5 + (-\underset{\beta}{\underset{\shortparallel}{1}}) \cdot 9$

$c = a\beta m_2 + b\alpha m_1 = 4\cdot(-1)\cdot 9 + 3\cdot 2\cdot 5 = -6$

$[-6]_{45}$ ad es: 39 é ok

Piccolo Teorema di Fermat

Prop: In $\mathbb{Z}_n$ un elemento $\bar{a}$ é invertibile $\iff MCD(a,n)=1$.

Corollario: $\mathbb{Z}_p$ é un campo $\iff p$ é primo.

dim: • l'enunciato é ben posto

se $c \equiv a \pmod n$, e $MCD(a,n)=1$

$\overset{?}{\implies} MCD(c,n) = 1$.

$\exists\, \alpha, \beta$ t.c. $1 = \alpha a + \beta n$

se $c \equiv a \pmod n \implies c = a + kn$ $a = c - kn$ per qualche $k \in \mathbb{Z}$

$1 = \alpha a + \beta n = \alpha(c-kn) + \beta n$
$= \alpha c - \alpha k n + \beta n = \alpha c + (\beta - \alpha k) n$

cioè $1 = \alpha c + \gamma n$ $\quad \gamma = \beta - \alpha k$

$\Longrightarrow \mathrm{MCD}(c,n) = 1$

un elemento $\bar{a}$ è invertibile $\Longleftrightarrow \mathrm{MCD}(a,n) = 1$

($\Longrightarrow$) $\bar{a}$ invertibile, $\exists\, \bar{b}$ t.c.

$\bar{a} \cdot \bar{b} = \overline{ab} = \bar{1}$ in $\mathbb{Z}_n$

cioè $\exists\, k$ t.c. $ab = 1 + kn$

$$\underbrace{1 = ab + (-k)n}_{\Longleftrightarrow\ \mathrm{MCD}(a,n) = 1}$$

($\Longleftarrow$) $\mathrm{MCD}(a,n) = 1$

$\exists\, \alpha, \beta$ t.c. $1 = \alpha \cdot a + \beta n$

$\Longrightarrow 1 \equiv \alpha a \pmod{n}$

$\bar{1} = \overline{\alpha a} = \bar{\alpha} \cdot \bar{a}$

inverso di $\bar{a}$

$\#$

Prop: Sia $n \geq 1$, e siano $a, b, c, d \in \mathbb{Z}$ tali che:

$$\begin{cases} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{cases}$$

Allora: $a + c \equiv b + d \pmod{n}$

$a \cdot c \equiv b \cdot d \pmod{n}$ –

dim per casa usare: $\boxed{\begin{matrix} n \mid a - b \\ n \mid c - d \end{matrix}}$

<u>oss:</u> usando il risultato sopra, posso anche dim che $a \equiv r \pmod n \Longrightarrow a^k \equiv r^k \pmod n$

per ogni $k \in \mathbb{N}$

<u>Piccolo teo di Fermat:</u> Sia p un primo e sia $a \in \mathbb{Z}$ un intero non divisibile per p. Allora

$$a^{p-1} \equiv 1 \pmod p.$$

<u>dim:</u> Sia p primo > 0 e sia

$S = \{1, 2, 3, \dots, p-1\}$

Sia $a \in \mathbb{Z}$ non divisibile per p.

Per ogni $k \in S$, dividiamo $a \cdot k$ per p:

$$a \cdot k = q_k p + r_k \qquad 0 \leq r_k < p$$

<u>oss:</u> $p \nmid a$ (→ non divide) $\qquad p \nmid k$ per nessun $k \in S$

$\Longrightarrow p \nmid a \cdot k$ (perché p è primo)

$\Longrightarrow$ i resti r_k sono tutti $\neq 0$

e sono tutti $0 < r_k < p$ cioè

gli $r_k \in S = \{1, 2, \dots, p-1\}$

definiamo $\varphi : S \longrightarrow S$, $k \longmapsto r_k$

φ è biettiva: è sufficiente dim. che è iniettiva, perché è un'applicazione da un insieme finito in se stesso.

