Teoria dei Numeri 1 (BASIC)

Titolo nota 06/09/2010

$X^2 + X + 1 = y^2$ $\quad x, y$ interi positivi

Equazione diofantea

$X \longrightarrow X^2 \neq x^2 + x + 1$ (piccolo)

$(X+1) \longmapsto X^2 + 2X + 1$ (grosso)

Rappresentazioni in base

$(3\,2\,2)_{10} = 3 \cdot 10^2 + 2 \cdot 10^1 + 2 \cdot 10^0$

11

102221_3

1, 3, 9, 27, 81, 243

~~729~~

Resto $79 - 54 = 25$

(IMO) $f : \mathbb{N} \longrightarrow \mathbb{N}$ (f va dagli interi ≥ 0 agli interi ≥ 0)

$f(0) = f(1) = 0, \quad f(2n) = 2f(n) + 1,$

$f(2n+1) = 2f(n)$

f è ben definita su $\{0, 1, \ldots, n\}$

$f(m+1) = ?$

	n	$f(n)$	
0	0	0	0
1	1	0	0
10	2	1	(0)1
11	3	0	(0 0)
100	4	3	(0)11
101	5	2	(0)10
110	6	1	(0 0)1

Fissato n $\exists\, m$ t.c.

$$f^m(n) = 0$$

$n_2 = \underbrace{1\ldots}_{n \text{ cifre}}$

$f(n)$ = al più $n-1$ cifre

FORMALIZZATA?

Per induzione sul numero di cifre di n_2

- 1 cifra (verifica)
- Passo induttivo $n_2 = \underline{a_1 \dots a_k}\ \begin{matrix} 0 & (a) \\ 1 & (b) \end{matrix}$

a) $f(n) = f(2_{10}\ \underline{a_1 \dots a_k}) = 2 f(a_1 \dots a_k) \overset{+1}{=}$

$\overset{\uparrow}{=}$ ipot. induttiva $\overline{a_1}\ \overline{a_2} \dots \overline{a_k}\ 0 + 1 = \overline{a_1}\ \overline{a_2} \dots \overline{a_k}\ \overline{0}$

b) ---

DIVISIONE EUCLIDEA

$23 : 5 = 4$ resto 3 (?)

$$23 = 5 \cdot 4 + 3$$

a, b interi positivi, e $b \neq 0$, allora

$\exists!\ q, r$ t.c.

$$a = bq + r, \qquad 0 \leq r \leq b-1$$

$3 \mid 12$ ("3 divide 12")

$a \mid b \iff b = ka$ per qualche k intero

- $d \mid a,\ d \mid b \longrightarrow d \mid ka + hb$

  $a = md,\ b = nd$

  $a + b = (m+n)d$

- $d \mid a \Rightarrow |d| \leq |a|$

- $a - b \mid a^n - b^n \qquad \forall a, b, n$

$$\frac{a^n - b^n}{a-b} = a^{n-1} + a^{n-2} \cdot b + \dots + b^{n-1}$$

- $a + b \mid a^n + b^n$ (n dispari)

Def. Un numero p è primo se:

- $p = ab \rightarrow a = \pm 1$ o $b = \pm 1$ (irriduc.)
- $p \mid ab$ → $p \mid a$ / → $p \mid b$ $\left(\begin{array}{l} 5 \mid 4 \cdot \underline{5} \\ 10 \mid 8 \cdot 5 \end{array} \right)$

__Es__ $2^n - 1^n$ e' primo, allora n e' primo.

__Dim__ Diciamo che n non sia primo, $n = a \cdot b$
$a > 1$, $b > 1$

$$X - 1 \mid \underset{\underset{X}{\shortparallel}}{(2^a)}^b - 1^b \leftarrow \text{primo}$$

$X - 1 \neq 1$ $\quad 2^a \neq 2$ $\quad$ si! (perche' $a \neq 1$)

__Es__ $2^n + 1$ e' primo $\longrightarrow n = 2^k$

__Dim__ Supp. di no. Allora $\exists\, p \neq 2$, $p \mid n$

$n = pb$

$$\underbrace{2^b + 1}_{\neq 1} \mid (2^b)^p + 1^p \quad (p \text{ dispari})$$

$2^b + 1 \neq 1$; $\quad 2^b + 1 \neq 2^{bp} + 1$ (ok)

