TdN 2 Esercizi

Titolo nota 06/09/2007

④ Ultime 5 cifre di $5^{5^{5^5}} = A$

$\updownarrow$

congruenza mod 10^5

$\updownarrow$ cinese

Congruenza mod 5^5 e mod 2^5

$A \equiv 0 \quad (5^5)$

$A \equiv ? \quad (2^5 = 32)$ Come si comportano le potenze di 5 (mod 32)

$\text{ord}_{32}(5) \mid \phi(32) = 16$ ord = 1, 2, 4, 8, 16

$$5^4 \equiv 25^2 \equiv (-7)^2 \equiv 49 \not\equiv 1 \pmod{32}$$

$\operatorname{ord}_{32}(5) = 8$

$A = 5^B$ la congruenza di $A \pmod{32}$ dipende dalla congruenza di $B \pmod 8$

Le potenze di 5 $\pmod 8$ sono alternate: 5, 1, 5, 1, ...

pari

disp

$B \equiv 5 \pmod 8$

Conclusione:

$$\left.\begin{aligned} A &\equiv 5^5 \pmod{32} \\ A &\equiv 5^5 \pmod{5^5} \end{aligned}\right\} \Rightarrow A \equiv 5^5 \pmod{10^5}$$

$\Rightarrow$ le ultime 5 cifre sono quelle di 5^5

$$\boxed{03125}$$

Se scriviamo le ultime 5 cifre di 5^n al variare di n otteniamo una succ. di periodo 8 da un certo p.to in poi. C'è un antiperiodo fino a $n=5$

— o — o →

(7) Esistono infiniti n t.c. $2^n - n \equiv 0 \ (p)$

Dimostro di più: esistono infiniti n t.c.

$$\begin{cases} 2^n \equiv 1 \ (p) \\ n \equiv 1 \ (p) \end{cases}$$

← basta che n sia multiplo di $p-1$

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

COPRIMI ⇓ ciuese ok

— o — o —

(8) Sia (2^n) ↑ gradi sessagesimali, cioè capire $2^n \pmod{360}$

$360 = 8 \cdot 5 \cdot 9$

cioè 2^n →
- $\pmod 8$: $2^n \equiv 0$ da $n \geq 3$
- $\pmod 5$: $2, 4, 3, 1$
- $\pmod 9$: $2, 4, 8, 7, 5, 1$

Il periodo di $2^n \bmod 360$ è $12 = \text{m.c.m.}(\text{periodi})$

Basta calcolare $2^0, 2^1, \dots, 2^{12} \pmod{360}$

Facendo i conti, il + vicino a 30 è $2^6 = 64$.

In alternativa: controllare a mano che i multipli di 8 + vicini a 30 non siano potenze di 2.

Es. 10 PPP (Più Piccolo Primo)

(a) $2^p + 1 \equiv 0 \quad (p)$

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

$\downarrow$ ← FERMAT

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

$2^{2p} \equiv 1 \quad (p)$ — Per ora non serve

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

$3 \equiv 0 \quad (p) \Rightarrow p = 3$

(b) $2^n + 1 \equiv 0 \quad (n)$

Sia p un primo t.c. $p \mid n$

$\Downarrow$

$2^n + 1 \equiv 0 \quad (p) \Rightarrow 2^n \equiv -1 \quad (p)$

$\Downarrow$

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

$\Downarrow$

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

$4^n \equiv 1 \ (p)$ $\quad \text{ord}_p(4) \mid p-1$ FATTO GENERALE

$\Rightarrow \text{ord}_p(4) \mid n$ DALL'EQUAZIONE

SIA p IL PPP che divide n

I fattori primi di $\text{ord}_p(4)$ devono dividere n e devono dividere $p-1$

Conseguenza: se $\text{ord}_p(4)$ non è 1, allora ha un fattore primo q. Questo primo q divide $p-1$, quindi è + piccolo di p ma deve dividere anche n. Assurdo perchè n non ha fattori + piccoli di p.

$\Rightarrow \text{ord}_p(4) = 1 \Rightarrow 4^1 \equiv 1 \ (p) \Rightarrow p = 3$

Quindi: se $n \in D$, allora il PPP che divide n è 3. Questo dimostra (d).

Al punto (b) ci dicevano quali potenze di 3 appartengono a D.

$3 \mid 2^3+1$ $\quad$ $9 \mid 2^9+1 = 513 = 27 \cdot 19$

$3^2 \mid 2^3+1$ $\quad$ $3^3 \mid 2^9+1$ $\quad$ $3^4 \mid 2^{27}+1$

Congettura: $3^{k+1} \mid 2^{3^k}+1$ $\quad$ ($\Rightarrow$ tutte le potenze di 3 stanno in D)

Induzione $\quad k \Rightarrow k+1$

3^{k+1} divide $\quad$ $1-(-1)+1$ ← NUOVO FATT. 3

$$2^{3^{k+1}}+1 = \left(2^{3^k}\right)^3+1 = \left(2^{3^k}+1\right)\left(2^{2\cdot 3^k}-2^{3^k}+1\right)$$

$$a^3+1 = (a+1)(a^2-a+1)$$

Oss. Migliorando la dimostrazione si può dim. che

$$3^{k+1} \parallel 2^{3^k}+1$$

(basta fare $a^2-a+1 \bmod 3$)

(c) $2^{pq}+1 \equiv 0 \quad (pq)$

$2^{3q}+1 \equiv 0 \quad (3q)$

$8^q+1 \equiv 0 \quad (3q) \Rightarrow 8^q \equiv -1 \quad (q)$

↕ FERMAT

$8 \equiv -1 \quad (q)$

$9 \equiv 0 \quad (q) \Rightarrow q=3$

9 è l'unico prodotto di 2 primi che sta in D

(e)

$2^{3p^2} + 1 \equiv 0 \quad (3p^2)$

$\Updownarrow$

$8^{p^2} + 1 \equiv 0 \quad (3p^2)$

$\Downarrow$

$(8^p)^p + 1 \equiv 0 \quad (p)$

↓ PICCOLO FERMAT 2 VOLTE

$8 + 1 \equiv 0 \quad (p)$

↓

$p = 3$ che non va bene perchè $p = q$

$2^{9q} + 1 \equiv 0 \quad (9q)$

$\Downarrow$

$(2^9)^q + 1 \equiv 0 \quad (q)$

↓ FERMAT

$512 + 1 \equiv 0 \quad (q)$

↓

$513 \equiv 0 \quad (q)$

$\|$

$27 \cdot 19$

↓

$q = 19$

Resta da verificare che 19 va bene, cioè $9 \cdot 19 =$ 6D

$$2^{171} + 1 \equiv 0 \quad (171)$$

$$\downarrow$$

$$2^{171} + 1 \equiv 0 \quad (9) \qquad 2^{9 \cdot 19} + 1 \equiv 0 \quad (9)$$

$$2^{171} + 1 \equiv 0 \quad (19) \qquad 2^{3 \cdot 3 \cdot 19} + 1$$

$$2^{9 \cdot 19} + 1 = \left(2^{9} + 1\right) \cdot \text{ROBA} \qquad = \left(2^{3}\right)^{3 \cdot 19} + 1 \equiv 0 \quad (9)$$

$\uparrow$

c'è 19