SENIOR 2015 – N2 BASIC

Titolo nota 25/08/2015

- TEOREMA CINESE DEL RESTO

Es: . $\begin{cases} x \equiv 2 \ (5) \\ x \equiv 3 \ (6) \end{cases}$ $\quad x = 2 + 5k$ $\quad x = 3 + 6h$

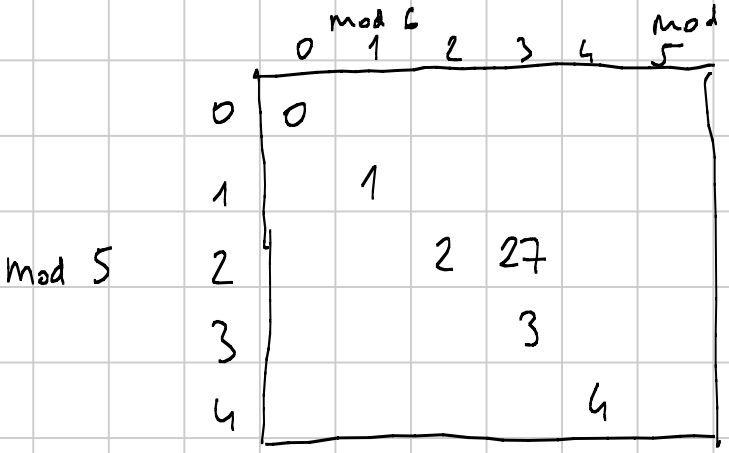
$2 + 5k = 3 + 6h$

$5k - 6h = 1$ $\quad k = -1 + 6t$ $\quad h = -1 + 5t$

$x = 2 + 5k = 2 + 5(-1 + 6t) = -3 + 30t$

$x \equiv -3 \ (30)$

$\begin{cases} x \equiv a \ (5) \\ x \equiv b \ (6) \end{cases}$ $\quad \begin{matrix} 0 \le a \le 4 \\ 0 \le b \le 5 \end{matrix}$ } soluzioni: tutte tra 0 e 29



Teorema $\quad \begin{cases} x \equiv a_1 \ (m_1) \\ x \equiv a_2 \ (m_2) \\ \vdots \\ x \equiv a_n \ (m_n) \end{cases}$ $\quad (m_i, m_j) = 1$ per ogni $i \neq j$

Allora c'è esattamente una soluzione mod $m_1 m_2 \dots m_n$.

Detto in un altro modo: $\begin{cases} \cdot \\ \cdot \\ \cdot \end{cases} \iff x \equiv b \ (m_1 m_2 \dots m_n)$

Esempio

$$\begin{cases} A & x \equiv 33 \ (40) & 2^3 \cdot 5 \\ B & x \equiv 38 \ (45) & 3^2 \cdot 5 \\ C & x \equiv 13 \ (50) & 2 \cdot 5^2 \end{cases}$$

$$\begin{cases} x \equiv 3 \ (4) \\ x \equiv 8 \ (16) \end{cases}$$

$$A \begin{cases} x \equiv 33 \ (8) \leftarrow & x \equiv 1 \ (8) \\ x \equiv 33 \ (5) \leftarrow & x \equiv 3 \ (5) \end{cases}$$

$$B \begin{cases} x \equiv 2 \ (9) \\ x \equiv 3 \ (5) \end{cases}$$

$$C \begin{cases} x \equiv 1 \ (2) \\ x \equiv 13 \ (25) \end{cases}$$

$\rightarrow x \equiv 1 \ (8) \iff x \equiv 1 \ (8)$
$\rightarrow x \equiv 1 \ (2)$

$1 \quad (8)$
$1 \ 3 \ 5 \ 7 \ (8)$

$$\begin{cases} x \equiv 1 \ (8) \\ x \equiv 2 \ (9) \\ x \equiv 13 \ (25) \end{cases} \Big] \ x \equiv a \ (72)$$

$$\begin{cases} x \equiv 3^2 \ (5) \\ x \equiv 3 \ (5) \\ x \equiv 13 \ (25) \end{cases} \quad x \equiv 13 \ (25)$$

