CORREZIONE ESERCIZI DI ARITMETICA

Titolo nota 15/10/2013

1) Trovare il minimo $n \in \mathbb{N}$ positivo
- composto da 5 e 7
- multiplo di 9 ← ↑ SEMBRA COMODO IL CRITERIO DI DIV. PER 9

Se n ha x cifre 5 e y cifre 7
allora è multiplo di 9 se e solo se $5x+7y$ è multiplo di 9

$$9 \mid 5x+7y$$

MODO 1 $\left(x = 0 \rightarrow y = 9 \text{ (come minimo!)} \right)$

777777777

$x = 1$ $\quad 7y + 5 \equiv 0 \ (9)$

$49 + 5$

$(y = 7)$ $\quad$ 57777777

$x = 2$

$\vdots$

$x = 9 \ (8)$ $\quad x = 10$ è superfluo

MODO 2 $\quad 9 \mid 5x + 7y$

$[\ 5x + 7y \equiv 0 \ (9)$

Un numero è multiplo di 9 se e solo se il suo doppio lo è

$$10x + 14y \equiv 0 \ (9)$$

$$1 \cdot x + 5 \cdot y \equiv 0 \ (9)$$

$$x + 5y \equiv 0 \ (9)$$

$$x \equiv -5y \equiv 4y \ (9)$$

$$\boxed{x \equiv 4y \ (9)}$$

Se $y \equiv 0 (9) \Rightarrow x \equiv 0 (9)$

$y \equiv 1 (9) \Rightarrow x \equiv 4 (9)$

...

$x = 0, y = 9$

$x = 9, y = 0$

$\boxed{x = 4, y = 1}$ → 55557

MODO 3

$$9(5x+7y$$

$$27 = 5+5+5+5+7$$

2) $x^4 \equiv 13 \ (17)$

1^4, $2^4 = 16$, $3^4 = 81 \equiv 13 \ (17)$

Oss: Se $\bar{x}$ è soluzione, allora anche $\bar{x} + 17k$ è soluzione

Infatti, la classe di congruenza di x^4 dipende solo dalla classe di congruenza di x

$(\bar{x} + 17k)^4 = \bar{x}^4 + \ldots$ ← multipli di 17

Se troviamo le soluzioni per $x \in \{0, 1, \dots, 16\}$ abbiamo finito

MODO 1: provarle tutte

MODO 2:

$$x^4 \equiv 13 \ (17)$$

3 è soluzione $\rightsquigarrow$ $3^4 \equiv 13 \ (17)$

$$x^4 \equiv 3^4 \ (17)$$

$$(x^2 + 3^2)(x^2 - 3^2) \equiv 0 \ (17)$$

$$(x+3)(x-3)$$

$x^2+9 \sim x^2-(-9) =$

$= x^2-(-1)\cdot 9 \equiv x^2-2^4\cdot 9 = x^2-4^2\cdot 3^2 =$

$2^4 = 16 \equiv -1 \ (17)$

↑ modulo 17

$= (x+12)(x-12)$

$(x+3)(x-3)(x+12)(x-12) \equiv 0 \ (17)$

17 è primo $\Rightarrow$

$x+3 \equiv 0 \ (17) \longrightarrow x \equiv 14 \ (17)$

$x-3 \equiv 0 \ (17) \longrightarrow x \equiv 3 \ (17)$

$x+12 \equiv 0 \ (17) \longrightarrow x \equiv 5 \ (17)$

$x-12 \equiv 0 \ (17) \longrightarrow x \equiv 12 \ (17)$

MODO 3: generatori

$x^4 \equiv 13 \ (17)$

$x = g^k \qquad g^{4k} \equiv g^{\square} \ (17) \longrightarrow 4k \equiv \ldots \ (16)$

RIFLESSIONE

$x^4 - 13 = 0$ in $\mathbb{Z}/17\mathbb{Z}$ ← è un campo (17 è primo)

≤ 4 radici

---

3) $7x - 5y = 2$ con $x, y \in \mathbb{Z}$

↓ $ax + by = c$ (algoritmo di Euclide)

$7x - 2 = 5y$ "Per quali x, $7x - 2$ è multiplo di 5 ?"