iniettiva: siano $h, k \in S$ tali che $\underset{\substack{\parallel \\ r_h}}{\varphi(h)} = \underset{\substack{\parallel \\ r_k}}{\varphi(k)}$

$a \cdot h \equiv a \cdot k \pmod p$

$p \mid ah - ak = a \cdot (h-k) \Longrightarrow$ $p \mid a$ <u>no</u>; $p \mid h-k \Longrightarrow h-k=0$, $h=k$

<u>OSS:</u> $r_k \equiv a \cdot k \pmod p$

$\underbrace{r_1 \cdot r_2 \cdot \ldots \cdot r_{p-1}}$ $= (p-1)!$

sono tutti i numeri da 1 a $p-1$ permutati.

$a \cdot k \equiv r_k \pmod p$

$a^{p-1} \cdot (p-1)! = (a \cdot 1)(a \cdot 2) \cdot (a \cdot 3) \cdot \ldots \cdot (a \cdot (p-1))$

$\equiv r_1 \cdot r_2 \cdot r_3 \cdots r_{p-1} \pmod p$

$\equiv (p-1)! \pmod p$

$p \mid a^{p-1}(p-1)! - (p-1)! = (a^{p-1} - 1)(p-1)!$

$\Longrightarrow$ $p \mid (p-1)!$ <u>no</u>; $p \mid a^{p-1} - 1$

Cioé $a^{p-1} \equiv 1 \pmod p$ #

<u>Prop:</u> Sia p un primo positivo, e siano $a, b \in \mathbb{Z}$. Allora

$$(a+b)^p \equiv a^p + b^p \pmod p$$

(no dim)

Esercizio 5 foglio 6: $\mathbb{Z}_9$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{0}$
$\overline{2}$	$\overline{2}$		$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$								
$\overline{4}$	$\overline{4}$								
$\overline{5}$	$\overline{5}$								
$\overline{6}$	$\overline{6}$								
$\overline{7}$	$\overline{7}$								
$\overline{8}$	$\overline{8}$								

$+$ é commutativo $\Longrightarrow$ la tavola é simmetrica rispetto alla diagonale

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{3}$			$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{0}$	$\overline{3}$	$\overline{6}$
$\overline{4}$				$\overline{7}$	$\overline{2}$	$\overline{6}$	$\overline{1}$	$\overline{5}$
$\overline{5}$					$\overline{7}$	$\overline{3}$	$\overline{8}$	$\overline{4}$
$\overline{6}$						$\overline{0}$	$\overline{6}$	$\overline{3}$
$\overline{7}$							$\overline{4}$	$\overline{2}$
$\overline{8}$								$\overline{1}$

$\mathbb{Z}_n^* = \{\bar{a} \mid MCD(a,n)=1\}$

A^* = tutti gli elem. invertibili

$\mathbb{Z}_9^* = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$

- calcolare l'ordine
- $\mathbb{Z}_9^* \overset{?}{\cong} \underbrace{(\mathbb{Z}_6,+)}_{6}, \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_3}_{6}, \underbrace{D_3}_{6}, \underbrace{A_3}_{3}$

$|\mathbb{Z}_9^*| = 6$

OSS: • poiché $|\mathbb{Z}_9^*| = 6 \neq 3 = |A_3|$ sicuramente $\mathbb{Z}_9^* \not\cong A_3$.

- D_3 non è commutativo, quindi $\mathbb{Z}_9^* \not\cong D_3$.
- per il teo. cinese dei resti, siccome $MCD(2,3)=1$, $\mathbb{Z}_6 \xrightarrow{\sim} \mathbb{Z}_2 \times \mathbb{Z}_3$ quindi o entrambi $\mathbb{Z}_6$ e $\mathbb{Z}_2 \times \mathbb{Z}_3$ sono iso a $\mathbb{Z}_9^*$, o nessuno dei 2.