__Teo__ (Fattorizz. unica) Ogni intero > 1 si scrive in modo unico come prodotto di numeri primi

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_n^{a_n}$$

$a_1 = v_{p_1}(n)$ "Valutazione p_1-adica"

- $v_p(a \cdot b) = v_p(a) + v_p(b)$
- $v_p(a) < v_p(b) \longrightarrow v_p(a+b) = v_p(a)$

$a = p_1^{c} \cdot q \qquad b = p_1^{c} \cdot (p_1^{d} \cdot r)$

$a + b = p_1^{c} \left(\underbrace{q + r \cdot p_1^{d}}_{\text{NON è divisib. per } p_1} \right)$

MCD e mcm

Dati due numeri a, b il $MCD(a,b) = (a,b)$ è

* il max tra i d che dividono sia a che b
* un numero d t.c. $d|a$, $d|b$ e se $c|a$, $c|b$ allora $c|d$

$$a \cdot b = (a,b) \cdot mcm(a,b)$$

$$(a,b) = (a-hb, b) \quad \text{per ogni } h.$$

$$d|a,\ d|b \longrightarrow d|a-hb$$

$$d|(a-hb)+hb \longleftarrow d|a-hb,\ d|b$$

$$(20,15) = (20-15,15) = (5,15) = 5$$

$$(64,13) = \qquad 64 = 13\cdot 4 + 12$$

$$= (64-13\cdot 4, 13) = (12,13) = (12, 13-12)$$

$$= (12,1) = 1$$

(12−12, 1)

Algoritmo di Euclide

Il resto è < divisore. Il minore dei due decresce ad ogni passo.

$$(0,m) = m$$

Teorema di Bézout

Se a, b sono interi, esistono h, k t.c. $h \cdot a + k \cdot b = (a, b)$

$(a \mid b \rightarrow |a| \leq |b|)$

Dim $(23, 15) = 1$

$23 = 15 \cdot 1 + 8$

$15 = 8 \cdot 1 + 7$

$8 = 7 \cdot 1 + 1$

$7 = 7 \cdot 1 + 0$ /

$23a + 15b = 1$

$1 = 2 \cdot 23 - 3 \cdot 15$

$1 = (23 - 15) - (15 - 23 + 15)$

$1 = 8 - (15 - 8)$

$1 = 8 - 7$

In generale, $a_1, \dots, a_n$ sono interi,

$$(a_1, \dots, a_n) = h_1 a_1 + h_2 a_2 + \dots + h_n a_n$$

IMO 1959/1) $\dfrac{21n+4}{14n+3}$ è sempre irriducibile.

Sol. $(21n+4, 14n+3) = (21n+4-14n-3, 14n+3)$

$= (7n+1, 14n+3) = (14n+3-2\cdot(7n+1), 7n+1)$

$= (1, 7n+1) = 1$

Es $d_n = \mathrm{mcd}\left(n^2+100, (n+1)^2+100\right)$.

Max d_n ?

Dim $\left(n^2+2n+1+100-(n^2+100), n^2+100\right) =$

$= (\underbrace{2n+1}_{\text{dispari}}, 2(n^2+100)) = (2n^2+200-n(2n+1), 2n+1)$

$= (200-n, 2n+1) =$

$= (2n+1+2\cdot(200-n), 200-n) =$

$= (401, 200-n) \begin{matrix} \nearrow 1 \\ \searrow 401 \end{matrix}$

$n = 200$ $\qquad$ $n = 200+401$

Def. a, b si chiamano "coprimi" $(a,b) = 1$

CONGRUENZE

Fissato m, "lavoriamo mod m"

$580 \equiv 4 \quad (12) \qquad (\text{mod } 12)$

↑ "congruo"

$abcd = a\cdot 10^3 + b\cdot 10^2 + c\cdot 10^1 + d\cdot 10^0 \equiv a\cdot(1)^3 + b\cdot 1^2 + c\cdot 1 + d \quad (9)$

$a \cdot b = c \implies a\cdot b \equiv c \quad (9)$

$3x + 9y = 2 \qquad \text{mod } 3$

$0 + 0 \equiv 2 \quad (3)$ ↙ NO

IMO 2009 / 1) $a_1, \dots, a_k$ sono interi distinti presi in $\{1, \dots, n\}$ t.c. $n \mid a_i \cdot (a_{i+1} - 1)$. $i = 1, \dots, k-1$

