**Recap:** $a \equiv b \mod m \iff m \mid a-b$

"sono congruenti modulo m"

si comporta bene per somma, prodotto, differenza

MA NON per la divisione

Esempio $1 \equiv 4 \mod 3$ ✓

$2 \equiv 8 \mod 6$

$\frac{1}{2} \equiv \frac{4}{8} \mod 6$ ✗ $\quad 1 \equiv 4 \mod 6$

In generale dato $a \mod m$

esiste il suo INVERSO moltiplicativo

$a^{-1}$ t.c. $a \cdot a^{-1} \equiv 1 \mod m$

se e solo se $(a, m) = 1$

$\Leftarrow$ Teorema di Bezout: $a, m$ coprimi

$ax - 1 = km$ allora

$ax + km = 1$

$\Leftarrow$ Algoritmo di Euclide

Esempio Qual è l'inv. molt. di 7 mod 19?

| $7 \cdot k = 7$ | 14 | 21 | 28 | 35 | 42 | 49 | 56 |
|---|---|---|---|---|---|---|---|
| $7 \cdot k \bmod 19$ | -5 | 2 | 9 | -3 | 4 | 11 | 18 |

$7 \cdot (-8) = -56 \equiv 1 \mod 19$

- **Teorema Cinese del Resto**

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \end{cases} \quad \text{con } (m_1, m_2) = 1$$

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ x \equiv a_r \mod m_r \end{cases}$$

è equivalente a un'unica equazione $(M_i, M_j) = 1$

$$x \equiv a_3 \mod M_1 \cdot M_2$$

Esempio. Quali sono le ultime 2 cifre di $2^{30}$? 24

$2^{30} = ? \mod 100$, $100 = 2^2 \cdot 5^2$

$$\begin{cases} 2^{30} \equiv 0 \mod 2^2 = 4 \\ 2^{30} \equiv -1 \mod 5^2 = 25 \end{cases} \rightsquigarrow \begin{cases} x = 0 \mod 4 \\ x = -1 \mod 25 \end{cases}$$

$2^1\ 2^2\ 2^3$ ——

$2\ -1\ -2$ 1, $2\ -1\ -2\ 1$ mod 5

$2^1\ 2^2\ 2^3\ 2^4\ 2^5$

$2\ 4\ 8\ 16\ 7$ mod 25

$(2^5)^6 = 7^6 \equiv (7^2)^3 = (-1)^3 \equiv -1 \mod 25$

$7^1\ 7^2$

$-1$

## La funzione $\phi$ di Eulero

$$\phi(n) := \#\, \mathbb{Z}/n\mathbb{Z}^\times$$
$$= \#\{ i \mid 1 \le i \le n \text{ t.c. } (n,i) = 1 \}$$

$(\mathbb{Z}/n\mathbb{Z})^\times$ $\quad$ $(\mathbb{Z}/n\mathbb{Z})^\times$

$k < n$, $[p]$

$\phi(p) = p - 1$

$\phi(p^k) = p^{k-1}(p-1)$

$= p^k - \frac{p^k}{p} = p^k - p^{k-1}$

**Lemma** $\phi$ è **moltiplicativa**

$$\phi(ab) = \phi(a) \cdot \phi(b) \quad \text{per ogni } a, b \text{ coprimi}$$

Così possiamo calcolare la $\phi$ ( $n = \prod_{i=1}^{r} p_i^{e_i} \rightsquigarrow \phi(n) = \prod_{i=1}^{r} \phi(p_i^{e_i}) = \_\_\_$ )

$$\{1 \le i_1 \le ab \mid (a,i_1)=1\} = \{(i_2,i_1) \mid 1 \le i_1 \le a,\ 1 \le i_2 \le b \text{ con } (a,i_1)=1,\ (b,i_2)=1\}$$