$7x - 2 \equiv 0 \ (5)$

$7x \equiv 2 \ (5)$

$2x \equiv 2 \ (5)$

ok, perché $MCD(2,5) = 1$

$x \equiv 1 \ (5)$

$\rightarrow \boxed{x = 1 + 5k}$

$$y = \frac{7x-2}{5} = \frac{7(1+5k)-2}{5} =$$

$$= \frac{7 + 35k - 2}{5} = \boxed{7k + 1} \quad \forall y$$

Al variare di $k \in \mathbb{Z}$: $(1+5k, 1+7k)$

4) $n = 9$

Vero esercizio: quali sono <u>tutti</u> gli n tali che

$$\begin{cases} 11 \mid n+2 \\ 13 \mid n+4 \\ 15 \mid n+6 \end{cases} \quad ?$$

TEOREMA CINESE DEL RESTO

$$\begin{cases} n \equiv -2 \ (11) \\ n \equiv -4 \ (13) \\ n \equiv -6 \ (15) \end{cases}$$

→ Esiste un'unica soluzione modulo $11 \cdot 13 \cdot 15 = m$

Tutte le soluzioni sono della forma $9 + \underbrace{K \cdot m}_{\text{pari}} = \boxed{9 + 2145k}$

$$\begin{cases} x \equiv -2 \ (11) \\ x \equiv -4 \ (13) \end{cases} \rightsquigarrow \begin{cases} x = -2 + 11a \\ x = -4 + 13b \end{cases}$$

$$-2 + 11a = -4 + 13b$$

$$11a - 13b = -2$$

5) OSS/ATTENZIONE: non è un criterio di congruenza

$$10a + b \rightsquigarrow a - 2b$$

$(182 = 10 \cdot 18 + 2)$

Falso: $10a + b \equiv a - 2b \ (7)$

$a = 1, b = 2 \quad 12 \equiv -3 \ (7)$ Appunto è FALSO!

$10a+b \equiv 3a+b \pmod 7$

TESI: $3a+b \equiv 0 \pmod 7 \iff a-2b \equiv 0 \pmod 7$

① Assumiamo che $3a+b \equiv 0 \pmod 7$

IDEA: moltiplicare per -2

$3a+b \equiv 0 \pmod 7 \iff \underbrace{-6a-2b}_{\| \\ a-2b} \equiv 0 \pmod 7$

SOLUZIONE 2:

$3a-6b = \cancel{3}(a-2b)$

SOL 3

$3a+b = 7k$

$\Rightarrow b = 7k-3a$

$a-2(7k-3a) =$

$= 7a-14k \equiv 0 \pmod 7$

6) $n = (143)_{238}$

$$n = 1 \cdot \underbrace{238}_{x}^{2} + 4 \cdot \underbrace{238}_{x} + 3 = \dots$$

$$n = x^2 + 4x + 3 = (x+3)(x+1)$$

$$\| $$

$$241 \cdot 239$$

↑ ↗ SONO PRIMI

(Basta provare a dividerli per i primi fino a $\sqrt{241} \simeq 15,\dots$)

7) $2^x + 1 = 3^y$ $\quad x, y$ naturali

- IDEA 1: lavorare modulo qualcosa

ES: mod 2 $\quad$ se $x \geq 1$ $\quad 1 \equiv 3^y$ (2)

NULLA

mod 4 $\quad$ se $x \geq 2$, 2^x è multiplo di 4

$\rightsquigarrow 1 \equiv 3^y \equiv (-1)^y$ (4)

$$(-1)^y \equiv \begin{cases} 1 \text{ se } y \text{ è pari} \\ -1 \text{ se } y \text{ è dispari} \end{cases}$$

$\Rightarrow$ y deve essere pari

$x \leq 1$

- $x = 0$ $\quad 1+1 = 3^y$ NO
- $x = 1$ $\quad 2+1 = 3$

$y = 1$

y qua è dispari!

