SENIOR 2016 – N2 BASIC

Note Title 9/5/2016

INVERSO MOLTIPLICATIVO mod m

a mod m $\qquad ax \equiv 1 \ (m)$?

$x =$ "inverso di a mod m"

a ammette inverso mod $m \iff (a,m) = 1$; inoltre, se $(a,m) = 1$ c'è esattamente un inverso definito mod m.

Es: $m = 9$

$m-1 \equiv -1$

$a =$	0	1	2	3	4	5	6	7	8
$a^{-1} =$	×	1	5	×	7	2	×	4	8

Oss $d = (a, m)$. (Se $d > 1$), allora $d \mid ax$ per ogni x

$\Rightarrow ax \not\equiv 1 \ (m)$

$4x \equiv 1 \ (9)$ $\qquad 4x = \begin{cases} 1 \\ 1+9 = 10 \\ 1+9\cdot 2 = 19 \\ 1+9\cdot 3 = 28 \end{cases}$

$2x \equiv 1 \ (9)$ $\qquad 2x = 1$ NO, $2x = 1+9$ Sì $\rightarrow x = 5$

$(a,m) = 1 \implies$ c'è esattamente un inverso di a mod m

$ax \equiv 1 \ (m)$

$\iff ax = km + 1$

$\iff ax - km = 1$

↗ Algoritmo di Euclide

ha soluzioni $\iff (a,m) = 1$

inoltre $\boxed{x = x_0 + t \cdot m}$ Con tutte le soluzioni

Es Calcolare le ultime 4 cifre in base 8 di

$$\frac{2^{2016}-1}{3}.$$

$$\frac{2^{2016}-1}{3} \equiv \frac{0-1}{3} \quad (8^4)$$

$$\left(2^{2016}-1\right)\cdot 3^{-1} \equiv -3^{-1} \quad (8^4)$$

$8^4 \not\equiv 1 \pmod 3$ $\qquad \left(\frac{2\cdot 8^4+1}{3}\right)$

Es Ultima cifra di $\frac{2^{2016}-1}{3}$ in base 3 ?

$$\frac{2^{2016}-1}{3} \not\equiv \frac{1-1}{3} \not\equiv \frac{0}{3} \pmod 3$$

Ridurre mod 9 il numeratore

$$\text{numeratore} \equiv 6 \ (9) \qquad \text{num} = 6+9k$$

$$\frac{\text{num}}{3} = 2+3k$$

2^{2016}

$2^0 = 1$
$2^1 = 2$
$2^2 = 4$
$2^3 = 8 \equiv -1 \ (9)$
$2^4 = 16 \equiv 7 \ (9)$
$2^5 \equiv 5 \ (9)$
$2^6 \equiv 1 \ (9)$
$2^7 \equiv 1\cdot 2 \equiv 2 \ (9)$

$2^8 \equiv 4$
$2^9 \equiv 8$
$\vdots$

$$2^{2016} \equiv 2^0 \equiv 1 \ (9)$$

$$2^{2016} - 1 \equiv 0 \ (9)$$

$$\Rightarrow \frac{2^{2016}-1}{3} \equiv 0 \ (3)$$

Quando si può dividere a destra e a sinistra in una congruenza?

$\underbrace{8^{-1}}_{1} \cdot 8x \equiv \underbrace{24 \cdot 8^{-1}}_{3 \cdot 8 \cdot 8^{-1} \equiv 3} \ (31) \quad \overset{?}{\Longrightarrow} \quad x \equiv 3 \ (31)$ Sì

$8x \equiv 24 \ (32) \quad \overset{?}{\Longleftarrow} \quad x \equiv 3 \ (32)$ NO

$8 \quad 8 \quad (32,8)$

$8x = 24 + 32k$
$\Leftrightarrow \quad x = 3 + 4k$
$\Leftrightarrow \quad x \equiv 3 \ (4)$

$8x \equiv 24 \ (18)$
$8 \quad 8 \quad 2 = (8,18)$

$\Longleftrightarrow \quad 8x = 24 + 18k$
$4x = 12 + 9k$
$4x \equiv 12 \ (9)$
$4 \quad 4$
$x \equiv 3 \ (9)$

TEOREMA CINESE DEL RESTO

$$\begin{cases} x \equiv 1 \ (3) \\ x \equiv 2 \ (4) \end{cases}$$

$x = 10$ va bene.

