Titolo nota: N1 basic (Edriv) — 08/09/2009

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}$

$\mathbb{N} = 0, 1, 2, 3, \dots$?

$1, 2, 3, \dots$

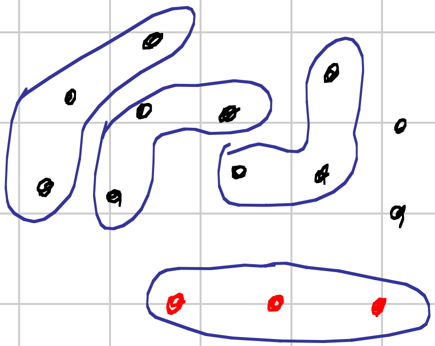
$\mathbb{Z} = \dots, -1, 0, 1, \dots$

positivi vuol dire > 0

NOTAZIONE POSIZIONALE

$$\underline{4\ 7\ 2\ 6} = 4\cdot\underbrace{1000}_{10^3} + 7\cdot\underbrace{100}_{10^2} + 2\cdot\underbrace{10}_{10^1} + 6\cdot\underbrace{1}_{10^0}$$

in base 11? $4\cdot 11^3 + 7\cdot 11^2 + \dots$



102 in base 3

CESENATICO 3:

numero $n = \cancel{aabb}\ abab$

$(ab)^2 \mid n^2$

IMPOSTAZIONE

$0 \leq a, b \leq 9$

$$n = a \cdot 1000 + b \cdot 100 + a \cdot 10 + b$$
$$= 1010a + 101 b$$
$$= 101(10a+b)$$

$$(ab)^2 \mid [101(10a+b)]^2$$

$x^{\cancel{2}} \mid y^{\cancel{2}}$ perché?

$x^n \mid y^n \iff x \mid y$

dimostraz. dopo

IMO 1988/3

$f : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$

- $f(1) = 1$
- $f(3) = 3$
- $f(2n) = f(n)$
- $f(4n+1) = 2f(2n+1) - f(n)$
- $f(4n+3) = 3f(2n+1) - 2f(n)$

Trovare le soluzioni di $f(n) = n$ per $n \leq 1988$

IDEA: scrivere tutti i numeri in binario

m, che in binario si scrive ∼∼∼
$f(∼∼∼\,0) = f(∼∼∼)$

DIVISIBILITÁ

$a, b \in \mathbb{Z}$

$a \mid b$ a divide b
b é multiplo di a

$\exists\, k \in \mathbb{Z}$ t.c. $b = ka$

$a \mid 0 \quad \forall a$

i divisori di 1 sono $+1$, -1

PROPRIETÀ

- $a \mid b \qquad b \mid c \longrightarrow a \mid c$

  $b = ka \qquad c = jb \qquad c = (jk)a$

- $a \mid b \qquad b \mid a \longrightarrow a = b \ \vee \ a = -b$

  $b = ka \qquad a = jb \longrightarrow a = (jk)a$

  $jk = 1$

- $a \mid b \longrightarrow |a| \leq |b|$

  $2 \mid -6$

- $a \mid b \qquad a \mid c \longrightarrow$
  - $a \mid b + c$
  - $a \mid b - c$
  - $a \mid 15b - 70!\,c$
  - $a \mid kb + jc \quad \forall k, j \in \mathbb{Z}$