$\mathbb{Z}_9^* = \{\overset{1}{\bar{1}}, \overset{6}{\bar{2}}, \overset{3}{\bar{4}}, \overset{6}{\bar{5}}, \overset{3}{\bar{7}}, \overset{2}{\bar{8}}\}$

$ord(\bar{x}) \mid |\mathbb{Z}_9^*| = 6$

$ord(\bar{x}) = \min n$ t.c. $\bar{x}^n = \bar{1}$

- $ord(\bar{1}) = 1$
- $ord(\bar{8}) = 2$ perché $\bar{8} \cdot \bar{8} = \bar{1}$

- $ord(\overline{2}) = 6$ (perché $\overline{2}^6 = \overline{1}$)
- $ord(\overline{4}) = 3$
- $ord(\overline{5}) = 6 = ord(\overline{2})$ perché $\overline{5} = \overline{2}^{-1}$
- $ord(\overline{7}) = 3$

$$(\mathbb{Z}_6, +) = \{ \overset{1}{\overline{\overline{0}}}, \overset{6}{\overline{\overline{1}}}, \overset{3}{\overline{\overline{2}}}, \overset{2}{\overline{\overline{3}}}, \overset{3}{\overline{\overline{4}}}, \overset{6}{\overline{\overline{5}}} \}$$

$ord(\overline{\overline{x}}) = \min n$ t.c. $n\overline{\overline{x}} = \overline{\overline{0}}$

$ord(\overline{\overline{2}}) = ? = 3$ perché $3 \cdot \overline{\overline{2}} = \overline{\overline{0}}$

$$\mathbb{Z}_9^* = \{ \overset{1}{\overline{1}}, \overset{6}{\overline{2}}, \overset{3}{\overline{4}}, \overset{6}{\overline{5}}, \overset{3}{\overline{7}}, \overset{2}{\overline{8}} \}$$

$$(\mathbb{Z}_6, +) = \{ \overset{1}{\overline{\overline{0}}}, \overset{6}{\overline{\overline{1}}}, \overset{3}{\overline{\overline{2}}}, \overset{2}{\overline{\overline{3}}}, \overset{3}{\overline{\overline{4}}}, \overset{6}{\overline{\overline{5}}} \}$$

$\varphi : \mathbb{Z}_9^* \longrightarrow \mathbb{Z}_6$ verificare che é un iso

$$\begin{aligned}
\overline{1} &\longmapsto \overline{\overline{0}} \\
\overline{2} &\longmapsto \overline{\overline{1}} \\
\overline{4} &\longmapsto \overline{\overline{2}} \\
\overline{5} &\longmapsto \overline{\overline{5}} \\
\overline{7} &\longmapsto \overline{\overline{2}} \\
\overline{8} &\longmapsto \overline{\overline{3}}
\end{aligned}$$

Esercizio 10 foglio 6:

$$G = \mathbb{Z}_6 \times \mathbb{Z}_5$$
$$H = \mathbb{Z}_3 \times \mathbb{Z}_{10}$$

(a) $\exists$ iso di gruppi additivi $G \cong H$?

(b) $\exists$ iso di gruppi moltiplicativi $G^* \cong H^*$?

$$\mathbb{Z}_{30} \cong \mathbb{Z}_6 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$
$$\mathbb{Z}_{30} \cong \mathbb{Z}_3 \times \mathbb{Z}_{10} \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_5$$

$$G^* = \mathbb{Z}_6^* \times \mathbb{Z}_5^*$$

A, B $\quad A \times B$

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$
$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2)$$

$$(A \times B)^* = A^* \times B^*$$

$$\mathbb{Z}_6^* = \{\bar{1}, \bar{5}\}$$
$$\mathbb{Z}_5^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

$$\mathbb{Z}_3^* = \{\bar{1}, \bar{2}\}$$
$$\mathbb{Z}_{10}^* = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$$