$$x \equiv b \ (2^3 \cdot 3^2 \cdot 5^2)$$

- INVERSO MOLTIPLICATIVO

$(a, m) = 1$ $\quad a$ ha esattamente un inverso moltiplicativo modulo m

$ab \equiv 1 \pmod n$

- lo indichiamo con a^{-1} $\quad 1/a$
- si trova con l'alg. di Euclide

Esempio $\quad \frac{2}{3}\left(4^{1003}-1\right) \pmod{11}$

4
$4^2 \equiv 5$
$4^3 \equiv 20 \equiv 9$
$4^4 \equiv 3$
$4^5 \equiv 1$

$$2\left(4^{1003}-1\right) \equiv 2\left(4^3-1\right)$$
$$\equiv 2(9-1) \equiv 5 \pmod{11}$$

$$\frac{2}{3}\left(4^{1003}-1\right) \equiv \frac{5}{3} \pmod{11} \equiv 5 \cdot 3^{-1} \pmod{11}$$

$$\frac{2}{3}\left(4^{1000}-1\right) \pmod{11}$$

mod 11

$$\equiv 2 \cdot 4 \left(4^{1000}-1\right) \pmod{11}$$

$4^{1000} \pmod{11^2}$

$$\equiv 2\left(4^{1003}-1\right) \cdot 3^{-1}$$

$3^{-1} \equiv 4 \pmod{11}$ $\quad$ perché $3 \cdot 4 = 12 \equiv 1 \pmod{11}$

$3^{-1} \equiv 9 \pmod{13}$ $\quad$ 14, $27/3 = 9$

- STRUTTURA MOLTIPLICATIVA mod p (primo)

- Tutte le classi di congruenza $\neq 0$ hanno un inverso
- ordine di un elemento (o ordine moltiplicativo)

$a \not\equiv 0 \pmod p$

$a, a^2, a^3, \ldots \quad a^k \equiv 1 \pmod p$

$\operatorname{ord}_p(a)$ = il minimo $k > 0$ tale che $a^k \equiv 1 \pmod p$

Oss: $\left(a^{-1}\right)$ = inverso di a

$$(a^{-1})^4 \cdot a^5 \equiv a \ (p)$$

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

$$a \cdot \underbrace{a^{k-1}}_{\text{è l'inverso!}} \equiv a^k \equiv 1 \ (p)$$

$$a^{3k+5} \equiv a^5 \ (p) \quad \text{se} \quad k = \text{ord}_p(a)$$

- Piccolo teorema di Fermat

$$\boxed{a^p \equiv a \ (p)} \qquad \text{per ogni } a, \ p \text{ primo}$$

Se $a \not\equiv 0 \ (p)$

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

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

Con la congruenza quando vuoi dividere, moltiplica per l'inverso!

- Esiste un $k > 0$ t.c. $a^k \equiv 1 \ (p)$
- $\text{ord}_p(a) \leq p-1$
- $\boxed{\text{ord}_p(a) \mid p-1}$

$p = 7$

$a, a^2, a^3, \underbrace{a^4 \equiv 1 \ (7)}, a^5, \underbrace{a^6 = 1}$

$$a^{6-4} \equiv a^6 \cdot a^{-4} \equiv 1 \cdot (a^4)^{-1} \equiv 1 \cdot 1^{-1} \equiv 1$$

$\text{ord}_p(a) = k \nmid p-1$

$p-1 = k \cdot h + r$ ← resto della div. per k, $0 < r < k$

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

$$a^k \equiv 1 \ (p)$$

$$\rightarrow a^{(p-1)-kh} \equiv a^{p-1} \cdot \left((a^k)^h\right)^{-1} \equiv 1 \cdot (1^h)^{-1} \equiv 1$$

$0 < r < k$ ASSURDO

a^r

- $k = ord_p(a)$

  $\rightarrow a^n \equiv 1 \ (p)$ se e solo se $k \mid n$

$a \not\equiv 0 \ (p)$

$a^0, a^1, a^2, \ldots, a^k, a^{k+1}, \ldots$

$\|1 \quad\quad\quad\quad\quad\quad\quad\quad \|1$

$1 \quad\quad\quad\quad\quad\quad\quad\quad 1$

PERIODO k

$1 \quad\quad\quad\quad\quad\quad\quad\quad 1$

- in un periodo ci sono solo classi di congruenza diverse

$$a^m \equiv a^n \quad m > n$$

$$a^{m-n} \equiv 1 \ (p) \quad \text{NO}$$

Esempio $p = 5$

		a^0	a^1	a^2	a^3	a^4		$ord_5(a)$
$a \equiv 1 \ (5)$		1	1	1	1	1	...	1
$\rightarrow a \equiv 2 \ (5)$		1	2	4	3	1	...	4
$\rightarrow a \equiv 3 \ (5)$		1	3	4	2	1	...	4
$a \equiv 4 \ (5)$		1	4	1	4	1	...	2

$ord_p(a) \mid p-1 = 4$

1 primo t. di F.