Dim. che $n \nmid a_k (a_1 - 1)$

Dim $n \mid a_1 (a_2 - 1) \iff a_1 a_2 \equiv a_1 \quad (n) \qquad (i)$

$a_2 a_3 \equiv a_2 \quad (n) \qquad (ii)$

$\vdots$

$a_1 a_3 \overset{(i)}{\equiv} a_1 (a_2 a_3) \overset{(ii)}{\equiv} a_1 a_2 \overset{(i)}{\equiv} a_1 \quad (\text{mod } n)$

$a_1 a_4 \equiv a_1 a_3 a_4 \overset{(iii)}{\equiv} a_1 a_3 \equiv a_1$ ↙ $\cdot a_4$

Per induz., $a_1 a_m \equiv a_1 \quad (\text{mod } n) \quad m = 1, 2, \dots, k$

Tesi: $a_1 a_k \not\equiv a_k \pmod n$

Supponiamo falsa la tesi. Allora $\begin{cases} a_1 a_k \equiv a_k \ (n) \\ a_1 a_k \equiv a_1 \ (n) \end{cases}$

$a_k \equiv a_1 \ (n) \longrightarrow n \mid a_1 - a_k$

$|n| \le |a_1 - a_k| \longrightarrow a_1 = a_k$

Es $\dfrac{n^2+3n-2}{n+11}$ è intero? (*)

$$\frac{(n+11)(n-8)+86}{n+11}$$

$$\begin{array}{r|l} n^2+3n-2 & n+11 \\ n^2+11n & \hline \\ -8n-2 & n-8 \\ -8n-88 & \\ \hline 86 & \end{array}$$

SSe $86/(n+11)$ è intero

(*) $\iff n+11 \mid n^2+3n-2 \iff n^2+3n-2 \equiv 0 \ (n+11)$

$(\underbrace{n+11}_{\equiv 0} - 11)^2 + 3(\underbrace{n+11}_{\equiv 0} - 11) - 2 \equiv 0 \ (n+11)$

$11^2 - 3\cdot 11 - 2 \equiv 0 \ (n+11)$

$86 \equiv 0 \ (n+11)$

$\begin{cases} a \equiv b \pmod m \\ c \equiv d \pmod m \end{cases} \longrightarrow \begin{array}{l} a+c \equiv b+d \pmod m \\ a \cdot c \equiv b \cdot d \pmod m \end{array}$

$4 \equiv 10 \pmod 6$

$2 \equiv 5 \pmod 6$ NO!

$4 - 10 = 6k$

$2 - 5 = 3k$ $\qquad 2 \equiv 5 \ (3)$

$15 \equiv 5 \ (10)$

$3 \equiv 1 \ (2)$

$2 \equiv 24 \ (11)$ $\qquad 2 \cdot 6 \equiv 1 \ (11)$

$2 \equiv 2 \cdot 12 \ (11)$

$1 \cancel{2} \equiv \cancel{12}^{1} \cdot 12 \ (11)$

$1 \equiv 12 \ (11)$

Quando esiste l'inverso?

Fissato a, so risolvere $a \cdot x \equiv 1 \pmod m$
Se e solo se $(a, m) = 1$

Supp. che $(a, m) = 1$. $\qquad h \cdot a + k \cdot m = 1$

$$h \cdot a \equiv 1 \pmod m$$

Supp. di saper risolvere $a \cdot x \equiv 1 \ (m)$.

$$1 = a \cdot x + h \cdot m$$

$d \mid a, \ d \mid m \longrightarrow d \mid 1 \Rightarrow (a, m) = 1$

Modulo i primi? Sia p primo. a si inverte mod p $\Leftrightarrow$ $(a, p) = 1$

- a è multiplo di p, ma allora $a \equiv 0 \ (p)$
- a NON è mult. di p, e allora si inverte

$$5 \cdot 3X \equiv 1 \cdot 5 \ (7)$$

$$X \equiv 5 \ (7)$$

$$\frac{1}{2} - \frac{1}{3} \equiv \frac{1}{6} \pmod{p} \qquad p \neq 2, 3$$

$$\underset{a}{(1/2} - \underset{b}{1/3} - \underset{c}{1/6}) \equiv 0 \ (p) \iff 3 - 2 - 1 \equiv 0 \ (p)$$

$$a - b - c \equiv 0 \ (p) \iff 6(a - b - c) \equiv 0 \ (p)$$

Mod m "rapper. privilegiati" $\rightarrow \{0, 1, \dots, m-1\}$

$\rightarrow \{"-\frac{m}{2}", -\frac{m}{2}+1, \dots, 0, \dots, "+\frac{m}{2}"\}$

Mod 7 $\{0, 1, 2, \dots, 6\} \cdot 3$

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

$X \neq y \qquad 3X \equiv 3y \ (7)$ NO

$\downarrow$

$X \equiv y$

Mod m, moltiplicare per a dove $1 = (a, m)$ è una funzione biiettiva (perché è iniett.)