caso particolare: $a \mid b \longrightarrow a \mid b + ka$

- $\underline{a + b} + c = \underline{d + e}$ se a, b, d, e sono multipli di k

  $\hookrightarrow$ anche c lo è

DIVISIBILITÁ PARTICOLARI

$a-b \mid a^n - b^n$

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \dots + b^{n-1})$$

$a+b \mid a^{2n+1} + b^{2n+1}$

$2^n - 1$ numero primo $\Longrightarrow$ n é primo

$n = ab \rightarrow 2^{ab} - 1$ é divisibile per $2^a - 1 > 1$

$2^n + 1$ numero primo $\Longrightarrow$ n é potenza di 2

se n é dispari : $2+1 \mid 2^n + 1 \longrightarrow n = 1$

se $d \mid n$ e d é dispari $\quad n = a \cdot d$

$$2^n + 1 = 2^{a \cdot d} + 1 = (2^a)^d + 1^d$$

divisibile per $2^a + 1$

se $d \mid e$ allora $a^d - b^d \mid a^e - b^e$

$e = kd$ $\quad (a^d)^k - (b^d)^k$

se $d \mid e$ e sono entrambi dispari $a^d + b^d \mid a^e + b^e$

MCD, mcm, e come si trovano

NOTAZIONE

MCD di a, b $\quad d = (a, b) \longrightarrow MCD(a,b)$

Massimo Comun divisore

$d \mid a$, $d \mid b$,

per ogni e t.c. $e \mid a$, $e \mid b$ $\quad e \leq d$

$e \mid d$

mcm = minimo comune multiplo ~~tale~~

$$d = [a, b]$$

$a \mid d$, $b \mid d$ e per ogni $e \in \mathbb{Z}$ t.c. $a \mid e$, $b \mid e$

si ha $d \mid e$

$\mathrm{MCD}(a, b) = ?$

$d \mid a \wedge d \mid b \longrightarrow d \mid a-b$

$d \mid b \wedge d \mid a-b \longrightarrow d \mid a$

$$\boxed{\begin{aligned} \mathrm{MCD}(a, b) &= \mathrm{MCD}(a, a-b) \\ &= \mathrm{MCD}(a, b+ka) \end{aligned}} \qquad k \in \mathbb{Z}$$

Euclide deve trovare $\mathrm{MCD}(13, 8)$

$$= \mathrm{MCD}(13-8, 8) = \mathrm{MCD}(5, 8)$$

$$= \mathrm{MCD}(5, 3) = \mathrm{MCD}(2, 3) = \mathrm{MCD}(2, 1) = 1$$

$MCD(100, 11) = MCD(100 - 9 \cdot 11, 11) = MCD(1, 11) = 1$

$$\boxed{\text{def.} \quad MCD(a,b) = 1 \quad a,b \text{ primi tra loro / coprimi}}$$

TEOREMA DI BEZOUT

$MCD(a,b) = d \implies \exists\, j,k \in \mathbb{Z} : \quad d = ja + kb$

Conseguenza: se $\boxed{(a,b) = 1}$ $\boxed{ja + kb = 1}$ per qualche j,k

Come trovare j,k?

$MCD(49, 13) = MCD(49 - 3 \cdot 13, 13) = MCD(10, 13) =$

$= MCD(10, 13 - 10) = MCD(10, 3) = MCD(10 - 3 \cdot 3, 3) = MCD(1, 3) = 1$

trovare j,k $\quad 49j + 13k = 1$

$10 - 3 \cdot 3 = 1$

$10 - 3 \cdot (13 - 10) = 1 \qquad 4 \cdot 10 - 3 \cdot 13 = 1$

$4 \cdot (49 - 3 \cdot 13) - 3 \cdot 13 = 1$

$\boxed{4 \cdot 49 - 15 \cdot 13 = 1}$

IMO 1992 / 1

TECNICHE IN TDN
- divisibilità, fattori, congruenze
- disuguaglianze

a, b, c interi $\quad 1 < a < b < c$

$$(a-1)(b-1)(c-1) \mid abc - 1$$

II casi:

I $\quad (a-1)(b-1)(c-1) = abc - 1$

$\cancel{abc} - ab - bc - ca + a + b + c \cancel{-1} = \cancel{abc} \cancel{-1}$

$ab + bc + ca = a + b + c$

$ab > a$

$ca > c$

$bc > b$ $\qquad$ impox.

II $\quad 2(a-1)(b-1)(c-1) \leq abc - 1$

$$2abc - 2ab - 2bc - 2ca + 2(a+b+c) - 2 \le abc - 1$$

$$abc + \underbrace{2(a+b+c)} \le 2(ab+bc+ca) + \underbrace{1}$$

$$abc \le 2(ab+bc+ca)$$

$$\frac{1}{3} abc \ge 2ab \qquad c \ge 6$$

$$\frac{1}{3} abc \ge 2bc \qquad b \ge 6$$

$$\frac{1}{3} abc \ge 2ca \qquad a \ge 6$$

se $a, b, c \ge 6$ allora $abc \ge 2(ab+bc+ca)$

quindi $a = b = c = 6$ ... non va bene

andate avanti voi

IMO 1959/1

Dimostrare che $\dfrac{21n+4}{14n+3}$ é irriducibile $\forall n \in \mathbb{N}$

Dovrei dimostrare che $MCD(21n+4, 14n+3) = 1$

$$(21n+4, 14n+3) = (7n+1, 14n+3) = (7n+1, 1) = 1$$

$\square$

$\dfrac{n^2+3n-2}{n+11} \in \mathbb{Z}$ $\qquad n+11 \mid n^2+3n-2$

$$n+11 \mid n^2+3n-2 - n\cdot(n+11)$$
$$n+11 \mid -8n-2 + 8(n+11)$$
$$n+11 \mid 86$$

