N1B - CONGRUENZE

Titolo nota 04/09/2023 Sam

Dato $m>0$ intero, $a \equiv b \mod m$ se $m \mid a-b$

Lo si comporta bene con somme, differenze, prodotti

In generale, se $a \equiv b \mod m$ e $c \mid (a,b)$

non è vero che $\frac{a}{c} \equiv \frac{b}{c} \mod m$

Es: $2 \equiv 12 \mod 10$ ma $1 \not\equiv 6 \mod 10$

- Se $(c,m)=1$, allora ok
- Se $(c,m)=d>1$, allora $\frac{a}{c} \equiv \frac{b}{c} \mod \frac{m}{d}$

Def: a si dice INVERSO MOLTIPLICATIVO di $b \mod m$ se

$$ab \equiv 1 \mod m$$

Fatto: b ha un inverso molt. mod $m \iff (b,m)=1$.

Teo di Bezout: Dati $b, m \in \mathbb{Z}$ esistono sempre $a, k \in \mathbb{Z}$ t.c.

$$ab + km = (b,m)$$

dim: algoritmo di Euclide per l'MCD. □

$\Rightarrow$ Pertanto $\mod m$ ho $ab \equiv (b,m) = 1 \mod m$.

Es: Inverso di 31 mod 1024

$(1024, 31) = (31, 1) = 1$

$1024 : 31 = 33$
94
1

$1024 = 31 \cdot 33 + 1$

$1024 - 31 \cdot 33 = 1 \Rightarrow$ l'inv. di $31 \bmod 1024$ è $-33 \equiv 991 \bmod 1024$

Es: Inverso di $55 \bmod 1024$

$(1024, 55) = (55, 34) = (34, 21) = (21, 13) = (13, 8) =$

$1024 : 55 = 18$ (474, 34) $\quad 55 : 34 = 1$ (21) $\quad 34 : 21 = 1$ (13) $\quad 21 : 13 = 1$ (8) $\quad 13 : 8 = 1$ (5)

$1024 = 55 \cdot 18 + 34 \quad 55 = 34 \cdot 1 + 21 \quad 34 = 21 \cdot 1 + 13 \quad 21 = 13 \cdot 1 + 8 \quad 13 = 8 \cdot 1 + 5$

$= (8, 5) = (5, 3) = (3, 2) = (2, 1) = 1$

$8 : 5 = 1$ (3) $\quad 5 : 3 = 1$ (2) $\quad 3 : 2 = 1$ (1)

$8 = 5 \cdot 1 + 3 \quad 5 = 3 \cdot 1 + 2 \quad 3 = 2 \cdot 1 + 1$

$1 = 3 - 2 \cdot 1 = 3 - (5 - 3 \cdot 1) = 2 \cdot 3 - 5 = 2(8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5 =$

$= 2 \cdot 8 - 3(13 - 8) = 5 \cdot 8 - 3 \cdot 13 = 5 \cdot (21 - 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13$

$= 5 \cdot 21 - 8 \cdot (34 - 21) = 13 \cdot 21 - 8 \cdot 34 = 13 \cdot (55 - 34) - 8 \cdot 34 =$

$= 13 \cdot 55 - 21 \cdot 34 = 13 \cdot 55 - 21 \cdot (1024 - 55 \cdot 18) =$

$= 391 \cdot 55 - 21 \cdot 1024$

$\Rightarrow$ l'inverso di $55 \bmod 1024$ è 391 (se non abbiamo sbagliato i conti)

Es: Inverso di $3 \bmod 8 = 3$

Inverso di $5 \bmod 17 = 7$

Es: Trovare tutti gli interi che sono coprimi con tutti i termini della successione

$$a_n = 2^n + 3^n + 6^n - 1 \qquad n \geq 1$$

In pratica voglio trovare i primi p t.c. $\exists n$ per cui $a_n \equiv 0 \mod p$

Oss: se $n = -1$, $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1 = 0$

p è primo, se $p \neq 2, 3$ $(p,2) = (p,3) = (p,6) = 1$.

$\Rightarrow$ 2, 3, 6 hanno un inverso mod p

e $2^{-1} + 3^{-1} + 6^{-1} \equiv 1 \mod p$

Inoltre le potenze mod p sono periodiche con periodo che divide $p-1$

$\Rightarrow$ $n = k(p-1) - 1$ allora $a_n \equiv 0 \mod p$ $\quad \forall p \neq 2,3$

$a_1 \equiv 0 \ (2)$ $\quad a_2 \equiv 0 \ (3)$ $\Rightarrow$ **1**.