Questo ci dice che $\exists$ una soluz. dell'eq.

$$a \cdot X \equiv 1 \pmod{m}$$

$\downarrow$

$$a \cdot X = 1 + hm$$

$\downarrow$

d

$1 = a \cdot x - h \cdot m$ (Bézout)

$ax \equiv ay \ (m) \iff m \mid ax - ay$

$\iff m \mid a(x-y) \iff m \mid x-y$

m e a: NO FATTORI COMUNI

$\iff x \equiv y \ (m)$

Struttura moltiplicativa

$x \longmapsto ax$

$x \longmapsto x^a$??

Mod p: $\nearrow$ $x \equiv 0 \ (p)$, allora $x^1 \equiv x^2 \equiv x^n \equiv 0 \ (p)$

$\searrow$ $x^1, x^2, x^3, \dots, x^p, x^{p+1} \dots$

$\exists a, b$ t.c. $x^a \equiv x^b \ (p)$ (PIGEONHOLE) $b > a$

$(x^{-1})^a x^a \equiv (x^{-1})^a x^b \ (p)$

$1 \equiv x^{-1} \cdot x \cdot x^{-1} \cdot x \cdot \dots$ $\quad \| \| \| \quad x^{b-a} \pmod p$

Per ogni $x \not\equiv 0 \ (p)$, $\exists c > 0$ t.c. $x^c \equiv 1 \pmod p$.

Def. L'"ordine" (moltiplicativo) di x mod p

= il più piccolo $c > 0$ t.c. $x^c \equiv 1 \ (p)$

$c = \mathrm{ord}_p(x)$

Supponiamo che $x^d \equiv 1 \ (p)$. Dico che $c \mid d$.

$$\begin{cases} X^d \equiv 1 \ (p) \\ X^c \equiv 1 \ (p) \end{cases} \qquad d = K \cdot c + r, \quad 0 \le r \le c-1$$

$$X^{c\cdot K + r} \equiv 1 \ (p) \longrightarrow \underbrace{(X^c)}_{\equiv 1}{}^K \cdot X^r \equiv 1 \ (p)$$

$$\longrightarrow X^r \equiv 1 \ (p), \quad \text{con} \quad r < c \implies \boxed{r = 0}$$

Piccolo Teorema di Fermat

$$a^p \equiv a \ (p)$$

- $a \equiv 0 \ (p)$
- $a \not\equiv 0 \quad a^{p-1} \equiv 1 \ (p)$

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

$a^y \equiv 1 \ (p)$

$\text{ord}_p(a) \mid y$

Dim 1. Per induzione su a.

$* \ a = 0, \ a = 1$

$$* \ (a+1)^p \equiv \sum_{n=0}^{p} \binom{p}{n} a^n \equiv \binom{p}{0} a^0 + \binom{p}{p} a^p$$

$$\binom{p}{1}, \binom{p}{2}, \dots, \binom{p}{p-1} \equiv 0 \ (p)$$

$$\frac{p!}{n!(p-n)!} \quad \begin{matrix} \leftarrow 1 \text{ fattore } p \\ \leftarrow \text{no fattori } p \end{matrix}$$

$$\overset{\text{ip. ind.}}{\equiv} 1 + a \pmod p$$

2. $\{1, 2, \dots, p-1\}$ $\qquad \{a, 2a, 3a, \dots, (p-1)a\}$

permutazione di $\{1, 2, \dots, p-1\}$

perché $(a, p) = 1$.