per il TCR

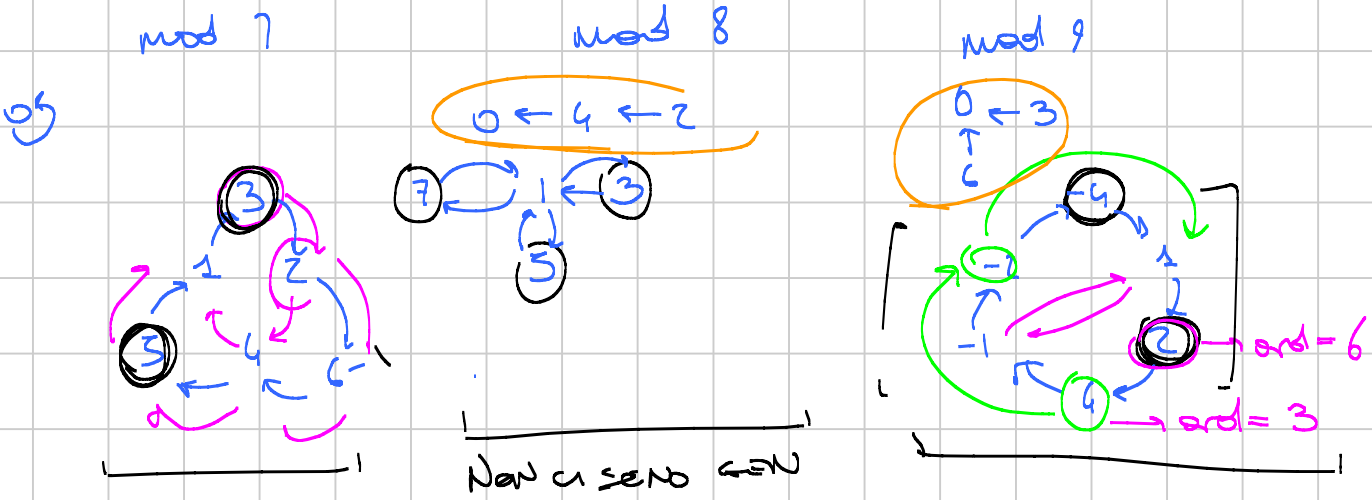
$$\phi(12) = \phi(4)\cdot\phi(3) = 2(2-1)\cdot(3-1) = 4$$

Fine recap

# Potenze mod m

Prendo a intero e guardo

$a^0, a^1, a^2, a^3, a^4, \dots \quad \text{mod } m$




1. Per il principio dei cassetti,

$a^0, a^1, a^2, \dots \pmod m$ è eventualmente periodica

$\exists i \neq j \geq 0$ t.c. $a^i \equiv a^j \text{ mod } m$

$\Rightarrow a^{i+1} \equiv a^{j+1} \text{ mod } m$

$\Rightarrow a^{i+2} \equiv a^{j+2} \text{ mod } m$

$\dots$ etc. $\dots$

2. Il termine $(i+1)$-esimo della successione dipende solo da quello $i$-esimo

3. Se $(a, m) = 1$, allora non c'è antiperiodo

Se so che $a^i \equiv a^j \text{ mod } m$

$\Rightarrow a^{i-1} \equiv a^{j-1} \text{ mod } m$

4. Teorema di Eulero-Fermat

Se $(a, m) = 1$, allora $a^{\varphi(m)} \equiv 1 \text{ mod } m$

Corollario Piccolo teorema di Fermat

$(a, p) = 1$ allora $a^{p-1} \equiv 1 \text{ mod } p$

Dim $(\mathbb{Z}/m\mathbb{Z})^\times = \{x_1, x_2, \dots, x_{\varphi(m)}\}$

$\| (*)$

$\{ax_1, ax_2, \dots, ax_{\varphi(m)}\} = (\mathbb{Z}/m\mathbb{Z})^\times$

- $(ax_i, m) = (x_i, m) = 1$ (perché $(a,m)=1$)
- Se $x_i \not\equiv x_j \bmod m$, allora $ax_i \not\equiv ax_j \bmod m$

$\Longrightarrow$ Vogliamo $*$

Quindi $x_1 \cdot x_2 \cdot \dots \cdot x_{\varphi(m)} \equiv ax_1 \cdot ax_2 \cdots ax_{\varphi(m)} \pmod m$

$\equiv a^{\varphi(m)} \cdot (\dots) \pmod m$

Divido per $x_1 \cdots x_{\varphi(m)}$ che ha un mod.

$a^{\varphi(m)} \equiv 1 \bmod m$ ∎

5. Corollario Se $(a,m)=1$, allora le potenze di $a \pmod m$ ci danno una succ. periodica senza subperiodo di periodo al più $\varphi(m)$.