TCR Se $(m_1, m_2) = 1$, allora il sistema

$$\begin{cases} x \equiv a_1 \ (m_1) \\ x \equiv a_2 \ (m_2) \end{cases}$$

è equivalente a un'unica congruenza modulo $m_1 \cdot m_2$

$$x \equiv a_3 \ (m_1 \cdot m_2)$$

Es: $2^{30} \mod 1000 \iff \begin{cases} 2^{30} \mod 2^3 \\ 2^{30} \mod 5^3 \end{cases}$

$$\begin{cases} x \equiv 0 \mod 2^3 \\ x \equiv 7h \mod 5^3 \end{cases} \qquad x = 7h + k \cdot 125 \quad \text{con } 125k + 7h \equiv 0 \ (8)$$

$5k \equiv -2 \pmod 8$ $\qquad 6 \cdot 125 + 74$

$k \equiv 10 \pmod 8$

$k \equiv -2 \pmod 8$

$k \equiv 6 \pmod 8$

φ di EULERO $\qquad \varphi : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$

$$\varphi(n) = \left| \{ i \mid 0 \le i < n \text{ e } (i,n) = 1 \} \right|$$

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

Lemma fondamentale (moltiplicatività di φ)

Se $(a,b) = 1$, allora $\varphi(ab) = \varphi(a) \cdot \varphi(b)$

dim $\quad (i, ab) = 1 \iff \begin{cases} (i,a) = 1 \\ (i,b) = 1 \end{cases}$

$$\{ i \mid (i,ab) = 1,\ 0 \le i \le ab-1 \} \longleftrightarrow \left\{ (i,j) \;\middle|\; \begin{matrix} 0 \le i < a & (i,a) = 1 \\ 0 \le j < b & (j,b) = 1 \end{matrix} \right\}$$

$\uparrow$ biiezione x il TCR $\qquad \|$

$$\{ i \mid 0 \le i < a,\ (i,a) = 1 \} \times \{ j \mid 0 \le j < b,\ (j,b) = 1 \}$$

$\Rightarrow \varphi(ab) = \varphi(a) \cdot \varphi(b)$

$p > 2$

Quante sol ha $x^2 - 2 \equiv 0 \pmod p$? 0 oppure 2

Quante sol ha $x^2 - 2 \equiv 0 \pmod{p \cdot q}$?

$$\begin{cases} x^2 \equiv 2 \mod p \\ x^2 \equiv 2 \mod q \end{cases} \to a, -a \quad b, -b$$

$$\begin{cases} x \equiv a \mod p \\ x \equiv b \mod q \end{cases} \quad \begin{cases} x \equiv -a \\ x \equiv b \end{cases} \quad \begin{cases} x \equiv a \\ x \equiv -b \end{cases} \quad \begin{cases} x \equiv -a \\ x \equiv -b \end{cases}$$

POTENZE MOD m

1) Per il principio dei cassetti prima o poi la successione delle potenze $a^0, a^1, a^2, a^3, \dots$ si ripete mod m

2) Il termine i-esimo dipende solo da quello $(i-1)$-esimo

$$a^i = a \cdot a^{i-1}$$

$\Rightarrow$ se $a^i \equiv a^j \mod m$ allora $a^{i+k} \equiv a^{j+k} \mod m$

Se $m = p^k$, $(a, p^k) \neq 1$ (cioè $p \mid a$) $\to$ nulla da un certo punto in poi

se $(a, p^k) = 1$ e $a^i \equiv a^j \mod p^k$ $\quad i > j$

$$a^{i-j} \equiv 1 \mod p^k \quad i - j > 0$$

$\Rightarrow$ non c'è antiperiodo

Thm (Eulero-Fermat): Se $(a, m) = 1$, allora $a^{\varphi(m)} \equiv 1 \ (m)$.

dim: $\{ j \mid 0 < j \leq m, (j, m) = 1 \} = \{ x_1, \dots, x_{\varphi(m)} \} = A$

$\{ ax_1, \dots, ax_{\varphi(m)} \} = B$

$ax_i \equiv ax_j \mod m \iff x_i \equiv x_j \mod m$

$(ax_j, m) = 1$ $\quad$ $(a, m) = 1$ $\iff i = j$

A e B hanno gli stessi elementi mod m

$\Rightarrow$ $x_1 \cdot \ldots \cdot x_{\varphi(m)} \equiv a x_1 \cdot \ldots \cdot a x_{\varphi(m)} \pmod m$

