ARITMETICA - ESERCIZI

Titolo nota 20/10/2010

- CLAUDIOFILIPPO.BIANCHI01@UNIVERSITADIPAVIA.IT
- DAVIDE.LOMBARDO@SNS.IT

n intero, n^2 che resto lascia nella divisione per 4?

n pari $(2 \mid n) \Rightarrow 4 \mid n^2 \qquad n^2 \equiv 0 \ (4)$

n disp. $\quad n = 2K+1 \qquad n^2 = 4K^2 + 4K + 1$

$\equiv 1 \pmod 4$

$x^2 - y^2 = 2010 \qquad \bmod 4$

$x^2 - y^2 \equiv 2 \pmod 4$

$0 - 0$

$0 - 1$

$1 - 0$

$1 - 1$

Quadrati mod 3? $\quad n \equiv 0 \ (3)$

$n^2 \equiv 0 \ (\bmod 3, \bmod 9)$

$n^2 \equiv 7 \pmod{49}$ IMPOSSIBILE

$n^2 \equiv p \pmod{p^2}$ IMPOSS

$n = 3k \pm 1$

$n^2 = 9k^2 \pm 6k + 1 \equiv 1 \pmod{3}$

Non esistono n t.c. $n^2 \equiv 2 \pmod{3}$

$n^{3-1} \equiv 1 \pmod{3}$ ← Fermat

<u>Esempio</u> $x^2 - 7y^2 = 5$

Mod 7 $x^2 \equiv 5 \pmod{7}$

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

$$\begin{array}{ccccccc} \downarrow & \downarrow & \downarrow & \downarrow & & & \\ 0 & 1 & 4 & 2 & 2 & 4 & 1 \end{array}$$

$4 \equiv -3 \pmod 7$

$4^2 \equiv (-3)^2 \equiv 3^2 \pmod 7$

Struttura molt. mod m

$a, a^2, a^3, \dots \quad \bmod m$

$a^k \equiv a^h \pmod m \qquad k \neq h$

$\Downarrow$

$a^{k+1} \equiv a^{h+1} \pmod m$

Se $\text{mcd}(a, m) = 1$, esiste h t.c. $a^h \equiv 1 \pmod{m}$

$5^a \mod 7$ → basta $a \mod 6$

$5, \; 4, \; -1, \; 2, \; 3, \; \boxed{1}$

$5^1, \; 5^2, \; 5^3, \; 5^4, \; 5^5, \; \boxed{5^6}$

$5^{2010} \mod 7 \equiv 5^{6k} \equiv (5^6)^k \equiv 1^k \equiv 1 \pmod{7}$

$5^{2013} \mod 7 \equiv 5^{6k+3} \equiv 5^{6k} \cdot 5^3 \equiv -1 \pmod{7}$

C1) i. Se l'ultima cifra di un quadrato è 6, la penultima è dispari

ii. $2006\,2006 \ldots 2006 \equiv 06 \equiv 2\ (4)$ ASSURDO

$\boxed{C2}$ $2^m - n^2 = 1$

$m = 0 \implies n = 0$

$m = 1 \implies n = 1 \qquad n^2 = 1 \longrightarrow n = +1$

$(n \in \mathbb{N})$

$m = 2 \qquad 4 - n^2 = 1 \qquad n^2 = 3 \equiv 3\ (4)$

$m = 3 \qquad 8 - n^2 = 1 \qquad n^2 = 7 \equiv 3\ (4)$

Se $m \geq 2$, $\underset{\substack{\equiv \\ 1}}{2^m} - n^2 \equiv 0 - n^2 \; (4)$

Allora $n^2 \equiv -1 \; (4)$ impossib.