- Cosa succede se $ord_p(a) = p-1$?

  il periodo contiene tutti i numeri da 1 a $p-1$ in qualche ordine

a si dice <u>generatore</u> mod p

Se g è un generatore mod p

$g^0, g^1, g^2, \dots, g^{p-2}$ sono tutte le classi di congruenza $\not\equiv 0$

Qualsiasi classe di congruenza mod p $\not\equiv 0$ si può esprimere come potenza di un generatore.

- STRUTTURA MOLTIPLICATIVA mod m ($\Leftrightarrow (a,m)=1$ c'è l'inverso)
  - $\mathrm{ord}_m(a)$ $\quad (a,m)=1$

$$a, a^2, a^3, \dots, a^k \equiv 1$$

Se $(a,m) \neq 1$ non posso ottenere 1 come potenza di a !

$p \mid (a,m)$

$p \mid a^k$ per ogni k

$a^k \not\equiv 1 \ (m)$ $\qquad$ $a^k \equiv 1 \ (m)$

$\Downarrow$

$0 \equiv a^k \equiv 1 \ (p)$

- Teorema di Eulero-Fermat

$$a^{\varphi(m)} \equiv 1 \ (m) \quad \text{se} \quad (a,m)=1$$

$\varphi(m)$ = il numero di elementi dell'insieme $\{1, 2, \dots, m-1\}$ coprimi con m

"funzione di Eulero"

Es: $\varphi(12) = 4$ $\qquad$ $\{1, 5, 7, 11\}$

Esempio $m = 12$

	a^0	a^1	a^2	a^3	a^4	$\mathrm{ord}_m(a)$
$a \equiv 1$	1	(1)	1	1	1	1
$a \equiv 5$	1	5	(1)	5	1	2
$a \equiv 7$	1	7	(1)	7	1	2
$a \equiv 11 \equiv -1$	1	−1	(1)	−1	1	2

↑ Tco E.F.

- $\boxed{\mathrm{ord}_m(a) \mid \varphi(m)}$ Dimostrazione: uguale al caso $m = ?$ primo
- $m = p$ primo $\quad \varphi(p) = p - 1$

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

∴ Non c'è un generatore!

Teorema

DOMANDA: Quando c'è un generatore?

RISPOSTA:
- $m = 2$
- $m = 4$
- $m = p^n$ $\quad p$ primo dispari
- $m = 2p^n$ $\quad$ "

Dimostrazione del t. di Eulero - Fermat

$(a, m) = 1$ $\qquad$ TESI: $a^{\varphi(m)} \equiv 1 \ (m)$

$b_1, b_2, \dots, b_{\varphi(m)}$ le classi di congruenza coprime con m

$ab_1, ab_2, \dots, ab_{\varphi(m)}$

Es: $m = 12$

$1, 5, 7, 11$

$a = 7$ ↓

$7, 11, 1, 5$

OSS: la riga sotto è una permutazione di quella sopra

$$ab_i \equiv ab_j \pmod m$$
$$\Downarrow$$
$$b_i \equiv b_j \pmod m$$

Quindi le classi di cong. della riga sotto sono tutte diverse

$b_1 b_2 \cdots b_{\varphi(m)}$

$ab_1\, ab_2 \cdots ab_{\varphi(m)} \equiv a^{\varphi(m)} b_1 b_2 \cdots b_{\varphi(m)} \pmod m$

$$\cancel{b_1 b_2 \cdots b_{\varphi(m)}} \equiv a^{\varphi(m)} \cancel{b_1 b_2 \cdots b_{\varphi(m)}} \pmod m$$
$$1 \equiv a^{\varphi(m)} \pmod m$$

□

- φ DI EULERO
  - $\varphi(p) = p-1$ se p è primo
  - $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$

$\{1, 2, 3, \dots, p^k\}$ ← ce ne sono p^k

tolgo quelli multipli di p

$p, 2p, 3p, \dots, p^{k-1}\cdot p$ ← ce ne sono p^{k-1}

  - $\varphi(m)$ P.I.E.

