TEOREMA CINESE E ALTRO

Titolo nota 15/10/2013

ES. 1 TROVARE LE SOL. INTERE ≥ 0 DI

$$2^m - n^2 = 1$$

A OCCHIO $m = 0$ $n = 0$

$m = 1$ $n = 1$

mod 4

$m \geq 2$ $\quad 2^m - n^2 \equiv 0 - n^2 \equiv 1 \quad (4)$

$n^2 \equiv \begin{cases} 1 \\ 0 \end{cases} \quad (4)$

ES. 2

$15x^2 - 7y^2 = 9$ CERCO x, y NATURALI

y È UN MULTIPLO DI 3 $\quad y = 3y'$

$$15x^2 - 7 \cdot 9y'^2 = 9$$

$$5x^2 - 21y'^2 = 3$$

x È UN MULTIPLO DI 3 $\quad x = 3x'$

$$45x'^2 - 21y'^2 = 3$$

$$15x'^2 - 7y'^2 = 1$$

mod 3

$0 - y^{12} = 1$ ASSURDO

(mod 36) $a \equiv b \quad (36)$

$a - b$ è multiplo di 36

cioè è multiplo di 4 e di 9

cioè $a \equiv b \quad (4)$ e $a \equiv b \quad (9)$

IDEM $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$

$a \equiv b \quad (n)$ equivale a dire

$a \equiv b \pmod{p_1^{\alpha_1}}$, $a \equiv b \pmod{p_2^{\alpha_2}}$, ..., $a \equiv b \pmod{p_k^{\alpha_k}}$

CALCOLARE LE ULTIME 2 CIFRE DI 27^{26}

$\varphi(100) = 40$

$27^{26} \equiv (-1)^{26} \equiv 1 \pmod 4$

$27^{26} \equiv 2^{26} \equiv 2^6 \equiv 14 \pmod{25}$

$\varphi(25) = 20$

$89 \equiv 1 \quad (4) \qquad 89 \equiv 14 \quad (25)$

TEOREMA CINESE DEL RESTO

$n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ dati $b_1, \ldots b_k$ interi

$$\begin{cases} x \equiv b_1 & (p_1^{\alpha_1}) \\ x \equiv b_2 & (p_2^{\alpha_2}) \\ \\ \\ x \equiv b_k & (p_k^{\alpha_k}) \end{cases}$$

$0 \leq b_1 \leq p_1^{\alpha_1} - 1$

$0 \leq b_2 \leq p_2^{\alpha_2} - 1$

$0 \leq b_k \leq p_k^{\alpha_k} - 1$

ESISTE ESATTAMENTE UN x COMPRESO TRA 0 E $n-1$ CHE RISOLVA IL SISTEMA

$$a \equiv b \ (n) \Rightarrow a \equiv b \ (p_j^{\alpha_j})$$

DIM $\Rightarrow$ PRENDO I NUMERI DA 1 A n E PER OGNUNO SCRIVO LA LISTA DEI RESTI MODULO $p_j^{\alpha_j}$

1 1 1 1 1 1

2 2 2 2 2 2

(oppure 0)

ℓ $\quad b_1(\ell)\ b_2(\ell) \quad \ldots \quad b_k(\ell)$

PER b_1 HO $p_1^{\alpha_1}$ SCELTE $\quad 0 \le b_1 \le p_1^{\alpha_1} - 1$

b_j $\quad p_j^{\alpha_j}$ $\quad 0 \le b_j \le p_j^{\alpha_j} - 1$

IN TUTTO HO n LISTE $(b_1, \ldots, b_k)$ POSSIBILI

NUMERI DA 1 A n

LISTE

PER ASSURDO ESISTONO x E y CHE GENERANO LA STESSA LISTA

$x \equiv b_1 \quad y \equiv b_1 \quad (p_1^{\alpha_1}) \quad x \equiv b_2 \quad y \equiv b_2 \quad (p_2^{\alpha_2})$

$x \equiv b_n \quad y \equiv b_n \quad (p_n^{\alpha_n})$

$x - y \equiv 0 \quad (p_1^{\alpha_1})$ MA ANCHE $(p_2^{\alpha_2})$ _ _ _

$x - y$ È DIVISIBILE PER n

$1 \leq x \leq n$

$1 \leq y \leq n$

$x \neq y$

$$\begin{cases} x \equiv 1 & (p_1^{\alpha_1}) \\ x \equiv 0 & (p_2^{\alpha_2}) \\ \\ \\ x \equiv 0 & (p_k^{\alpha_k}) \end{cases}$$

x È MULTIPLO DI $p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

$$x = \lambda \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

$$\lambda \cdot (p_2^{\alpha_2} \cdots p_k^{\alpha_k}) \equiv 1 \quad (p_1^{\alpha_1})$$