$x_1 \cdot \ldots \cdot x_{\varphi(m)} \equiv a^{\varphi(m)} x_1 \cdot \ldots \cdot x_{\varphi(m)} \pmod m$

$(a^{\varphi(m)} - 1)\, x_1 \cdot \ldots \cdot x_{\varphi(m)} \equiv 0 \pmod m$

$x_1 \cdot \ldots \cdot x_{\varphi(m)}$ coprimi con m $\Rightarrow$ li semplifico $\Rightarrow$ $a^{\varphi(m)} \equiv 1 \ (m)$. □

Cor: Se $(a, m) = 1$ le potenze di a mod m sono periodiche senza antiperiodo di periodo che divide $\varphi(m)$

Il periodo di a^k mod m è detto ORDINE MOLTIPLICATIVO di a mod m e si indica con $\mathrm{ord}_m(a)$

Oss: mod p si ha il Piccolo Teorema di Fermat: $a^{p-1} \equiv 1 \pmod p$ se $(a, p) = 1$

$q(x) = x^{p-1} - 1 \in \mathbb{Z}[x]$

E-F $\Rightarrow$ tutti i residui $1, \ldots, p-1$ sono radici di $q(x)$ mod p

$\Rightarrow q(x) \equiv (x-1)(x-2)\cdots(x-(p-1)) \pmod p$ ← coeff. per coeff.

$\downarrow$

$x^{p-1} - \left(p \frac{p-1}{2}\right) x^{p-2} + \ldots - 1$

$\equiv 0 \pmod p$

Cor: $-1 \equiv (-1)^{p-1} (p-1)!$ cioè $(p-1)! \equiv -1 \pmod p$ (Teo di WILSON)

segue valutando in $x = 0$ la congruenza tra polinomi.

$\sum_{j=1}^{p-1} j \equiv 0 \mod p$ $\quad \sum_{1\le i<j\le p-1} ij \equiv 0 \mod p$ $\quad$ (Coeff di x^{p-2} e x^{p-3})

$$\Rightarrow \sum_{j=1}^{p-1} j^2 \equiv 0 \mod p \qquad (p \ge 5)$$

Def: a si dice GENERATORE mod m se $\mathrm{ord}_m(a) = \varphi(m)$

cioè se le potenze di a mod m generano tutti i numeri coprimi con m.

Es: Se esiste un generatore mod m allora $\sum_{(j,m)=1} j^k \equiv 0 \mod m$

$\forall k < \varphi(m)$

Dim: Sia g generatore mod m $\Rightarrow (j,m)=1$ allora $j = g^a$

e se $a \not\equiv b \mod \varphi(m)$ allora $g^a \not\equiv g^b \mod m$

$g^{a-b} \not\equiv 1 \mod m$

$$\Rightarrow \sum_{(j,m)=1} j^k \equiv \sum_{a=0}^{\varphi(m)-1} (g^a)^k \equiv \sum_{a=0}^{\varphi(m)-1} (g^k)^a \equiv \frac{(g^k)^{\varphi(m)} - 1}{g^k - 1} \mod m$$

se $(g^k - 1, m) = 1$, ho finito perché $(g^k)^{\varphi(m)} \equiv 1 \mod m$ per E-F.

- se $m = p$, $g^k - 1 \equiv 0 \ (p)$

$\Downarrow$

$g^k \equiv 1 \ (p) \iff p-1 \mid k \Rightarrow p-1 \le k$ assurdo.

- mancano da fare i casi $m = p^k$, $m = 2p^k$

Quando esiste un generatore?

mod m se $m = 2$, $m = 4$, $m = p^k$, $m = 2p^k$ (p primo dispari, p " ")

Potenze mod m - II

$\mathbb{Z}/m\mathbb{Z}^*$ = le classi di resto mod m coprime con m

$f : \mathbb{Z}/m\mathbb{Z}^* \longrightarrow \mathbb{Z}/m\mathbb{Z}^*$ $\quad f(x) = x^k$ (intesa mod m)

se $k=1$ è l'identità

se $k = \varphi(m)$ è la funzione costante 1

I caso: se $(k, \varphi(m)) = 1$, allora $\exists h$ t.c. $hk \equiv 1 \ (\varphi(m))$

$\Rightarrow$ $x \xmapsto{f} x^k$ $\quad g(x) = x^h$

$$g(f(x)) = (x^k)^h = x^{kh} = x^{\alpha\varphi(m)+1} = x \cdot \underbrace{(x^{\varphi(m)})^\alpha}_{\equiv 1 \text{ E-F}} \equiv x \bmod m$$

Es: Quanti sono i cubi mod 11?