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \equiv a \cdot 2a \cdot 3a \cdot \dots \cdot (p-1)a \ (p)$$

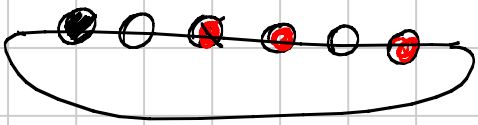
$$(p-1)! \equiv a^{p-1} \cdot (p-1)! \pmod p$$

$(p-1)! \not\equiv 0 \ (p)$

$1 \equiv a^{p-1} \pmod p$

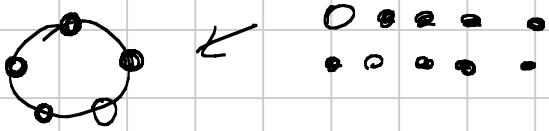
$a \equiv a^p \pmod p$

3. Collane con p perline di a colori

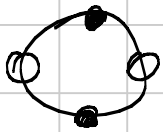


Collane aperte $= a^p$

* Collana monocromatica ($\to$ sono a)
* " non monocrom. ($\to$ sono $a^p - a$) APERTE



Sono $\dfrac{a^p - a}{p}$.



Se ruotandola di d scatti torna uguale, anche $2d$, $3d$... $kd = p \to d \mid p \to \begin{cases} d=1 \\ d=p \end{cases}$

$\dfrac{a^p - a}{p}$ collane non mon. chiuse

$\dfrac{a^p - a}{p}$ intero $\iff p \mid a^p - a \iff a^p - a \equiv 0 \ (p)$ ∎

Teo. Wilson $(p-1)! \equiv -1 \pmod p$

Mod 7 $\quad 1 \cdot \textcircled{2} \cdot \textcircled{3} \cdot \textcircled{4} \cdot \textcircled{5} \cdot 6$

Mod p $\quad 1 \cdot \underbrace{2 \cdot 3 \cdot \ldots \cdot (p-2)}_{1} \ (p-1) \equiv -1 \ (p)$

1 e -1 sono gli unici numeri t.c. $a^{-1} \equiv a \ (p)$

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

$a+1 \equiv 0 (p) \qquad a-1 \equiv 0 (p)$

Es $\{ p^4 - q^4 \}$ con p, q primi di almeno 2 cifre

$p, q > 10$

Quanto è mcd di tutti?

Svolg. $a = \nearrow$. Quali fattori primi ha a?

Dico che in a NON compaiono primi > 10.
Diciamo che $r \mid a$, $r \geq 10$, primo.

$a \mid r, \ a \mid p^4 - r^4 \longrightarrow a \mid p^4 \quad \forall p$

$\longrightarrow a = 1$ (No)

$p^4 - q^4 \equiv 0 \ (2) \longrightarrow 2 \mid a \quad (a \geq 2)$

$p^4 - q^4 \equiv (p^2)^2 - (q^2)^2 \overset{FLT}{\equiv} 1^2 - 1^2 \equiv 0 \ (3)$

$a^{p-1} \equiv 1 \ (p) \qquad a^2 \equiv 1 \ (3)$

$p^4 - q^4 \overset{FLT}{\equiv} 1 - 1 \equiv 0 \ (5)$

$13^4 - 11^4 = 3 \cdot 5 \cdot 29 \cdot 2^5$ (7 NON c'è)

$p^4 - q^4 \equiv 0 \ (2^4) \qquad p^4 \equiv 1 \ (16)$

$p^2 \equiv 1 \ (8) \qquad 1^2 \equiv 1 \ (8) \quad 5^2 \equiv (-3)^2 \equiv 9 \equiv 1 \ (8)$

$3^2 \equiv 1 (8) \quad 7^2 \equiv (-1)^2 \equiv 1 \ (8)$

$$p^2 = 1 + 8k \Rightarrow p^4 = (1+8k)^2 =$$
$$= 1 + 16k + 64k^2 \equiv 1 \ (16)$$

$17^4 - 11^4 = 2^4 \cdot$ dispari

$a = 2^4 \cdot 3 \cdot 5$

Residui quadratici. Quando è che $x^2 \equiv a$ ha soluzioni mod p?

3 è $\sqrt{2}$ mod 7 $\qquad 3^2 \equiv 2 \ (7)$

$x^2 \equiv 6 \ (7)$ $\qquad 4^2 \equiv (-3)^2 \equiv 2 \ (7)$

$5^2 \equiv (-1)^2 \equiv 1 \ (7)$

Mod 3: $x^2 \to 0 \quad (x \equiv 0)$
$\quad\ \ \to 1 \quad (x \not\equiv 0)$

$$3x^2 + 2 = y^2$$
$$\downarrow$$
$$2 \equiv y^2 \ (3) \qquad \text{IMPOSSIBILE}$$