$y = 2k$

$2^x + 1 = \underbrace{3^{2k}}$

è un quadrato

$2^x = (3^k + 1)(3^k - 1)$

Sono due interi pari (se $k \geq 1$)
che distano 2
e non possono avere fattori primi $\neq 2$
(Sono potenze di 2!)

$k = 0$:
$2^x + 1 = 1$ IMPOSSIBILE

2, 4

$3^k - 1$ $\quad$ $3^k + 1$

$k = 1$
$y = 2k = 2$, $\quad 2^x + 1 = 9$
$x = 3$

$2^x + 1 = 3^y$

mod 3 : $2^x + 1 \equiv 0 \ (3)$ $\quad (y \geq 1)$

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

x deve essere dispari.

$2^x \equiv 2 \ (3)$

$2, 2^2 = 4 \equiv 1, 2, 1, 2, \ldots$

x dispari

$(x^k + y^k) = (x+y)(\_\_\_)$ ...

8) $y^2 = x^5 - 4$

Se scegliamo un certo modulo m
la speranza è che y^2 e x^5 abbiano poche possibilità.

mod 3 $\quad x^5 = \underbrace{x^2}_{\equiv 1} \cdot \underbrace{x^2}_{\equiv 1} \cdot x \equiv x \quad (3)$

NON BUONO

$y^2 + 4 \equiv (y^2+4)^5$

$x = y^2 + 4$

mod p (primo)

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

x^5 $\quad 5 \mid p-1$ $\quad p=11$

$(x^5)^2 \equiv 1 \ (11)$ $\quad = x^{10} = x^{11-1}$

a meno che $x \equiv 0 \ (11)$

x^5 SODDISFA L'EQUAZIONE

$(x^5+1)(x^5-1) \equiv 0 \ (11)$

$z^2 \equiv 1 \ (11) \leftrightarrow (z+1)(z-1) \equiv 0 \ (11)$

$z = 1$

$z = -1$

y^2 $\quad 2 \mid p-1$ $\quad$ (Mod p, per p primo dispari, i quadrati sono esattamente $\frac{p+1}{2}$)

Mod 11

$x^5 \equiv 1, -1$

$y^2 \equiv |0, 1, 4, 9, 5, 3|$

$6^2 \equiv (11-5)^2 \equiv (-5)^2 \equiv 5^2$.

Se $5 \mid p-1$

$p-1 = 5 \cdot k$

$(x^5)^k \equiv 1 \ (p)$

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

$y^2 \equiv x^5 - 4 \quad (11)$ ha $\leq k$ soluzioni

$x^5 \equiv 1 \rightsquigarrow \quad y^2 \equiv -3 \equiv 8 \quad (11)$ NO!

$x^5 \equiv -1 \rightsquigarrow \quad y^2 \equiv -5 \equiv 6 \quad (11)$ NO!

$\Rightarrow$ L'EQUAZIONE È IMPOSSIBILE

9) $p \mid 2^n - n$

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

$2^n \equiv n \equiv 1 \ (p)$ è ancora vera per infiniti n

$$\begin{cases} n \equiv 0 \ (p-1) \\ n \equiv 1 \ (p) \end{cases} \longrightarrow \quad n = (p-1)k$$

$$2^n = (2^k)^{p-1} \equiv 1 \ (p)$$

$$2^n - n \equiv 1 - 1 = 0$$

TEOREMA CINESE DEL RESTO

$2^n \bmod p$ è controllato da $n \bmod (p-1)$

$n \bmod p$ " " $n \bmod (p)$

$(p-1)$ e (p) COPRIMI

$MCD(p-1, p) = 1$

$\bmod p(p-1)$

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

$$2^n \equiv 2^1 = 2 \ (p)$$

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