Poiché $(3, \varphi(11)) = (3,10) = 1$, $x \to x^3$ è biiettiva mod 11

Tra le classi di resto coprime con 11

$\Rightarrow$ Tutti gli elementi sono cubi.

II° caso: $k \mid \varphi(m)$

se ho un generatore g

$$g^0, g^1, \dots, g^{\varphi(m)-1}$$

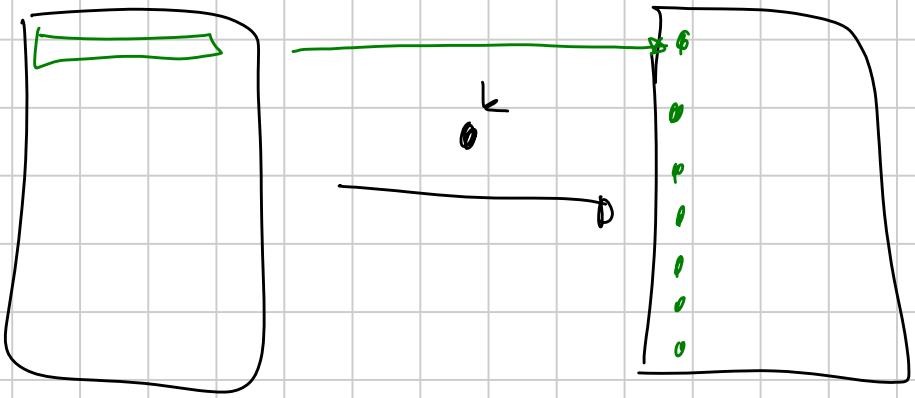
$$g^0, g^k, \dots, g^{k(\varphi(m)-1)}$$

se $\varphi(m) = k \cdot d$ allora $(g^d)^k = g^{\varphi(m)} \equiv 1 \mod m$

$\Rightarrow$ l'immagine di f contiene $d = \frac{\varphi(m)}{k}$ elementi.

e le controimmagini di 1 sono $(g^d)^i$ $i = 0, \dots, k-1$

che sono esattamente k.



Es: Se elevo al cubo mod 13, avrò $\frac{12}{3} = 4$ immagini ognuna data da 3 elementi diversi in partenza

2 è un generatore mod 13 $(2^6 \equiv -1 \mod 13)$

$2^4 \equiv 3 \mod 13 \Rightarrow 1, 3, 9$ elevati al cubo fanno 1 mod 13

2 è radice cubica di 8 mod 13
ma anche $2 \cdot 3$ e $2 \cdot 9$

Def: Le immagini di f si dicono RESIDUI k-ESIMI mod m

Es N2-10 $D = \{n > 1 : n \mid 2^n + 1\}$

Mostrare che tutti gli elementi di D sono divisibili per 3

Sol: $2^n + 1 \equiv 0 \mod n \to 2^n \equiv -1 \mod n$

$\to 2^{2n} \equiv 1 \mod n$ $\quad \text{ord}_n 2 \mid 2n$ $\quad (\text{e } \text{ord}_n 2 \nmid n)$

$\text{ord}_n 2 \mid \varphi(n)$

Se $\text{ord}_n 2 = 2$, allora $2^2 \equiv 1 \mod n$, cioè $n \mid 3$

Altrimenti sia p il più piccolo primo che divide n

$\Rightarrow 2^n \equiv -1 \mod p$, $2^{2n} \equiv 1 \mod p$

$\to \text{ord}_p(2) \mid 2n$ $\quad \text{ord}_p(2) \mid p-1$

$\Rightarrow \text{ord}_p(2) \mid (2n, p-1) =$ i fattori di $p-1$ sono $< p$

$= (2, p-1) = 2$ $\quad \Rightarrow$ non possono dividere n.

$\Rightarrow 2^2 \equiv 1 \ (p) \Rightarrow p \mid 3 \Rightarrow p = 3$

ESERCIZI

da PARTE 1: 42, 45, 48, 49, 52, 61, 62, 63, 66

da PARTE2 N1: 3, 6, 8, 10

da PARTE2 N2: 1, 6, 10

BIMO 2014/2: $2014 = \dfrac{a^3 + 2b^3}{c^3 + 2d^3}$ ← risolvere con $a, b, c, d \in \mathbb{Z}$.