Mod 4: $0^2 \equiv 0, \ 2^2 \equiv 0$
$1^2 \equiv 1, \ 3^2 \equiv 1 \qquad (\text{mod } 4)$

$\exists$ 2006 2006 ... 2006 che siano quadrati?
(111)

$06 \equiv 2 \ (4)$

Mod 8: $0^2 \equiv 0, \ 2^2 \equiv 4, \ 4^2 \equiv 0, \ 6^2 \equiv 4 \qquad (8)$

$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \ (8)$

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

$a^2 \equiv b^2 \pmod m$

$\downarrow ?$

$a \equiv \pm b$

$a^2 \equiv b^2 \pmod p \iff (a-b)(a+b) \equiv 0 \ (p)$

$\Updownarrow$

$p \mid a-b$ ↙ ↘ $p \mid a+b$

$a \equiv b \ (p)$ $\quad$ $a \equiv -b \ (p)$

Corollario: mod p ci sono $\frac{p-1}{2} + 1$ residui quad.

$\frac{p-1}{2}$: accoppiati $a \leftrightarrow -a$

$+1$: 0

Es. $15x^2 - 7y^2 = 9$ $\quad$ x, y interi posit.

Dim $\quad -7y^2 \equiv 0 \ (3) \rightarrow y^2 \equiv 0 \ (3) \rightarrow 3 \mid y$

$y^2 \equiv 0 \ (9) \not\Rightarrow 9 \mid y$

$y = 3k. \quad 15x^2 - 7 \cdot 9 \cdot k^2 = 9$

$5x^2 - 21k^2 = 3$

La legge mod 3 $\rightarrow 5x^2 \equiv 0 \ (3) \rightarrow 3 \mid x$

$x = 3a \quad 5 \cdot 9 \cdot a^2 - 21k^2 = 3$

$15a^2 - 7k^2 = 1$

$-7k^2 \equiv 1 \ (3)$

$-k^2 \equiv 1 \ (3) \rightarrow k^2 \equiv 2 \ (3)$ $\quad$ IMPOSS.

Cubi mod 7

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

) elevo al cubo

$$X^3 + 2 = 7y^5$$

Leggo mod 7 $\quad X^3 + 2 \equiv 0 \ (7)$

$X^3 \equiv 5 \ (7)$ $\quad$ NO

Mod 9 : $0, 1, -1$ / $0, 1, -1$ / $0, 1, -1$

$(a+3)^3 \equiv a^3 + 3a^2 \cdot 3 + 3 \cdot 9 \cdot a + 27$

$\equiv a^3 \ (9)$

Quarte potenze : 0 o 1 mod 16

$4^a + 4^b + 4^c = \text{un quadrato} = q^2$

1) ξ^c simmetrica in $a, b, c \longrightarrow a \le b \le c$

2) $\underbrace{4^a}_{\text{quadr.}} \cdot \underbrace{\left(1 + 4^{b-a} + 4^{c-a}\right)}_{\longrightarrow \text{quadrato}} = q^2$

$= q^2 / 2^{2a} = (q/2^a)^2$

3) $1 + 4^x + 4^y = z^2 \qquad (x \le y)$

$4^x \left(1 + 4^{y-x}\right) = z^2 - 1 = (z+1)(z-1)$

$\gcd\left(4^x, 1 + 4^{y-x}\right) = 2^e \longrightarrow 1 + 4^{y-x}$ è pari

$\longrightarrow 1 + 4^{y-x} \equiv 1 \ (2)$

- $y = x$ (Se $x = 0$, $1 + 1 + 4^y = z^2$

$2 + 2^{2y} = z^2$)

- $\gcd = 1$

Se $\gcd = 1$,

Ricaviamo che $z = 2k + 1$

$4^{x-1}\left(1 + 4^{y-x}\right) = 4k(k+1)$

$2^{2x-2} \cdot \left(1 + 4^{y-x}\right)$

Dico che serve $1 + 4^{y-x} \ge 4^{x-1} - 1$.

