CONGRUENZE: ESEMPI

Note Title 10/25/2017

Determinare le ultime 2 cifre del numero $13^{39^5} = 13^{(39^5)} = n$

$n \bmod 100$

Eulero-Fermat $\Rightarrow$ $13^{\varphi(100)} \equiv 1 \bmod 100$

$1 \quad 13 \quad 69 \quad \dots$

$1 \equiv 13^{\varphi(100)} \quad 13$

Il problema si riduce a calcolare

$$39^5 \equiv -1 \pmod{\varphi(100)}$$

$$(-1)^5 \equiv -1 \pmod{40}$$

$$13^{39^5} \equiv 13^{40k-1} \equiv (13^{40})^k \cdot 13^{-1} \pmod{100}$$

(Eulero Fermat)

$$\equiv 1^k \cdot 13^{-1} \pmod{100}$$

Oss $13^{39} \cdot 13 \equiv 13^{40} \equiv 1 \bmod 100$

cioè 13^{39} è un inverso di 13 (mod 100)

Troviamo l'inverso!

$$100 = 13 \cdot 7 + 9$$

$$13 = 9 + 4$$

$$9 = 4 \cdot 2 + 1$$

$$\Rightarrow \quad 1 = 9 - 4 \cdot 2 = 9 - 2 \cdot (13 - 9)$$

$$= 3 \cdot 9 - 13 \cdot 2$$

$$= 3 \cdot (100 - 7 \cdot 13) - 13 \cdot 2$$

$$= 3 \cdot 100 - 23 \cdot 13$$

Mod 100 otteniamo $1 \equiv (-23) \cdot (13) \pmod{100}$

13^{395} termina con le cifre $77 = 100 - 23$

$$12345 = 5 + 4 \cdot 10 + 3 \cdot 10^2 + 2 \cdot 10^3 + 1 \cdot 10^4$$

- $5^{5^{17}} \mod 13$

$\downarrow$

$5^{17} \pmod{\varphi(13) = 12}$

$\downarrow$

$17 \mod \varphi(12) = \varphi(4)\,\varphi(3) = 2 \cdot 2 = 4$

$17 = 4\cdot 4 + 1$ $\qquad 5^{17} \equiv 5^{4\cdot 4}\cdot 5 \mod 12$

$\equiv 1^4 \cdot 5 \equiv 5 \mod 12$

Per Eulero-Fermat,

$5^{5^{17}} \equiv 5^{12k+5} \equiv (1^k)\cdot 5^5 \equiv 5^2 5^2 5 \pmod{13}$

$\equiv (-1)(-1)5 \equiv 5$

$a \equiv b \mod m$ NON IMPLICA $2^a \equiv 2^b \mod m$

- Trovare gli x t.c. $X^X \equiv 3 \mod 5$

$5 \nmid x$ $\qquad (x \not\equiv 0 \mod 5)$

Può $x \equiv \pm 1 \mod 5$? No, perché

$(\pm 1)^x \equiv \pm 1$ e $\pm 1 \not\equiv 3 \mod 5$

Supponiamo $X \equiv 2 \mod 5$. Allora stiamo considerando il sistema

$$\begin{cases} X \equiv 2 \pmod 5 \\ X^X \equiv 3 \pmod 5 \end{cases}$$

$$\begin{cases} x \equiv 2 \mod 5 \\ 2^x \equiv 3 \mod 5 \end{cases}$$

~~$\begin{cases} x \equiv 2 \ (5) \\ x^2 \equiv 3 \ (5) \end{cases}$~~

$$\underbrace{(2+5k)(2+5k)\cdots(2+5k)}_{x \text{ volte}} \equiv 2^x \mod 5$$

$$(2+5k)(2+5k)\cdots(2+5k) \not\equiv (2+5k)^2$$

$$\begin{cases} x \equiv 2 \mod 5 \\ 2^x \equiv 2^3 \mod 5 \end{cases} \qquad \begin{cases} x \equiv 2 \mod 5 \\ 2^{x-3} \equiv 1 \mod 5 \end{cases}$$

$$\Downarrow$$

$$\text{ord}_5(2) \mid x-3$$

Calcoliamo $\text{ord}_5(2) = 4 = \varphi(5)$

$2^0 \equiv 1 \quad 2^1 \equiv 2 \quad 2^2 \equiv 4 \quad 2^3 \equiv 3 \quad 2^4 \equiv 1 \ (5)$

$$\begin{cases} x \equiv 2 \mod 5 \\ x-3 \equiv 0 \mod (\text{ord}_5(2) = 4) \end{cases}$$