T.C.R.

Lemma $\varphi(mn) = \varphi(m)\cdot\varphi(n)$ se $(m,n)=1$

"φ è moltiplicativa"

$S = \{0, 1, 2, 3, \dots, mn-1\}$

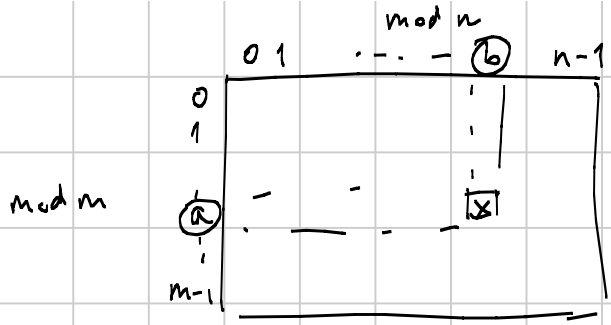
$S_1 = \{0, 1, \dots, m-1\}$ $S_2 = \{0, 1, \dots, n-1\}$

S^* = elem di S coprimi con mn

S_1^* = elementi di S_1 coprimi con m

S_2^* = " " S_2

coprimi con n



$$\begin{cases} x \equiv a \ (m) \\ x \equiv b \ (n) \end{cases}$$

S // $x \in S$

x è coprimo con mn ?

deve essere coprimo con m
e coprimo con n

$x \equiv a \ (m)$ $\quad a \in S_1^*$

$x \equiv b \ (n)$ $\quad b \in S_2^*$

$x \in S^* \Rightarrow a \in S_1^*$ e $b \in S_2^*$

$\Leftarrow$

Dim Per assurdo. Se $x \notin S^*$

$(x, mn) \neq 1$

$\Rightarrow (x,m) \neq 1$ oppure $(x,n) \neq 1$

wLog $(x,m) \neq 1$

$x \equiv a(m)$ $\quad a \notin S_1^*$

$x \in S^* \Leftarrow a \in S_1^*$ e $b \in S_2^*$ Assurdo

$$|S^*| = |S_1^*| \cdot |S_2^*|$$

$$\varphi(mn) = \varphi(m) \cdot \varphi(n)$$

□

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

$$m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \Rightarrow \varphi(m) = \varphi(p_1^{a_1})\,\varphi(p_2^{a_2}\cdots p_r^{a_r}) =$$

$$= \varphi(p_1^{a_1})\,\varphi(p_2^{a_2}) \cdots \varphi(p_r^{a_r})$$

$$= p_1^{a_1-1}(p_1-1)\cdot p_2^{a_2-1}(p_2-1)\cdots$$

- RESIDUI QUADRATICI, RESIDUI k-ESIMI, POTENZE...

mod p Quali sono le classi di congruenza che si possono ottenere da un quadrato perfetto?

Es: $p=3$ $x^2 \equiv_{(3)} \begin{matrix} 0 \\ 1 \end{matrix}$

x	x^2
0	0
1	1
2	1

$p=5$

x	x^2
0	0
1	1
2	4
3	4
4	1

In generale: mod p ci sono $\frac{p-1}{2}$ residui quadratici $\neq 0$

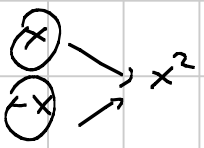
$(p \neq 2)$

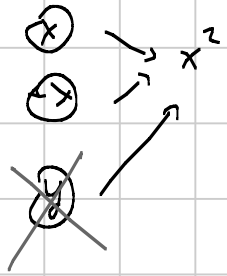
$$x \overset{f}{\longmapsto} x^2$$

$f(x) \equiv f(-x)$ $(-x)^2 \equiv x^2$

$0 \longrightarrow 0$

$x \not\equiv 0 \qquad x \not\equiv -x \ (p)$





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

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

$p \mid x-y \qquad y \equiv x \ (p)$

oppure $p \mid x+y \qquad y \equiv -x \ (p)$

I quadrati sono $\frac{p-1}{2}$ più lo 0.

mod p (Come sono fatte le potenze?)