$x = 10 + 12k$ va bene

$x \equiv 10 \ (12)$

$$\begin{cases} x = 1 + 3k \\ x = 2 + 4h \end{cases}$$

$$1 + 3k = 2 + 4h$$

$$\Rightarrow \quad 3k - 4h = 1$$

ci sono soluzioni.

$$\begin{cases} k = k_0 + 4t \\ h = h_0 + 3t \end{cases}$$

$$\begin{cases} x = 1 + 3k = 1 + 3(k_0 + 4t) = (1 + 3k_0) + 12t \\ x = 2 + 4h = 2 + 4(h_0 + 3t) = (2 + 4h_0) + 12t \end{cases}$$

$$x \equiv (?) \ (12)$$

Teorema $\circledast$ $\begin{cases} x \equiv a_1 \ (m_1) \\ x \equiv a_2 \ (m_2) \end{cases}$ con $(m_1, m_2) = 1$

Esiste b (unico mod $m_1 m_2$) tale che il sistema $\circledast$ è equivalente a $\boxed{x \equiv b \ (m_1 m_2)}$

$$\begin{cases} x \equiv 8 \ (9) \\ x \equiv 1 \ (16) \\ x \equiv -1 \ (6) \end{cases} \iff \begin{cases} x \equiv -1 \ (3) \\ x \equiv -1 \ (2) \end{cases}$$

$$x \equiv -1 \ (12) \iff \begin{cases} x \equiv -1 \ (2^2) \\ x \equiv -1 \ (3) \end{cases}$$

$$\begin{cases} x \equiv 8 \ (9) \\ x \equiv 1 \ (16) \end{cases} \iff \boxed{x \equiv 17 \ (9 \cdot 16)}$$

ATTENZIONE:

$x \equiv -1 \ (12) \iff$ ~~$x \equiv -1 \ (2)$~~ ~~$x \equiv -1 \ (2)$~~ ~~$x \equiv -1 \ (3)$~~

→
- Scomporre ogni congruenza in potenze di primi
- Confrontare le congruenze relative agli stessi primi

Es: $\begin{cases} x \equiv 9 \ (27) \\ x \equiv 80 \ (81) \end{cases} \Rightarrow x \equiv 80 \ (27)$

→
- Ricostruire la soluzione modulo $\prod_i p_i^{k_i}$

1, (17), 33, ...

$$\begin{cases} x \equiv ? & (\text{mcm dei moduli}) \\ \text{non c'è soluzione} \end{cases}$$

PERIODICITÀ DELLE POTENZE mod m

Es: potenze di 3 mod 20

$3^0 \equiv 1$
$3^1 \equiv 3$
$3^2 \equiv 9$
$3^3 \equiv 7$
$3^4 \equiv 7 \cdot 3 \equiv 1$

3
9
7
⋮

$(3, 20) = 1$

Es: potenze di 2 mod 20

$2^0 \equiv 1$
$2^1 \equiv 2$
$2^2 \equiv 4$
$2^3 \equiv 8$
$2^4 \equiv 16$
$2^5 \equiv 32 \equiv 12$
$2^6 \equiv 24 \equiv 4$

8
16
12
4
8
16
12
⋮

$2^k \bmod 20 \iff 2^k \bmod 4$ e $\bmod 5$

$(2, 5)$

$(2, 20) > 1$

Antiperiodo + Periodo.
$(a, m) = 1$

$(a, m) = 1$; vogliamo studiare le potenze di $a \bmod m$.

Fatto 1 Non c'è antiperiodo
Ovvero la prima potenza "già vista" è un $1 \bmod m$

$a^0, a^1, a^2, a^3, \dots, a^k, \dots, a^h$

$a^k \equiv a^h \pmod m$ $\quad h > k \geq 0$

$\Rightarrow 1 \equiv a^{h-k} \pmod m$

a^0

$k = 0$ era il vero "primo momento" di ripetizione.