Def Il periodo della successione, il più piccolo intero $k$ t.c. $a^k \equiv 1 \bmod m$ si chiama ORDINE MOLTIPLICATIVO e si indica con $\mathrm{ord}_m(a)$

6. Modulo $p$ primo ho che $\varphi(p) = p-1$

Eulero-Fermat: $a^{p-1} \equiv 1 \bmod p$ per $(a,p)=1$

$\varphi(x) = x^{p-1} - 1 = (x-1)(x-2)(x-3)\cdots(x-(p-1)) \bmod p$

coeff di $x^{p-2}$: $0 \equiv -(1+2+3+\dots+(p-1)) = p\frac{p-1}{2} \bmod p$

~~coeff di x~~

termine noto: $-1 \equiv 1 \cdot 2 \cdot \dots \cdot (p-1) \equiv (p-1)! \bmod p$

teorema di Wilson

**Def** $a$ si dice generatore mod $m$
se $\text{ord}_m(a) = \phi(m)$

**Fatto.** Esiste un gen. modulo $m$
se e solo se $m = 2, 4, p^k, 2p^k$.
con $p$ primo dispari

**Residui k-esimi modulo p**

Fatto $(\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ è biiettiva se e solo se
$x \longmapsto x^k$ $(k, \phi(p)) = 1$

[Se $k$ e $\phi(p)$ sono coprimi
allora $\exists h$ t.c. $kh \equiv 1 \bmod \phi(p)$ (Bezout)

$$(\mathbb{Z}/p\mathbb{Z}^\times) \xrightarrow{x^k} (\mathbb{Z}/p\mathbb{Z}^\times) \xrightarrow{x^h} (\mathbb{Z}/p\mathbb{Z}^\times)$$
$$x \longmapsto x^k \longmapsto (x^k)^h \equiv x^{kh}$$
$$\equiv x \bmod p$$
$$= (x^{p-1} \cdot x \equiv x \bmod p$$

(Esempio) Lepotenze ottave mod 4
chi è l'immagine di $x^3$ mod 4?

4 è primo $\exists g$ generatore t.c. $g^1, g^2, \dots g^{\phi(4)}$
sono tutti i resti mod 4 (non zero)

$$\{(g^1)^3, (g^2)^3, \dots, (g^{\phi(4)})^3\} = \{g^1, g^2, \dots g^{\phi(4)}\}$$

Se gli esp sono $\{1, 2, 3, \dots \phi(4)\}$
ora sono $\{1 \cdot 3, 2 \cdot 3, 3 \cdot 3, \dots 10 \cdot 3\}$ mod 10
$\|$

cioè $\{1, 2, 3, \dots, 10\}$

Se $(k, \phi(p)=p-1) \neq 1$, allora ci sono $\frac{\phi(p-1)}{(k, \phi(p))}$ residui k-esimi

[Brno 2014 P2] Trova tutte le sol. intere di

$$2014 = \frac{a^3+2b^3}{c^3+2d^3} \qquad (a,b,c,d \neq 0)$$

$$(c^3+2d^3)\,2014 = (a^3+2b^3)$$

$2014 = 2 \cdot 19 \cdot 53$

$\rightsquigarrow$ $0 \equiv a^3+2b^3 \mod 19$

$\rightsquigarrow$ $0 \equiv a^3+2b^3 \mod 53$

• modulo 2: $0 \equiv a^3 \Rightarrow a$ pari

$\rightsquigarrow$ $(a/b)^3 \equiv -2 \mod 19$ (* se $19 \nmid b$)

$b^{-1}$ è l'inv. mod di $b$ mod 19

$2b^{-1}$

Residui cubici: sono $\frac{18}{(3,18)} = 6$.

$\rightarrow$ $-2$ è un cubo modulo 19?

Se $(-2) = a^3$, allora $(-2)^6 \equiv a^{18} \equiv 1 \mod 19$

$4^3 \equiv 7 \not\equiv 1 \mod 19$

Quindi $-2$ non è un cubo!

Quindi $b$ è div. per 19 e quindi anche $a$

$a = 19a_1$, $b = 19b_1$

$$(c^3+2d^3)\cdot \frac{2014}{19} = \frac{19^3}{19}(a_1^3+2b_1^3) \qquad (2014 = 2\cdot 53 \cdot 19)$$

$$(c^3+2d^3)\cdot 2\cdot 53 \equiv 0 \mod 19$$

$\rightarrow$ come prima $19 \mid c,d$

$c = 19c_1$, $d = 19d_1$

$$19^4 \cdot 2 \cdot 53\,(c_1^3+2d_1^3) = 19^3 \cdot (a_1^3+2b_1^3)$$

Ripeto all'infinito... $\rightarrow$ $19^k \mid a,b,c,d \Rightarrow a=b=c=d=0$

assurdo per discesa infinita

$\Longrightarrow$ Non ci sono soluzioni

[CIME TST 2006] Trova tutti gli $(a,n)$ di interi positivi t.c.