$\boxed{C3}$ $11 \mid 2a + 3b \implies 11 \mid a^2 - 5b^2$

$$2a + 3b \equiv 0 \pmod{11}$$

$$2a \equiv -3b \pmod{11}$$

$$3 \cdot \; 4a^2 \equiv 3 \cdot 9b^2 \pmod{11}$$

$$12a^2 \equiv a^2 \pmod{11}$$

$$12a^2 \equiv 27b^2 \equiv 5b^2 \pmod{11}$$

$$\begin{array}{c} 12a^2 \\ \equiv \\ a^2 \end{array}$$

$$11 \mid a^2 - 5b^2$$

$\boxed{C4}$ $3x^2 - 2y^2 = 1998$

$$\underset{3}{3x^2} - 2\underset{3}{y^2} = \underset{3}{1998}$$

$$0 - 2y^2 \equiv 0 \pmod{3}$$

$$y^2 \equiv 0 \pmod{3}$$

$$3 \mid y \cdot y \implies 3 \mid y$$

$$y = 3a$$

$$3x^2 - 18a^2 = 2 \cdot 3^3 \cdot 37$$

$$x^2 - 6a^2 = 2 \cdot 3^2 \cdot 37$$

$$3 \mid x \implies x = 6b$$

$$2 \mid x$$

$$2^2 3^2 b^2 - 6a^2 = 2 \cdot 3^2 \cdot 37$$

$$6b^2 - a^2 = 3 \cdot 37$$

$$a = 3d$$

$$2b^2 - 3d^2 = 37$$

$d^2 \equiv 1 \pmod 2$

Mod 3 : $\quad 2b^2 - 0 \equiv 1 \pmod 3$

$b^2 \equiv 4b^2 \equiv 2 \ (3)$ ASSURDO

$\boxed{C5}$ (m, n) interi positivi t.c.

$$\frac{3^m + 3}{2^n + 2^{n-1}}$$ sia intero.

$$\frac{\cancel{3}(3^{m-1}+1)}{2^{n-1} \cdot \cancel{(2+1)}}$$

$n = 1 \rightarrow m$ qualsiasi

$n = 2 \rightarrow$ " "

$n \geq 3 \qquad 4 \mid 2^{n-1}$ e $2^{n-1} \mid 3^{m-1}+1$

In particolare $4 \mid 3^{m-1}+1 \quad (\Rightarrow)$

$(-1)^{m-1}+1 \equiv 3^{m-1}+1 \equiv 0 \quad (4) \quad \Rightarrow m$ pari

$n = 3$, m pari. $\qquad n \geq 4$?

$8 \mid 3^{m-1}+1 \qquad 1, 3, 3^2 \equiv 9 \equiv 1 \pmod 8$

$3^{m-1}+1 \equiv 0 \pmod 8$

$$3^{m-1} \equiv 7 \pmod 8$$ NO

Anche con $n > 4$ non ci sono soluz.

$\boxed{F1}$ Trovare a, b interi t.c. $a^3 + b^3 = 91$

$$(a+b)(a^2 - ab + b^2) = 7 \cdot 13$$

Attenzione! $\exists$ divisori negativi!

$$a^2 - ab + b^2 \geq 0$$

$$\left(a - \frac{b}{2}\right)^2 + \frac{3}{4} b^2$$

$$\begin{cases} a+b=h \\ a^2-ab+b^2=91/h \end{cases}$$

$h \mid 91$

$h = 1, 7, 13, 91$

$a = -b + h$

$$b^2 + h^2 - 2bh + b^2 - bh + b^2 = 91/h$$

$$\Delta = \frac{91 \cdot 12}{h} - 3h^2$$

$\Delta(h=13) < 0$

$\boxed{F2}$ $3^n - 1 = a^3$

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

$$\left.\begin{array}{l} a+1 \mid 3^n \\ a^2 - a + 1 \mid 3^n \end{array}\right. \begin{array}{l} \Rightarrow \\ \Rightarrow \end{array} \left\{\begin{array}{l} a+1 = 3^k \\ a^2 - a + 1 = 3^h \end{array}\right.$$

$$a = 3^k - 1$$

$$\underbrace{3^{2k} + 1 - 2 \cdot 3^k}_{a^2} + 1 - 3^k + 1 = 3^h$$

$$3^{2k} - 3 \cdot 3^k + 3 = 3^h$$

Caso antipatico: $k = 0 \to a = 0$ soluz.

$$3\left(\underbrace{3^{2k-1} - 3^k + 1}_{\equiv\, 1 \pmod 3}\right) = 3^h$$

Può essere 1! $\quad 3^{2k-1} = 3^k \iff 2k-1 = k$

$k = 1$

$(a = 2,\ n = 2)$

F3 $\frac{1}{m} + \frac{1}{n} = \frac{1}{p}$, p primo

Oss. $m > p, \quad n > p$

$$\frac{m+n}{m \cdot n} = \frac{1}{p} \iff p(m+n) = m \cdot n$$

$$m \cdot n - p \cdot m - p \cdot n + p^2 - p^2 = 0$$

$$(m-p)(n-p) = p^2$$

$m - p = 1, \quad n = p^2 + p \qquad m - p = p^2, \quad n - p = 1$

$m - p = p, \quad n - p = p$

$\boxed{F5}$ $p^n + \underset{12^2}{\underset{\parallel}{144}} = m^2$, p primo, $m \in \mathbb{N}$.