La prima ripetizione è un 1.

Def ordine moltiplicativo di a mod m

$\text{ord}_m(a) =$ minimo $h>0$ tale che $a^h \equiv 1 \ (m)$

Ovvero: è il <u>periodo</u> delle potenze di a

Es: $\text{ord}_{20}(3) = 4$

Fatto 2 $a^k \equiv 1 \ (m) \iff \text{ord}_m(a) \mid k$.

PICCOLO TEOREMA DI FERMAT

$m = p$ primo

$a^p \equiv a \ (p)$ per ogni a

ovvero: $a^{p-1} \equiv 1 \ (p)$ per ogni a non multiplo di p.

Dim $S = \{1, 2, 3, \dots, p-1\}$ $\quad (p \nmid a)$

$\downarrow \cdot a$

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

Esempio: $p = 7$, $a = 2$

$\{1, 2, 3, 4, 5, 6\}$

$\downarrow$

$\{2, 4, 6, 1, 3, 5\}$

$i, j \in \{1, \dots, p-1\} = S$

$i \neq j \Rightarrow ai \not\equiv aj \ (p)$

perché, se per assurdo $ai \equiv aj \ (p)$, allora dividendo per a trovo $i \equiv j \ (p)$

Prodotto degli elementi di S: $(p-1)!$ / $(p-1)! \cdot a^{p-1}$

$(p-1)! \equiv (p-1)! \cdot a^{p-1} \ (p)$

$\Rightarrow a^{p-1} \equiv 1 \ (p)$. $\square$

$a^{p-1} \equiv 1 \ (p)$ se $p \nmid a$.

$\rightarrow$ $\boxed{\text{ord}_p(a) \mid p-1}$

Esempi $p = 11$

a^0	a^1	a^2	a^3	a^4	a^5	
1	5	3	4	9	1	
1	10	1				

- $a = 5$
- $a = 10 \equiv -1$
- $a = 2$
- $a = 1$

$\text{ord}_{11}(5) = 5 \mid p-1 = 10$

$\text{ord}_{11}(10) = 2$

$\text{ord}_{11}(2) = 10$

$\text{ord}_{11}(1) = 1$

Esempio Dimostrare che, se $p \mid x^2+x+1$, allora $p=3$ oppure $p \equiv 1 \ (3)$.

$x^2+x+1 \equiv 0 \ (p)$

$\downarrow \cdot (x-1)$

$x^3 - 1 \equiv 0 \ (p)$

$x^3 \equiv 1 \ (p) \Rightarrow \boxed{\text{ord}_p(x) \mid 3}$

$\text{ord}_p(x) = 1 \Rightarrow x \equiv 1 \ (p) \Rightarrow 1+1+1 \equiv 0 \ (p) \Rightarrow p = 3$

$\text{ord}_p(x) = 3 \Rightarrow 3 \mid p-1$

$\Rightarrow p \equiv 1 \ (3)$.

Esercizio: Come possono essere fatti i fattori primi di x^2+1?

Es (N2-10) $n \mid 2^n+1 \Rightarrow 3 \mid n$ $(n \geq 1)$

$$2^n \equiv -1 \quad (n)$$

Sia p un fattore primo che divide n.

$$n = p \cdot m$$

$$n \mid 2^n + 1 \quad \Rightarrow \quad p \mid 2^n + 1$$

$$2^n \equiv -1 \quad (p)$$

$$2^{pm} \equiv -1 \quad (p)$$

$$\mid 2^m \equiv -1 \quad (p) \mid \qquad 2^{pm} \equiv (2^m)^p \equiv 2^m \quad (p)$$

elevando al quadrato: $2^{2m} \equiv 1 \quad (p)$

$\Rightarrow \cdot \ ord_p(2) \mid 2m$

ci ricordiamo che $\cdot \ ord_p(2) \mid p-1$

Prendiamo come p il più piccolo primo che divide n $(p \geq 3)$

$$ord_p(2) \mid (2m, p-1) \mid 2$$

$$\Rightarrow ord_p(2) = \begin{cases} 1 \Rightarrow 2 \equiv 1 \ (p) \text{ assurdo} \\ 2 \Rightarrow 2^2 \equiv 1 \ (p) \end{cases}$$

ovvero $3 \equiv 0 \ (p) \Rightarrow p = 3.$

TEOREMA DI EULERO

$$(a, m) = 1 \quad \Rightarrow \quad \boxed{a^{\varphi(m)} \equiv 1 \quad (m)}$$

$\varphi(m) =$ # elementi di $\{1, \dots, m\}$ coprimi con m.