$$\frac{(a+1)^n - a^n}{n} \text{ sia intero}$$

$\Longleftrightarrow$ $(a+1)^n = a^n \mod n$

se $n=1$, allora $(a,1)$ funziona

In gen. $2^2 = 4 \equiv 3^2 \mod 5$

$\Uparrow$

per il TCR $n = \prod p_i^{e_i}$

$\Downarrow$

$\begin{cases} (a+1)^n = a^n \mod p_i^{e_i} \end{cases} \Longrightarrow \begin{cases} (a+1)^n = a^n \mod p_i \end{cases}$

$a$

- $a, n$ sono coprimi, $\exists a^{-1} \mod n$ — $a+1$ e $n$ sono coprimi

$\Longleftrightarrow$ $(1+1/a)^n = 1 \mod n$ — $(1+1/a)^n \equiv 1 \mod p$

ci dice che $\operatorname{ord}_n(1+1/a) \mid n$ — $\operatorname{ord}_p(1+1/a) \mid n$

$\mid \phi(n)$ — $\mid \phi(p)$

$\operatorname{ord}_n(1+1/a) \mid (n, \phi(n))$ — $\operatorname{ord}_p(1+1/a) \mid (n, \phi(p) = p-1) = 1$

se $n$ fosse primo $\phi(n) = n-1$ e $(\ldots) = 1$

$(\prod p_i^{e_i}, \prod p_i^{e_i - 1}(p_i - 1))$ — $(\prod p_i^{e_i}, p_i - 1)$

Se $p$ è il più piccolo primo che divide $n$,

allora $(n, p-1) = 1$

$(\prod p_i^{e_i}, p_i - 1)$

$\Uparrow$ $p-1$ ha solo fattori primi più piccoli di $p$ e quindi di $n$

$$(1+1/2)^{\operatorname{ord}_p(1+1/2)} \equiv 1 \mod p$$

$$\| 1$$

$$(1+1/2)^1 \implies 0 \equiv 1/2 \mod p \quad \text{↯}$$

Assurdo!

$\implies$ Non ci sono soluzioni con $n \neq 1$.

3. Trovare tutti gli $n$ per cui $n \mid 2^{n-1}+1$

$\nu_2(5) = 0$

$\nu_2(10) = \nu_2(2 \cdot 5) = 1$

$2^{n-1} \equiv -1 \mod n$ usando TCR $\rightsquigarrow$ $2^{n-1} \equiv -1 \mod p$ per ogni $p \mid n$

$2^{2(n-1)} \equiv 1$

Quindi $\operatorname{ord}_p(2) \mid (2(n-1), p-1)$ dal p.t. di first

non è $n-1$ una qualsiasi cosa

$$\nu_2(n-1) + 1 = \nu_2(\operatorname{ord}_p(2)) \leq \nu_2(p-1)$$

l'esponente di 2

ASSURDO

$$\nu_2(n-1) = \min_{p \mid n} \{ \nu_2(p-1) \}$$ (esercizio)

$n = \prod p_i^{e_i}$ $\qquad$ $n-1 = \prod p_i^{e_i} - 1$

$p_i = 2^{e_i} \cdot d + 1 \implies \prod p_i \equiv 1 \mod 2^{e_i}$

1. Dato $x \in (0,1)$ reale, sia $y \in (0,1)$ il numero reale la cui $n$-esima cifra dopo la virgola coincide con la $2^n$-esima cifra dopo la virgola di $x$.
Dimostra che se $x$ è razionale, allora anche $y$ è razionale.

2. Siano $c \in \mathbb{Z}$ un intero e $p$ un primo. Dimostra che $x^x \equiv c \bmod p$ ha (almeno) una soluzione

3. Trova tutte le coppie di primi $p, q$ tali che $p \cdot q \mid 5^p + 5^q$

4. Sono dati numeri naturali $k \geq 2$ e $n_1, n_2, \dots, n_k$ tali che

$$n_2 \mid 2^{n_1} - 1, \quad n_3 \mid 2^{n_2} - 1, \quad \dots, \quad n_k \mid 2^{n_{k-1}} - 1, \quad n_1 \mid 2^{n_k} - 1.$$

Dimostra che $n_1 = n_2 = \dots = n_k = 1$.