$$\lambda (p_2^{\alpha_2} \cdots p_k^{\alpha_k}) + \mu p_1^{\alpha_1} = 1$$

$$\begin{cases} x \equiv 0 & (p_1^{\alpha_1}) \\ x \equiv 0 & (p_2^{\alpha_2}) \\ \\ \\ x \equiv 1 & (p_k^{\alpha_k}) \end{cases}$$

$$\begin{cases} x \equiv b_1 & (p_1^{\alpha_1}) \\ \\ x \equiv b_k & (p_k^{\alpha_k}) \end{cases}$$

$$\boxed{b_1 x_1 + \dots + b_k x_k}$$

mod 6

$6 = 2 \cdot 3$

1	1	1
2	0	2
3	1	0
4	0	1
5	1	2
6	0	0

$$\begin{cases} x_1 \equiv 1 \quad (2) \\ x_1 \equiv 0 \quad (3) \end{cases}$$

$$x_1 \equiv 3$$

$$\begin{cases} x_2 \equiv 0 \quad (2) \\ x_2 \equiv 1 \quad (3) \end{cases}$$

$$x_2 = 4$$

$$\begin{cases} x \equiv 1 \quad (2) \\ x \equiv 2 \quad (3) \end{cases} \qquad x = 1 \cdot 3 + 2 \cdot 4 \equiv 5 \quad (6)$$

$n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ $\qquad \varphi(n) = ?$

$$\begin{cases} x \equiv b_1 \quad (p_1^{\alpha_1}) \\ \\ x \equiv b_k \quad (p_k^{\alpha_k}) \end{cases}$$

con

b_1 coprimo con $p_1^{\alpha_1}$

b_k coprimo con $p_k^{\alpha_k}$

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k})$$

$\varphi(n)$ è pari per $n \geq 3$

$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ è quasi sempre pari

$\pmod 5$

$2^0 \quad 2^1 \quad 2^2 \quad 2^3 \quad 2^4 \quad 2^5 \quad 2^6 \quad 2^7 \ldots$

$1 \quad 2 \quad 4 \quad 3 \quad 1 \quad 2 \quad 4 \quad 3 \ldots$

$4^0 \quad 4^1 \quad 4^2 \quad 4^3 \quad 4^4 \ldots$

$1 \quad 4 \quad 1 \quad 4 \quad 1$

ORDINE MOLTIPLICATIVO

a, n con a coprimo con n. a intero qualunque

$$a^{\varphi(n)} \equiv 1 \quad (n) \qquad n \geq 2$$

$\mathrm{ord}_n(a)$ è il più piccolo esponente $s \geq 1$ per cui $a^s \equiv 1 \pmod{n}$

$$a^0 \quad a^1 \quad a^2 \quad a^3 \quad \_ \quad \_ \quad a^s \quad \_ \quad a^{s+1} \quad \_ \quad \_ \quad a^{2s} \quad \_ \quad a^{\varphi(n)}$$

$$1 \qquad\qquad\qquad 1$$

$$a^1 \equiv a^3 \quad (n) \implies a^2 \equiv a^2 \quad (n)$$

s divisore $\varphi(n)$

g è un generatore $(\mod n)$ se $\mathrm{ord}_n(g) = \varphi(n)$
cioè le potenze di g coprono tutte le classi coprime con n $(\mod n)$

FATTI 1) DATO p primo, esiste sempre un generatore $(\mod p)$

2) DATO p primo DISPARI, esiste un generatore $\mod p^k$

$(\mathrm{mod}\ 7)$

5^0	5^1	5^2	5^3	5^4	5^5	5^6
1	5	4	6	2	3	1

$(\mathrm{mod}\ 9)$

2^0	2^1			2^4	2^5	2^6
1	2	4	8	7	5	1

TEOREMA DI WILSON. p PRIMO DISPARI.

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

$1, 2, \dots, p-1$

$g^0, g^1, \dots \underbrace{g^{p-2}} \quad g^{p-1} \equiv g^0$

$$(p-1)! \equiv g^0 \cdot g^1 \cdot \dots \cdot g^{p-2} = g^{0+1+2+\dots+p-2} \equiv$$

$$\equiv g^{\frac{(p-1)(p-2)}{2}} \equiv \left(g^{\frac{p-1}{2}}\right)^{p-2}$$

$g^{\frac{p-1}{2}}$ è una classe h t.c. $h^2 \equiv 1 \quad (p)$

$h^2 - 1 = \underbrace{(h-1)}_{g^{\frac{p-1}{2}}-1}(h+1)$ è divisibile per p

$g^{\frac{p-1}{2}} \equiv -1 \quad (p)$ $\qquad \left(g^{\frac{p-1}{2}}\right)^{p-2} \equiv -1 \quad (p)$