Quante sono le potenze n-esime?

$0 = 0^n$

Sia g un generatore mod p

mod p $\{1, 2, 3, \dots, p-1\} = \{g^0, g^1, g^2, \dots, g^{p-2}\}$

I generatori trasformano problemi moltiplicativi in problemi additivi.

elevo alla n

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

$\frac{p-1}{(n, p-1)}$

- $g^{kn} \equiv g^{hn} \ (p)$?

$\cdot g^{-hn}$

$g^{kn-hn} \equiv 1 \ (p)$

$g^{(k-h)n} \equiv 1 \ (p)$

$\text{ord}_p(g) \mid (k-h)n$

$\|$

$p-1$

$p-1 \mid (k-h)n$

$\iff \quad \frac{p-1}{(n, p-1)} \mid k-h$

$\iff \quad k \equiv h \quad \left(\frac{p-1}{(n,p-1)}\right)$

Ci sono $\left|\frac{p-1}{(n,p-1)}\right|$ potenze n-esime mod p

$\| \quad \text{ord}_p(g^n) \longrightarrow g^0, g^n, g^{2n}, g^{3n}, \dots, g^{kn}, \dots$

$\|$

1

Es: $n=2$, p dispari $\quad \frac{p-1}{(2,p-1)} = \frac{p-1}{2}$

Es: $y^2 = x^5 - 4$

0

1

-1

$\frac{p-1}{(n,p-1)}$ $\quad (n, p-1)$ è grande

vogliamo che $p-1$ abbia tanti fattori in comune con gli esponenti

mod 11 ci sono $5+1$ quadrati:

ci sono $2+1$ potenze quinte $\rightarrow 0, 1, -1$

mod 7 quante potenze quinte? Tutte

$(5, 7-1) = 1$

Ci sono $\frac{\varphi(p^k)}{(n, \varphi(p^k))}$ potenze n-esime coprime con p^k

$n = p^k$ p dispari

ESERCIZI pag 11 49, 51, 53, 54, 66

pag 40 7, 9, (10)

CORREZIONE

I generatori mod m (quando esistono) generano le classi di cong. coprime con m.

m = 4 1, 5, 7, 11

(49) $n^2+5n+16 = 169\,y$

$n^2+5n+16 \equiv 0 \quad (13^2)$

$n^2+5n+16 \equiv 0 \quad (13)$

$x^2+5x+16=0$ x numero reale complesso

$$x = \frac{-5 \pm \sqrt{5^2-16\cdot 4}}{2}$$

$$\left(x+\frac{5}{2}\right)^2 + 16 - \frac{25}{4} = 0$$

$$x+\frac{5}{2} = \pm\sqrt{\frac{25}{4}-16}$$

$n^2+5n+16 \equiv 0 \quad (13)$

$n^2+5n+3 \equiv 0 \quad (13)$

$$n^2+5n+3 \equiv \left(n+\frac{5}{2}\right)^2 + 3 - \frac{25}{4} \equiv \frac{1}{4}\left((2n+5)^2+0\right) \equiv \frac{1}{4}(2n+5)^2$$

$$\equiv 10\,(2n+5)^2$$

14
27
40

$10(2n+5)^2 \equiv 0 \ (13)$

$2n+5 \equiv 0 \ (13)$

$n \equiv -5/2 \equiv -5 \cdot 7 \equiv 4 \ (13)$

$n \equiv 4 \ (13)$

$n^2+5n+3 \equiv n^2-8n+16 = (n-4)^2$

$n = 13k+4$

$0 \equiv n^2+5n+16 = (13k+4)^2 + 5(13k+4) + 16 \equiv$

$\equiv 13 \cdot 4 \cdot 2k + 16 + 5 \cdot 13k + 20 + 16$

$\equiv 13(8k+5k) + 52$

$\equiv 13^2k + 52 \ (13^2)$

WHAT IF...