divisori di 86? $\quad 43 \cdot 2$

$\pm 1, \pm 2, \pm 43, \pm 2 \cdot 43$

8 soluzioni in $\mathbb{Z}$

$$\mathrm{MCD}(100+n^2,\ 100+(n+1)^2) = d_n$$

trovare $\max d_n$

$$\mathrm{MCD}(100+n^2,\ 100+n^2+2n+1) = \mathrm{MCD}(100+n^2,\ 2n+1)$$

$d \mid 100+n^2$ e $\underline{d \mid 2n+1}$

$d \mid 2\cdot(100+n^2) - n(2n+1) = \underline{200-n}$

$d \mid (2n+1) + 2\cdot(200-n) = 401$

quindi $\mathrm{MCD}(100+n^2,\ 100+(n+1)^2) \mid 401$

devo trovare un n per cui $401 \mid 100+n^2$ e $401 \mid 100+(n+1)^2$

$401 \mid 200-n$ $\quad 200-n = 401k$

$n = 200-401k$

provo $k=0$ $\quad n=200$ funziona $\square$

NUMERI PRIMI

p é primo se non si può scrivere come

$$p = ab \quad \text{dove } a>1 \text{ e } b>1.$$

inoltre 1 non é primo

LEMMA DI EUCLIDE

$$p \mid ab \implies p \mid a \ \vee \ p \mid b$$

supponiamo che $p \nmid a$

consideriamo $MCD(p, a) = 1$

$$kp + ja = 1 \quad \text{per } j, k \in \mathbb{Z}$$

$p \mid ab$

$p \mid jab$

$p \mid (1-kp)b$

$p \mid b - kpb$

$p \mid b$

TH. FONDAMENTALE DELL' ARITMETICA

ogni ~~nume~~ naturale si scrive in modo unico come prodotto di numeri primi.

1. (esistenza)

per induzione. n: se é primo, ok

se $n = ab$

2. (unicitá)

$p_1 p_2 \cdots p_j = q_1 q_2 \cdots q_k$ $\quad p_i, q_i$ primi

posso supporre che $p_i \neq q_j \quad \forall i, j$

$p_1 \mid q_1 \cdots q_k \longrightarrow$ esiste i t.c. $p_1 \mid q_i \quad p_1 = q_i$ assurdo

CONSEGUENZE

- é piú facile calcolare MCD, mcm

$3^3 \cdot 5^7 \cdot 11^2, \qquad 3^2 \cdot 5^3 \cdot 11^{20}$

$MCD = 3^2 \cdot 5^3 \cdot 11^2$

per ogni primo, prendo l'esponente piú basso

- calcolare l'mcm?

  scompongo tutti, e cerco il max esponente.

- n é una k-potenza perfetta

  se nella scomposizione in primi, ogni esponente é multiplo di k.

VALUTAZIONE p-ADICA

$n \in \mathbb{Z}$ p primo

con quale esponente compare p nella fattorizzazione di n?

$$\boxed{v_p(n)}$$

$v_2(84) = 2$ perché $2^2 \mid 84$ ma $2^3 \nmid 84$

2^2 divide esattamente 84

$2^2 \parallel 84$ $7 \parallel 84$

PROPRIETÁ

$$\nu_p(a \cdot b) = \nu_p(a) + \nu_p(b)\,,$$ come il logaritmo

$$p \mid a \iff \nu_p(a) > 0$$

$$\nu_p(a+b)\ ?$$

se $\nu_p(a) \neq \nu_p(b)$ allora $\nu_p(a+b) = \mathrm{MIN}\{\nu_p(a), \nu_p(b)\}$

altrimenti, se $\nu_p(a) = \nu_p(b)$ allora $\nu_p(a+b) \geq \nu_p(a)$

come si calcola $\nu_p(n!)$

$\nu_{41}(2009!)$ $\quad 1 \cdot 2 \cdot 3 \cdot \ \ldots \ \cdot 2009$

i multipli di 41 sono $\left\lfloor \frac{2009}{41} \right\rfloor$ ✓

i multipli di 41^2 sono $\left\lfloor \frac{2009}{41^2} \right\rfloor$

$$\nu_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

$$\left\lfloor \frac{2009}{41} \right\rfloor = 49 \qquad \left\lfloor \frac{2009}{41^2} \right\rfloor = 1$$

$$\nu_{\cancel{p}41}(2009!) = 49 + 1 = 50$$

NUMERO DI DIVISORI

quanti divisori ha 72?