$$p^n = m^2 - 12^2 = (m+12)(m-12)$$

$$\begin{cases} m+12 = p^a \\ m-12 = p^b \end{cases}$$

$m+12 > m-12$

$\hookrightarrow a > b$

Attenzione $m - 12 = 1 \Rightarrow m = 13,\ p = 5,\ n = 2$

Per diff, $24 = p^a - p^b = p^b\left(p^{a-b} - 1\right)$

$p \mid 24 \Rightarrow p = 2$ o $p = 3$

* $p=2$ $\quad 24 = 2^b\left(2^{a-b}-1\right)$ $\quad b=3$

$3 = 2^{a-3}-1$ $\quad a=5$

$n=8, \quad m=20$

* $p=3$ $\quad b=1$ $\quad 8 = 3^{a-1}-1$ $\quad a=3$

$n=4, \quad m=15$

C6 $x_0 = 2, \quad x_{n+1} = 5 + x_n^2$

$x_1 = 9, \quad x_2 = 86, \quad x_3 = ?$

Mod 2: $\quad x_{n+1} \equiv 1 + x_n^2 \equiv 1 + x_n \pmod 2$

x_0 pari $\longrightarrow x_2, x_4, \ldots$ pari

Oss. x_n è crescente!

Mod 5 $\quad x_{n+1} \equiv x_n^2 \pmod 5$

$2, 4, 1, 1, \ldots$

Mod 3: $\quad x_{n+1} = 5 + x_n^2$

Se $x_n \not\equiv 0 \, (3) \Rightarrow x_{n+1} \equiv 5+1 \equiv 0 \pmod 3$

Anche mod 3, sono altern. $\equiv 0$, $\equiv 2$

Quelli $\equiv 0$ sono gli x_{2k+1}.

C7 $x^2 + 615 = 2^y$ x, y interi [positivi]

Se (x, y) soluz $\Leftrightarrow$ $(-x, y)$ soluz.

$2^y \geq 615$ $y > 0$

$615 = 3 \cdot 5 \cdot 41$

Mod 3: $x^2 \equiv (-1)^y \pmod 3$

x^2 e' congruo a 0 o a 1

$(-1)^y$ " " " -1 " " 1

$(-1)^y \equiv 1 \pmod 3 \Rightarrow y$ è pari

$y = 2a$

$x^2 + 615 = 2^{2a} = (2^a)^2 \qquad 2^a = z$

$(z-x)(z+x) = 615$

$\underbrace{(z-x)}_{h} + \underbrace{(z+x)}_{\frac{615}{h}} = 2z$ è una potenza di 2

Per quali $h \mid 615$ $\quad h + \frac{615}{h}$ è potenza di 2?

$h = 1, 3, 5, 41$ (o 15)

$h = 5 \qquad 5 + \frac{615}{5} = 128 = 2^7 = 2z$

$z = 2^6 \quad , \quad y = 12 \quad e \quad x = \pm 59$

C8) $a_1, \dots, a_k$ distinti in $\{1, \dots, n\}$.

$k \geq 2$ e $n \mid a_i \cdot (a_{i+1} - 1)$, $i = 1, \dots, k-1$.

Tesi: $n \nmid a_k(a_1 - 1) \iff a_1 a_k \not\equiv a_k \ (n)$

$n \mid a_1 (a_2 - 1) \iff a_1 \equiv a_1 \cdot a_2 \ (n)$

$n \mid a_2 (a_3 - 1) \iff a_2 \equiv a_2 a_3 \ (n)$

$$a_1 a_3 \equiv (a_1 \cdot a_2) \cdot a_3 \equiv a_1 (a_2 a_3) \equiv a_1 a_2 \equiv a_1 \pmod{n}$$

$$a_1 a_3 \equiv a_1 (a_3 a_4) \equiv (a_1 a_3) a_4 \overset{\text{induz}}{\equiv} a_1 a_4 \pmod{n}$$

$$\begin{array}{l} a_1 a_3 \\ \equiv \\ a_1 \end{array}$$

$$a_1 a_j \equiv a_1 a_j a_{j+1} \equiv a_1 a_{j+1} \pmod{n}$$

$$\begin{array}{l} a_1 a_j \\ \equiv \\ a_1 \end{array}$$

Cosa so? So che $a_1 a_k \equiv a_1 \pmod{n}$

Se per assurdo $a_1 a_k \equiv a_k \pmod{n}$

$\Rightarrow a_1 \equiv a_k \pmod{n}$ ASSURDO

ACHTUNG!

Con le congruenze, somma, differenza e prodotto funzionano senza problemi; ma dividere no:

$$6 \equiv 2 \pmod 4 \overset{\text{NO}}{\Longrightarrow} 3 \equiv 1 \pmod 4$$