Es: $m = p$ primo, $\varphi(p) = p-1$

$$a^{p-1} \equiv 1 \ (p)$$

Dim: è come quella del LFT.

$S = \{1, \dots, p-1\} \longrightarrow S = \{$ elementi coprimi con m tra 1 e $m\}$

$\downarrow \cdot a$

$\{a, 2a, \dots\}$

$|S| = \varphi(m)$

$\downarrow \cdot a$

S

$a^{\varphi(m)} \equiv 1 \pmod m$

$(a,m) = 1 \Rightarrow \boxed{\text{ord}_m(a) \mid \varphi(m)}$

GENERATORI

$\text{ord}_p(a) \mid p-1$

modulo p

Domanda: qualsiasi divisore di $p-1$ è l'ordine moltiplicativo di qualcosa?

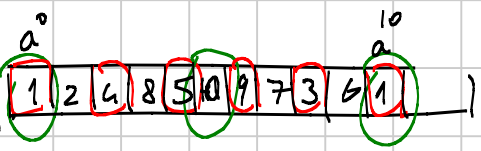
Se c'è un g tale che $\text{ord}_p(g) = p-1$, allora $\forall\, d \mid p-1$

$g^{\left(\frac{p-1}{d}\right)}$ ha proprio ordine d.

$p = 11$

$a = 2$

$\text{ord}_{11}(2) = 10$



$d = 5$

$g^{\frac{p-1}{d}} = 2^{\frac{10}{5}} = 2^2$

$d = 2$

$g^{\frac{p-1}{2}} = 2^{\frac{11-1}{2}} = 2^5$

Teorema Esiste sempre (mod p) almeno un elemento g di ordine $p-1$.

↗ GENERATORE mod p.

g è un generatore $\iff \{g^0, g^1, g^2, \dots, g^{p-2}\} = \{1, 2, \dots, p-1\}$

mod p

Es Tutti i primi $\equiv 1 \ (3)$ dividono qualche x^2+x+1.

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

$\operatorname{ord}_p(x) = \begin{cases} 1 \to p=3 \\ 3 \to 3 \mid p-1 \end{cases}$

Vogliamo costruire x con $\operatorname{ord}_p(x)=3$.

Esiste!

$$x \equiv g^{\frac{p-1}{3}} \ (p)$$

$$x^2+x+1 \equiv \frac{x^3-1}{x-1} \equiv \frac{g^{\frac{p-1}{3}\cdot 3}-1}{x-1} \equiv \frac{g^{p-1}-1}{x-1} \equiv 0 \ (p)$$

posso scriverlo se $x \not\equiv 1 \ (p)$

$$g^{\frac{p-1}{3}} \not\equiv 1 \ (p)$$

QUANTE SONO LE POTENZE K-ESIME mod p ?

$x^2 = y^5+4$

quadrati mod 11 : 5 più lo 0

potenze quinte mod 11 : 2 (± 1) più lo 0

Fatto generale: ci sono $\frac{p-1}{(k, p-1)}$ potenze k-esime mod p (più lo 0).

$\{1^k, 2^k, 3^k, \dots, (p-1)^k\}$ ← quanti elementi diversi ha?

$\| $

$\{(g^0)^k, (g^1)^k, (g^2)^k, \dots, (g^{p-2})^k\}$ per qualche generatore g

$= \{g^0, g^k, g^{2k}, g^{3k}, \dots, g^{(p-2)k}\}$

Sono le potenze di $g^k \mod p$.