$4^{x-1} = k \qquad 1 + 4^{y-x} = k + 1$

$1 + 4^{y-x} \ge 4^{x-1}$

$$2 + 4^{y-x} \geq 4^{x-1} \rightarrow \begin{cases} x = 1 \\ y \geq 2x-1 \end{cases}$$

$y = 2x-1$

$$1 + 4^x + 4^y =$$

$$= 1 + 4^x + \frac{1}{4} 4^{2x} =$$

$$= \left(1 + 2 \cdot 2^{2x-1} + 2^{4x-2}\right)$$

$$= \left(1 + 2^{2x-1}\right)^2$$

$y > 2x-1$ $\quad 1 + 4^x + 4^y < \left(2^y + 1\right)^2$

$(2^y)^2$

$$1 + 4^x + 4^y < 1 + 4^y + 2 \cdot 2^y$$

$$2^{2x} < 2^{y+1}$$

Probl. (Cese 1995/6) $x^2 + 615 = 2^y$

Dim. $x^2 \equiv 2^y \pmod 3$

Può essere $x \equiv 0 \ (3)$? No

$1 \equiv 2^y \ (3)$ $\quad$ $1 \equiv (-1)^y \ (3)$

y è pari! $\quad$ $2^y = 2^{2z} = a^2$

$a^2 - x^2 = 615$ $\quad$ $x = 59, \ y = \dots$

$(a-x)(a+x)$

$2a = (a-x) + (a+x)$

Prob (Cesenatico 1994/2) $y^2 = x^3 + 16$

$y^2 - 16 = x^3$

Dim

$$(y+4)(y-4) = x^3$$

- y dispari

$$(y+4, y-4) = (8, y+4) = 1$$

Allora, siccome sono coprimi, sono entrambi cubi:

$$y+4 = a^3, \quad y-4 = b^3$$

$$a^3 - b^3 = 8$$

$$(a-b)(a^2+ab+b^2) = 8$$

↑ potenze di 2 ↗

$a - b = 1$ $\quad (b+1)^3 - b^3 = 8$ no

$a - b \geq 2$ $\quad a^3 = (b+2)^3 > b^3 + 8$

$8 = a^3 - b^3 > 8$ no

- y pari $\quad y^2 = x^3 + 16$

Mod 2: x è pari

Mod 8: $y^2 \equiv x^3 \equiv 0 \ (8) \longrightarrow \underline{y \equiv 0 \ (4)}$

$y = 4k$

$$16(k^2 - 1) = x^3$$

$4 + v_2(k^2-1) = v_2(x^3) = 3\, v_2(x)$

↳ k è dispari $= 2m+1$

$16 \cdot 2m \cdot 2 \cdot (m+1) = x^3$

$64\, m(m+1) = x^3$

cubo

$\downarrow$

$m(m+1)$ è un cubo

$m=0,\ x=1,\ y=4 \longrightarrow x=0$

IMO 2006/4) Risolvere $1 + 2^x + 2^{2x+1} = y^2$ negli interi ≥ 0

$x=0 \rightarrow y=2$ ✓

Sol. $1 \equiv y^2 \pmod{2^x}$

$\Downarrow$

$2^x \mid (y+1)(y-1)$ $\qquad \gcd(y+1, y-1) = 2$

$\Downarrow$

$(2, y-1)$

$y \equiv \pm 1 \pmod{2^{x-1}}$

Quanto sarà grosso y? • $y \geq 3 \cdot 2^{x-1}$

$y^2 \geq 9 \cdot 2^{2x-2} = 2^{2x+1} + 2^{2x-2} \overset{?}{=} 2^{2x+1} + 2^x + 1$

$9 = 1 + 2^3$

Se $x \geq 3$, LHS > RHS $\qquad x = 0, 1, 2$

• $y \leq 2^{x-1}$ $\qquad y^2 = 2^{2x-2} < 2^{2x+1} + 2^x + 1$ No

Quindi: o $\quad y = 2^{x-1} + 1,\ 2 \cdot 2^{x-1} \pm 1,$

$3 \cdot 2^{x-1} - 1$

Test iniziale 13.

x, y interi, $y > x$, $11x + 7y = 2010$

$\min (y - x)$.

$2 \cdot 11 - 7 \cdot 3 = 1$

$2 \cdot 2010 = x_0$

$-3 \cdot 2010 = y_0$

$x = x_0 + a, \quad y = y_0 + b$

$11 x_0 + 11a + 7y_0 + 7b = 2010$

$11a + 7b = 0$

$a = -7k$

$b = +11k$ $\quad k$ intero

$-3 \cdot 2010 + 11k - 2 \cdot 2010 + 7k = y - x$

$-5 \cdot 2010 + 18k = y - x \equiv -5 \cdot 2010 \pmod{18}$

$\equiv -150 \equiv 30 \equiv 12 \pmod{18}$