$\Leftrightarrow \quad x \equiv 7 \pmod{20}$

Manca l'altro caso, $x \equiv 3 \mod 5$:

$$\begin{cases} x \equiv 3 \quad (5) \\ 3^x \equiv 3 \quad (5) \end{cases} \iff \begin{cases} x \equiv 3 \quad (5) \\ 3^{x-1} \equiv 1 \quad (5) \end{cases}$$

$$\Updownarrow$$

$$\text{ord}_5(3) \mid x-1$$

$$\begin{cases} x \equiv 3 \quad (5) \\ x \equiv 1 \quad (4) \end{cases} \overset{\text{TCR}}{\iff} x \equiv 13 \mod 20$$

- Dimostrare "senza fare conti" che

$$k = \text{ord}_{11}(9) = 5$$

Piccolo Teo Fermat $\Rightarrow k \mid \varphi(11) = 10$

$k \in \{1, 2, 5, 10\}$.

$$9^5 \equiv 3^{10} \equiv 1 \pmod{11}$$

Siccome $9^5 \equiv 1 \mod 11$ sappiamo che $k \mid 5$

Dunque $k = 1$ o $k = 5$, ma $k \neq 1$,

quindi $k = 5$

- Determinare le soluzioni di

$$x^3 + 5 \equiv 0 \pmod{7 \cdot 8 \cdot 11}$$

$$\Updownarrow$$

$$\begin{cases} x^3 + 5 \equiv 0 \mod 7 & \text{③} \\ x^3 + 5 \equiv 0 \mod 8 \iff x \equiv 3 \ (8) & \text{①} \\ x^3 + 5 \equiv 0 \mod 11 \iff x \equiv 8 \ (11) & \text{②} \end{cases}$$

① x è dispari $\Rightarrow x^3 \equiv x^{-1} \mod 8$

$$x^{-1} \equiv 3 \mod 8$$

$$\Rightarrow x \equiv (3^{-1}) \equiv 3 \mod 8$$

Più costruttivamente: $x^3 \equiv x^2 \cdot x \equiv x \mod 8$

② $x^3 \equiv 6 \pmod{11}$ $\quad (x, 11) = 1$

Siccome 3 e $\varphi(11) = 10$ sono coprimi,

posso scrivere $1 = 10 - 3 \cdot 3$

$$x^1 \equiv x^{10} \cdot x^{-9} \overset{FLT}{\equiv} 1 \cdot (x^3)^{-3} \quad (11)$$

$$\equiv 6^{-3} \equiv 2^3 \equiv 8 \quad (11)$$

③ $x^3 + 5 \equiv 0 \mod 7$

$x^3 \equiv 2 \mod 7$

$x = \cancel{0}, \cancel{1}, 2, 3, 4, 5, \cancel{6}$

$x^3 \equiv 0, 1, 1, -1, 1, -1, -1 \pmod 7$

Morale: • non ci sono soluz. dell'eqz. originaria

• modulo 7, $x^3 \equiv$ qualcosa può avere 0, 1, 3 soluzioni

Novembre 2014 Determinare per quali valori di a il seguente sistema ha soluzioni

$$\begin{cases} X^{27} \equiv X^2 & \text{mod } 144 = 16 \cdot 9 \\ 10X \equiv a & \text{mod } 25 \\ 2^{X-1} \equiv 4 & \text{mod } 11 \end{cases}$$

e determinarle

Soluzione

$$\begin{cases} X^{27} \equiv X^2 & \text{mod } 16 \\ X^{27} \equiv X^2 & \text{mod } 9 \\ 10X \equiv a & \text{mod } 25 \longrightarrow 10X \equiv a \ (5) \\ 2^{X-1} \equiv 4 & \text{mod } 11 \end{cases}$$

$0 \equiv 0$

I osservazione: affinché ci siano soluzioni deve valere $a \equiv 0 \text{ mod } 5$