Il numero di potenze k-esime è uguale a $\mathrm{ord}_p(g^k)$.

$$\mathrm{ord}_p(g^k) \mid p-1$$

$k = p-1 \longrightarrow \mathrm{ord}_p(g^k) = 1$

$k = \frac{p-1}{2} \longrightarrow = 2$

$d \mid p-1 \qquad k = \frac{p-1}{d} \longrightarrow = d$

Se $k \mid p-1$, allora $\mathrm{ord}_p(g^k) = \frac{p-1}{k}$

$\Rightarrow$ ci sono $\frac{p-1}{k}$ potenze k-esime.

Idea: guardare $\{g^0, g^k, g^{2k}, \dots, g^{(p-2)k}\} \mod p$

è un po' come guardare $\{0, k, 2k, \dots, (p-2)k\} \mod p-1$.

$d = (k, p-1)$

$k = h \cdot d$

$\{0, hd, 2hd, 3hd, \dots, (p-2)hd\} \mod p-1$

$\Updownarrow$ divido per d

$\{0, h, 2h, 3h, \dots, (p-2)h\} \mod \frac{p-1}{d}$

$\left(h, \frac{p-1}{d}\right) = 1$

$\{0, h, 2h, \dots, \left(\frac{p-1}{d} - 1\right)h\}$

sono tutti diversi

$\frac{p-1}{d}$ elementi distinti

$= \left| \frac{p-1}{(k, p-1)} \right|$

Esercizi "base": 46, 47, 51, 54, 60, 61, 66.

Esercizi dalla pagina N2: 4, 6, 9.

Esercizio extra: primi che dividono x^2+1.

(54) $3^y - x^2 = 41$ mod 8

3^y ↑ x^2 ↑

$3 + \begin{matrix}0\\4\end{matrix} \equiv 1$

$3 + 0 \equiv 3$

$3 + 4 \equiv 7$

$1 + 0 \equiv 1$

$1 + 4 \equiv 5$

$\Rightarrow$ y pari, x è multiplo di 4.

Se y pari: $z^2 - x^2 = 41$ $(z = 3^{y/2})$ ↑

$y = 0$ a parte

(60) $A = 5^n + 3^n + 1$ primo $\overset{?}{\Rightarrow}$ $12 \mid n$? $(n \geq 1)$

- n pari ?

$n=1$ $A=9$

$n=3$ $A=\dots$

mod 3: $A \equiv (-1)^n + 1 \equiv 0$ (3)

↑ n dispari

- $4 \mid n$?

$n \equiv 2$ (4)

$n=2 \rightarrow A = 25 + 1 + 1 = 35$

mod 5: $A \equiv 3^n + 1 \equiv 4 + 1 \equiv 0$ (5)

3, 4, 2, 1, ...

- $3 \mid n$?

mod 7 $7-1=6$ è multiplo di 3

n	0	1	2	3	4	5	
5^n	1,	5,	4,	−1,	2,	3,	1
3^n	1,	3,	2,	−1,	4,	5,	1

	3	2	0	-1	0	2
1						

non va bene $n \equiv 2, 4 \ (6)$

$\Rightarrow \boxed{n \equiv 0 \ (6)}$

mod 9

ord $|$ $\varphi(m)$

$\varphi(9) = 6$ ...

(66) $x^3 \equiv 2a \mod 14 \qquad 0 \le a \le 100$

Per quali a esiste una soluzione?

$\begin{cases} x^3 \equiv 2a \ (2) \iff x \equiv 0 \ (2) \\ x^3 \equiv 2a \ (7) \end{cases}$ per avere soluzioni, serve che $2a$ sia un cubo perfetto mod 7.

Quanti sono i cubi mod 7?