$13k + 52 \equiv 0 \ (13^2)$

$13^2 \mid 13k+52$

$13 \mid k+4$

$k \equiv -4 \ (13)$

$k = -4+13h$

$n = 13(-4+13h)+4$

$n \equiv -4 \cdot 13 + 4 \ (13^2)$

51) $x^2 \equiv 2 \ (100)$

$\Downarrow \quad 4 \mid 100$

$x^2 \equiv 2 \ (4)$ $\quad [x^2 \equiv 0,1 \ (4)]$

$n^k \equiv 2 \ (4)$ NO

53) $x^2+3y = 2$

$y = \frac{2-x^2}{3}$ $\quad \boxed{x^2 \equiv 2 \ (3)}$ $\quad [x^2 \equiv 0,1 \ (3)]$

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

mod 4 $\quad (-1)^y - x^2 \equiv 1 \quad (4)$

$(-1)^y$: 1 → -1 ; 0 → 1

- x è pari
- $(-1)^y \equiv 1 \ (4)$ cioè y è pari

$y = 2z$

$3^{2z} - x^2 = 41$

$(3^z + x)(3^z - x) = 41$

$41 = 1 \cdot 41$

$3^z = \frac{a+b}{2}$ NO

(66) (a) $a^x \equiv 1 \ (10)$ Sono 4 (10): 1, 3, 7, 9

(b) $x^2 \equiv a \ (19)$ Quanti? $\frac{p+1}{2} = 10$

(c) • $x^3 \equiv 2a \ (21)$

TCR $\Leftrightarrow$ $\begin{cases} x^3 \equiv 2a \ (3) \\ x^3 \equiv 2a \ (7) \end{cases}$

$x^3 \equiv x \ (3)$

$\frac{p-1}{(n, p-1)} = \frac{6}{(3,6)} = 2$

$0, 1, -1$

$x \equiv 2a \ (7)$ ha sempre soluzione, qualsiasi sia a.

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

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

(d) $3^x \equiv a \ (30)$

$=$

3
$3^2 = 9$
$\vdots$

$x > 0$ (altrim. c'è la sol. $a \equiv 1 \ (30)$)

$$\begin{cases} 3^x \equiv a \ (3) \leftarrow \begin{cases} a \equiv 0 \ (3) \\ a \equiv 3, 9, 7, 1 \ (10) \end{cases} \\ 3^x \equiv a \ (10) \end{cases} \quad \left.\begin{array}{l} 4 \text{ soluzioni per } a \\ \text{mod } 30 \end{array}\right\}$$

$3, 9, 27, 21$

(e) $x^3 \equiv 2a \ (14)$

$$\begin{cases} x^3 \equiv 0 \ (2) \Rightarrow \underline{x \text{ pari}} \\ x^3 \equiv 2a \ (7) \end{cases}$$

---

(7) p Esistono infiniti n t.c. $p \mid 2^n - n$

$2^n \equiv n \ (p)$

$$\begin{cases} 2^n \equiv 1 \ (p) \\ n \equiv 1 \ (p) \end{cases} \longrightarrow \operatorname{ord}_p(2) \mid n$$

Ci basta $p-1 \mid n$

ovvero $n \equiv 0 \ (p-1)$

$$\begin{cases} n \equiv 0 \ (p-1) \\ n \equiv 1 \ (p) \end{cases}$$

TCR: esiste una soluzione mod $\underline{p(p-1)}$

$2^n \equiv n \ (p)$

a $\quad$ a

$$\begin{cases} 2^n \equiv a \ (p) \\ n \equiv a \ (p) \end{cases}$$

(9) $\forall\ d, m, n$ $\exists$ progressione aritmetica con

$x,\ x+d,\ x+2d,\ x+3d,\ \dots,\ x+(m-1)d$

tutti multipli di qualche potenza n-esima > 1

$$\longrightarrow \begin{cases} x \equiv 0 \pmod{p_1^n} \\ x+d \equiv 0 \pmod{p_2^n} \\ \vdots \\ x+(m-1)d \equiv 0 \pmod{p_m^n} \end{cases} \quad \leftarrow \quad p_1, p_2, \dots, p_m \text{ primi distinti}$$

$$\begin{cases} x \equiv 0 \pmod{p_1^n} \\ x \equiv -d \pmod{p_2^n} \\ \vdots \\ x \equiv -(m-1)d \pmod{p_m^n} \end{cases}$$

TCR

Esiste una sol. per x mod $p_1^n \cdots p_m^n$