$a = 5K$ 3ª eqz diventa $10X \equiv 5K \ (25)$

$\iff 2X \equiv K \text{ mod } 5$

$25 \mid 10X - 5K$

$= 5(2X - K)$

Studiamo $2^{X-1} \equiv 4 \text{ mod } 11$

$\iff 2^{X-3} \equiv 1 \text{ mod } 11$

$\Longleftrightarrow 10 = \mathrm{ord}_{11}(2) \mid x-3$

$2^1 \overset{?}{\equiv} 1 \quad (11)$ NO

$2^2 \overset{?}{\equiv} 1 \quad (11)$ NO

$2^5 \overset{?}{\equiv} 1 \quad (11)$ NO

$2^{10} \overset{?}{\equiv} 1 \quad (11)$ Per il piccolo teo di Fermat, sì

Il sistema originario è equivalente a

$$\begin{cases} x^{27} \equiv x^2 & \text{mod } 16 \\ x^{27} \equiv x^2 & \text{mod } 9 \\ 2x \equiv k & \text{mod } 5 \\ x \equiv 3 & \text{mod } 10 \end{cases}$$

dove $k = a/5 \in \mathbb{Z}$

$\longrightarrow x \equiv 1 \ (2)$

$\searrow x \equiv 3 \ (5)$

$$\begin{cases} x \equiv 3 \ (5) \\ 2x \equiv k \ (5) \end{cases} \Longrightarrow k \equiv 1 \ \text{mod } 5$$

$$\Longrightarrow \boxed{a \equiv 5 \ \text{mod } 25}$$

La prima eqz. ora dà

e' dispari!

$$\begin{cases} x^2 (x^{25} - 1) \equiv 0 \ (16) \\ x \equiv 1 \ (2) \end{cases}$$

Inoltre x dispari $\Longrightarrow x^8 \equiv 1 \ (16)$ per Eulero

$$1 \equiv x^{25} \equiv x^8 x^8 x^8 x \equiv x \ (\text{mod } 16)$$

Sistema originale $\iff$ $\begin{cases} X \equiv 1 \mod 16 \\ X^2(X^{25}-1) \equiv 0 \mod 9 \\ X \equiv 3 \ (5) \\ a \equiv 5 \ (25) \end{cases}$

2 casi: o $3 \mid x$ (e la 2ª eqz. è verificata)

o $3 \nmid x$, nel qual caso

$$1 \equiv X^{25} \equiv (X^6)^4 \cdot x \equiv x \mod 9$$

Conclusione Se $a \not\equiv 5 \mod 25$ | NO SOLUZ |

Se $a \equiv 5 \ (25)$, le soluzioni rispettano

$\begin{cases} X \equiv 1 \ (16) \\ X \equiv 0 \ (3) \\ X \equiv 3 \ (5) \end{cases}$ o $\begin{cases} X \equiv 1 \ (16) \\ X \equiv 1 \ (9) \\ X \equiv 3 \ (5) \end{cases}$

$\Updownarrow$ $\Updownarrow$

$X \equiv 33 \mod 240$ $X \equiv ?? \mod (720)$

$\begin{cases} X \equiv 1 \ (16) \\ X \equiv 0 \ (3) \\ X \equiv 0 \ (5) \end{cases}$, $\begin{cases} X \equiv 0 \ (16) \\ X \equiv 1 \ (3) \\ X \equiv 0 \ (5) \end{cases}$, $\begin{cases} X \equiv 0 \ (16) \\ X \equiv 0 \ (3) \\ X \equiv 1 \ (5) \end{cases}$

- Sia p un numero primo tale che

$$2^{2^{30}} \equiv -1 \mod p$$

Quanto vale $\mathrm{ord}_p(2)$?

(p esiste? Congr. $\iff p \mid 2^{2^{30}}+1$)

$$2^{2^{31}} \equiv 1 \mod p \implies \mathrm{ord}_p(2) \mid 2^{31}$$

Può essere $\mathrm{ord}_p(2) < 2^{31}$?

$$\mathrm{ord}_p(2) = 2^a$$

Supponiamo $a < 31$. Allora $2^a \mid 2^{30}$.

$$\implies 2^{2^a} \equiv 1 \mod p$$

$\implies$ continuando a prendere quadrati,

$$-1 \equiv 2^{2^{30}} \equiv 1 \mod p$$

e questo è assurdo perché $p \neq 2$.