Parte 1

42, 45, 48, 49, 52, 61, 62, 63, 66

42 mod 7 i cubi sono ± 1 e 0. $\Rightarrow$ impossibile

45 $\longrightarrow$ ok

48 per quali a $x^2 \equiv a \ (11)$ ha almeno 1 sol

$x^3 \equiv 2a \mod 14 \qquad \varphi(14) = 6$

$x^2 + x - a \equiv 0 \ (7)$

$\Delta = 1 + 4a$ se questo è un quadrato, le sol sono

$$x = \frac{-1 \pm \sqrt{\Delta}}{2}$$

49 $\rightarrow$ mod 3 e mod 8

52

$n^k \equiv 02 \ (100)$ $\qquad n^k = 2^k m^k \Rightarrow n^k \equiv 0 \ (4)$

$\Downarrow$ $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \Downarrow$

$n \equiv 0 \ (2) \qquad n = 2m \qquad\qquad\qquad$ impossibile

61 mod 3 $5^n + 1 \equiv 0$ se n è dispari $\Rightarrow$ n pari se A primo

mod 5 $3^n + 1 \equiv 0$ se $n \equiv 2 \ (4) \Rightarrow n \equiv 0 \ (4)$ se A primo

mod 7 $\Rightarrow n \equiv 0 \ (3)$ se A primo

62 $p_1 \dots p_{2013}$ primi

$$\begin{cases} x \equiv 0 & (p_1^5) \\ x+1 \equiv 0 & (p_2^5) \\ \vdots \\ x+2012 \equiv 0 & (p_{2013}^5) \end{cases}$$

ha sol per il TCR

63 $\{2^k \bmod 100\}$ $\{2^k \bmod 1000\}$ $\{7^k \bmod 100\}$

mod 4 1 2 0 0

$k=0$ 1 2

mod 25 $\varphi(25)=20 \Rightarrow 2^{20}\equiv 1 \ (25)$

$\Rightarrow ord_{25}(2)=20$

(7^k è più facile) $2^{10}=1024\equiv -1 \ (25)$

66 — nei primi riduco l'esp mod $\varphi(n)$

e uso $\sum_{j=1}^{p-1} j^k \equiv 0 \ (p)$ se $k \le p-2$

$44^{55^{666^{777}}} \bmod 23$

$ord_{23}(44) \mid \varphi(23)=22$ $\quad 44 = 2^{22} \equiv 1 \ (23)$

$\Rightarrow ord_{23}(44)=11$

$\Rightarrow 44^{\cdots} \equiv 44^0 \equiv 1 \bmod 23$

Io PARTE2 N1: 3, 6, 8, 10

Io PARTE2 N2: 1, 6, 10

BIMO 2014/2: $2014 = \frac{a^3+2b^3}{c^3+2d^3}$ ← risolvere con $a,b,c,d \in \mathbb{Z}$.

N1-3 facile

N1-6 $p^4 - p^4 \equiv 0 \bmod 5 \ \forall p,q$

$p^4 - q^4 \equiv 0 \bmod 3 \ \forall p,q$

$p^2 - p^2 \equiv 0 \bmod 8$ e $p^2+q^2 \equiv 0 \ (2)$

$\Rightarrow (p^2+q^2)(p^2-q^2) \equiv 0 \quad (16)$

$\Rightarrow 2^4 \cdot 3 \cdot 5 \mid MCD(\dots)$

$p=13 \quad q=11 \qquad p^4-q^4 = 2 \cdot 24 \cdot 29 \cdot 10 = 2^5 \cdot 3 \cdot 5 \cdot 29$

$p=29 \quad q=11 \Rightarrow 29 \nmid p^4-q^4$

$p=17 \quad q=13 \Rightarrow 2^4 \parallel p^4-q^4 \Rightarrow 2^4 \cdot 3 \cdot 5$

8) $MCD(100+n^2, 100+(n+1)^2) = MCD(100+n^2, 2n+1)$

10) $y^2 = x^5 - 4 \mod 11 \quad x^5 \equiv \begin{cases} 0 \\ -1 \\ 1 \end{cases}$ ma $-4, -3, -5$ non sono res quad mod 11.

BNO: $2014 = \dfrac{a^3+2b^3}{c^3+2d^3}$ $\qquad 2014 = 2 \cdot 19 \cdot 53$

$a^3+2b^3 \equiv 0 \quad (19) \qquad$ se $b \not\equiv 0 \quad (19)$

allora $-2 \equiv \left(\frac{a}{b}\right)^3 \quad (19)$

ma -2 non è un cubo mod 19

$\Rightarrow b \equiv 0 \quad (19) \Rightarrow a \equiv 0 \quad (19) \rightarrow$ discesa infinita