5. Trova tutti gli interi positivi $n$ per cui esiste un intero $m$ per cui $2^n - 1 \mid m^2 + 9$.

6. Trova tutte le coppie di interi $(p, n)$ con $p$ primo e $n$ positivo per cui

$$\frac{n^p + 1}{p^n + 1} \in \mathbb{Z}$$

**1**

$x = 0.x_1 x_2 x_3 x_4 x_5 x_6 \dots \in \mathbb{Q}$

$y = 0.x_2 x_4 x_8 x_{16} \dots$

$x \in \mathbb{Q} \rightarrow$ la succ delle cifre $x_i$ è eventualmente periodica

$\exists k \; \exists i_0$ t.c. $\forall i \geq i_0 \quad x_{k+i} = x_i$

$\rightarrow \exists i_0$ t.c. $x_i = x_{i \bmod k}$ $\qquad x_i = x_j \Leftarrow i = j \bmod k$ e $i, j \geq i_0$

dipende solo dalla classe di $i \bmod k$

[la succ. $2^n$ è periodica modulo $k$: $\exists n_0$ t.c. $n_2 \geq n_0$ allora $2^n \equiv 2^{n+m} \bmod k$]

$x_{2^n}$ dipende solo, per $n$ sufficientemente grande ($n > \log_2(k)$), dalla classe di $2^n \bmod k$

$y_n = x_{2^n} = x_{2^n \bmod k} = x_{2^n + m \bmod k} = y_{n+m}$

↑ per simmetria

2. $x^x = c \mod p$

$\Leftarrow$ diretta $\quad \begin{cases} x \equiv 1 \mod \varphi(p) = p-1 \\ x \equiv c \mod p \end{cases}$ TCR: $\exists$ e tr...

$\rightsquigarrow x \equiv 2 \mod (p-1)$

$x^x = x^{k(p-1)+1} = (x^{p-1})^k \cdot x \equiv x \mod p$

$\in -F$

Il sistema ha soluzione per il TCR

che posso usare perché $(p, p-1) = 1$.

3. $p, q$ primi t.c. $pq \mid 5^p + 5^q$

Cosa succede se $p = 5$? $\quad q \mid 5^5 + 5^q$

$5^5 + 5 \equiv 0 \mod q$

$3130 = 2 \cdot 5 \cdot 313$

$q \leq 313$

$5, 2$

$5, 5$

$5, 313$

$10 \mid 5^5 + 5^2$ ✓

$25 \mid 5^5 + 5^5$ ✓

$5 \cdot 313 \mid$ —— ✓

Suppongo che $p \neq 5, q \neq 5$

$pq \nmid (5^{p-1} + 5^{q-1})$.

Quindi $5^{q-1} + 1 \equiv 0 \mod p$

$\longrightarrow 5^{q-1} \equiv -1 \mod p \longrightarrow 5^{2(q-1)} \equiv 1 \mod p$

Stare attenti a $p=2$

$\operatorname{ord}_p(5) \mid (p-1, \; 2(q-1))$

$\nmid q-1$

$v_2(q-1) + 1 = v_2(\operatorname{ord}_p(5)) \leq v_2(p-1)$

$\Longrightarrow v_2(q-1) < v_2(p-1)$

Ma il ragionamento simmetrico produce la dis. $v_2(p-1) < v_2(q-1)$

Quindi troviamo un contraddizione

4. Sono dati numeri naturali $k \geq 2$ e $n_1, n_2, \dots, n_k$ tali che

$$n_2 \mid 2^{n_1}-1, \quad n_3 \mid 2^{n_2}-1, \quad \dots, \quad n_k \mid 2^{n_{k-1}}-1, \quad n_1 \mid 2^{n_k}-1.$$

Dimostra che $n_1 = n_2 = \dots = n_k = 1$.

~~(1) (2) (3)~~

Se $a \mid b$, allora $2^a - 1 \mid 2^b - 1$.

$2^{b=(2^a)^k} = 1^k = 1 \mod (2^a - 1)$

Se $x = mcm(n_1, n_2, \dots n_k)$, allora $\boxed{x \mid 2^x - 1}$

perché $2^{n_i} - 1 \mid 2^x - 1$ per il fatto di sopra

e $n_i \mid 2^{n_i} - 1 \mid 2^x$ per ipotesi

$\Rightarrow$ Voglio risolvere $2^x \equiv 1 \mod x$

o anche $2^x \equiv 1 \mod p$ per $p \mid x$ primo

$\rightsquigarrow$ $\operatorname{ord}_p(2) \mid (p-1, x) = 1$

prendo $p$ il ppp che divide $x$

$\Rightarrow \operatorname{ord}_p(2) = 1$

$2^1 \equiv 1 \mod p$

$1 \equiv 0 \mod p$

ASSURDO

$\Rightarrow x = 1 \Rightarrow n_1 = n_2 = \dots = n_k = 1$