Esercizio 11 foglio 6:

stesse domande per

$\boxed{G = \mathbb{Z}_6 \times \mathbb{Z}_3 \not\cong \mathbb{Z}_{18}}$ qui non ci sono elt. di ordine 18

$H = \mathbb{Z}_2 \times \mathbb{Z}_9 \cong \mathbb{Z}_{18}$

$(\bar{1}, \bar{1})$ ha ordine $= \text{mcm}(\underbrace{\text{ord}(\bar{1})}_{\text{come elt. in } \mathbb{Z}_2}, \underbrace{\text{ord}(\bar{1})}_{\text{come elt. in } \mathbb{Z}_9})$

$= \text{mcm}(2,9) = 18$

$|G^*| = |\mathbb{Z}_6^* \times \mathbb{Z}_3^*| = 4$

$|H^*| = |\mathbb{Z}_2^* \times \mathbb{Z}_9^*| = 6$

sicuramente $G^* \not\cong H^*$

Esercizio 12 foglio 6:

$\text{Aut}(\mathbb{Z})$

$\text{Aut}(\mathbb{Z}_4)$

$\text{Aut}(\mathbb{Z}_5)$

$\text{Aut}(G) =$ automorfismi di G, cioè gli iso: $G \longrightarrow G$

$\text{Aut}(A) =$ automorfismi di A

$=$ automorfismi del gruppo additivo $(A, +)$ che rispettano il prodotto

OSS: un isomorfismo di gruppi ciclici deve mandare generatori in generatori.

$\mathrm{Aut}(\mathbb{Z})$?

$\mathbb{Z}$ gruppo ciclico $= \langle 1 \rangle = \langle -1 \rangle$

$\rightsquigarrow$ gli unici automorfismi sono:

$$\begin{aligned} id: \mathbb{Z} &\to \mathbb{Z} \\ 1 &\mapsto 1 \\ n &\mapsto n \end{aligned} \qquad \begin{aligned} -id: \mathbb{Z} &\to \mathbb{Z} \\ 1 &\mapsto -1 \\ n &\mapsto -n \end{aligned}$$

$$\begin{aligned} \mathrm{Aut}(\mathbb{Z}) &\cong \mathbb{Z}_2 \\ id &\mapsto \overline{0} \\ -id &\mapsto \overline{1} \end{aligned}$$

Siccome $\mathbb{Z}_4 = \langle \overline{1} \rangle = \langle \overline{3} \rangle$ ha 2 generatori, possiamo ripetere esattamente gli stessi passaggi: $\mathrm{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$.

$\mathbb{Z}_5$ invece è generato da qualsiasi suo elemento $\neq \overline{0}$:

$$\mathbb{Z}_5 = \langle \overline{1} \rangle = \langle \overline{4} \rangle = \langle \overline{2} \rangle = \langle \overline{3} \rangle$$

$$\Longrightarrow \quad \begin{aligned} id &: \overline{1} \mapsto \overline{1} & \overline{n} &\mapsto \overline{n} \\ -id &: \overline{1} \mapsto -\overline{1} = \overline{4} & \overline{n} &\mapsto \overline{4n} \\ \varphi &: \overline{1} \mapsto \overline{2} & \overline{n} &\mapsto \overline{2n} \\ \psi &: \overline{1} \mapsto \overline{3} & \overline{n} &\mapsto \overline{3n} \end{aligned}$$

$$\mathrm{Aut}(\mathbb{Z}_5) = \{ \mathrm{id}, -\mathrm{id}, \varphi, \psi \}$$

$$\mathrm{Aut}(\mathbb{Z}_5) \begin{cases} \cong \mathbb{Z}_4 \ ? \\ \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \ ? \end{cases}$$

$$\mathrm{ord}(\varphi) = 4 \implies \mathrm{Aut}(\mathbb{Z}_5) \cong \mathbb{Z}_4$$