$\frac{7-1}{3} = 2$ $\qquad 0, 1, -1$

$2a \equiv 0, 1, -1 \ (7)$

$a \equiv 0, 4, 3 \ (7)$

(4) $5^{5^{5^5}} \mod 10^5$

$\mod 5^5 \longrightarrow \equiv 0$

$\mod 2^5$

$5^{5^{5^5}} \mod 2^5$ ⊗

riduco l'esponente mod $\varphi(2^5) = 2^4$

$5^{5^5} \mod 2^4$

riduco l'esponente mod $\varphi(2^4) = 2^3$ ✳

$5^{5^5} \bmod 8 \equiv 5 \ (8)$

(*) $5^{5^{5^5}} \bmod 2^4 \equiv 5^5 \bmod 2^4$

$\equiv 5 \bmod 2^4$

5
9
-3
$-15 \equiv 1$

(*) $5^{5^{5^{5^5}}} \bmod 2^5 \equiv 5^5 \bmod 2^5$

$\equiv 21 \bmod 32$

$$\begin{cases} x \equiv 0 \ (5^5) \\ x \equiv 21 \ (2^5) \end{cases}$$

$x = 5^5 k$ $\qquad$ ~~$5^5 k \equiv 21 \ (2^5)$~~

$5^5 \equiv 1 \ (2^5)$

$k \equiv 1 \ (2^5)$

$x \equiv 5^5 \cdot 1 = 3125 \ (10^5)$

$\boxed{03125}$

(6) $2^n \equiv 18 \ (385)$

$$\begin{cases} 2^n \equiv 18 \equiv 3 \ (5) \\ 2^n \equiv 18 \equiv 4 \ (7) \\ 2^n \equiv 18 \equiv 7 \ (11) \end{cases} \longrightarrow \begin{cases} n \equiv 3 \ (4) \\ n \equiv 2 \ (3) \\ n \equiv 7 \ (10) \end{cases}$$

$n \equiv \boxed{7} \ (20)$

$$\begin{cases} n \equiv 7 \ (20) \\ n \equiv 2 \ (3) \end{cases}$$

$7, \ 7+20, \ 7+20 \cdot 2$

$n \equiv 7 + 20 \cdot 2 \equiv 47 \ (60).$

(9) d, m, n

$$\begin{cases} a & \equiv 0 \quad (p_1^n) \\ a+d & \equiv 0 \quad (p_2^n) \\ a+2d & \equiv 0 \quad (p_3^n) \\ a+3d & \vdots \\ \vdots & \\ a+(m-1)d & \equiv 0 \quad (p_m^n) \end{cases}$$

$p_1, p_2, \dots, p_m$ primi distinti

$\Rightarrow \exists$ soluzioni!

EXTRA $\quad x^2+1 \leftarrow$ fattori primi?

$p \mid x^2+1 \implies p = 2$ oppure $p \equiv 1 \ (4)$

$x^2 \equiv -1 \quad (p)$

$x^4 \equiv 1 \quad (p)$

$\Rightarrow \operatorname{ord}_p(x) \mid 4$

$\operatorname{ord}_p(x) = \begin{cases} 1 \longrightarrow x \equiv 1 \ (p) \Rightarrow x^2+1 \equiv 2 \\ \qquad\qquad 2 \equiv 0 \ (p) \Rightarrow p = 2 \\ 2 \\ 4 \longrightarrow x^2 \equiv 1 \ (p) \Rightarrow x^2+1 \equiv 2 \\ \qquad\qquad \equiv 0 \Rightarrow p = 2 \end{cases}$

$\Downarrow$

$4 \mid p-1$

ovvero $p \equiv 1 \ (4)$.

$\operatorname{ord}_p(x) = 4$

$x = g^{\frac{p-1}{4}}$ per qualche generatore g.

$x^2 + 1 \equiv g^{\frac{p-1}{2}} + 1 \equiv 0 \quad (p)$

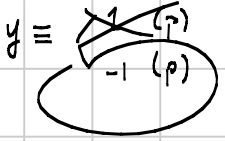
$g^{\frac{p-1}{2}} \equiv -1$

$g^{\frac{p-1}{2}} = y$

$y^2 \equiv g^{\frac{p-1}{2} \cdot 2} = g^{p-1} \equiv 1 \ (p)$

$y^2 \equiv 1 \ (p)$

$p \mid y^2 - 1 = (y+1)(y-1)$

$y \equiv$ 

$g^{\frac{p-1}{2}} \equiv -1 \quad \Rightarrow \quad x^2+1 \equiv 0 \ (p).$