$72 = 2^3 \cdot 3^2$

$2^a \cdot 3^b$ $\quad$ a varia tra 0 e 3

b varia tra 0 e 2

$4 \cdot 3 = 12$ divisori POSITIVI

in generale $\quad p_1^{e_1} \, p_2^{e_2} \cdots p_k^{e_k}$

ha $\quad (e_1+1)(e_2+1) \cdots (e_k+1)$ divisori $= \tau(n)$

conseguenza: il numero di divisori di n é dispari se e solo se ...

... $n = k^2$

CONGRUENZE

ovvero "MODULO n"

$\boxed{7 = 0}$

$8 = 1$

$14 = 0$

$11 = -3$

$1 = 0$ $\quad$ $2 = 0$

quali numeri sono "uguali" a 7

$\longrightarrow$ tutti i multipli di 7

quali numeri sono "uguali" a 1 ?

$\longrightarrow$ quelli della forma $7k+1$

dividiamo $\mathbb{Z}$ in 7 classi:

$7k+0$, $7k+1$, $\dots$, $7k+6$

cosa vuol dire guardare gli interi "modulo n"?

due numeri a, b sono congruenti se $a = b + kn$

se $n \mid a-b$

se hanno lo stesso resto per n

e si scrive $a \equiv b \pmod{n}$

$$\begin{cases} a \equiv a & \text{perché } n \mid a-a = 0 \\ a \equiv b \text{ e } b \equiv c \text{ allora } a \equiv c & \text{perché } n \mid a-b \text{ e } n \mid b-c \text{ allora } n \mid a-c \\ a \equiv b \longrightarrow b \equiv a & \end{cases}$$

SOMMA

es. lavoro modulo 7

$cl(12) + cl(15) = cl(27)$

$cl(12) = cl(5)$

$cl(15) = cl(8) = cl(1)$

VALE QUESTA PROPRIETÁ:

se $a \equiv b \pmod n$ e $c \equiv d \pmod n$

allora $a + c \equiv b + d \pmod n$.

PRODOTTO

se $a \equiv b \pmod n$ e $c \equiv d \pmod n$

allora $a \cdot c \equiv b \cdot d \pmod n$

~~$69200920092009 2009$ é un quadrato perfetto?~~

ALCUNI CRITERI DI CONGRUENZA

per 2: basta guardare l'ultima cifra

pari $\longrightarrow$ $0 \mod 2$

dispari $\longrightarrow$ $1 \mod 2$

per 3: $4726 = 4 \cdot 10^3 + 7 \cdot 10^2 + 2 \cdot 10^1 + 6$

$10 \equiv 1 \pmod 3$ $\qquad \equiv 4 \cdot 1^3 + 7 \cdot 1^2 + 2 \cdot 1 + 6 \pmod 3$

$10^2 \equiv 1^2 \equiv 1 \pmod 3$

$10^n \equiv 1 \pmod 3$

un numero é congruo alla somma delle sue cifre modulo 3.

per 4: $4726 = \cancel{47 \cdot 100} + 26 \equiv 2 \pmod 4$

basta guardare il numero formato delle ultime 2 cifre.

per 2^n: bastano le ultime n cifre

per 5: conta l'ultima cifra

per 5^n: contano le ultime n cifre

per 6: $6 = 2 \cdot 3$ teorema cinese del resto, vedi dopo.

per 9: visto che $10 \equiv 1 \pmod 9$

$$4726 = 4 \cdot 10^3 + 7 \cdot 10^2 + 2 \cdot 10 + 6$$

$$\equiv 4 + 7 + 2 + 6 \pmod 9$$

é congruo alla somma delle cifre

per 10: é l'ultima cifra

per 10^n: le ultime n cifre

per 11: $10 \equiv -1 \pmod{11}$

$$4726 = 4 \cdot 10^3 + 7 \cdot 10^2 + 2 \cdot 10 + 6$$
$$\equiv 4 \cdot (-1)^3 + 7 \cdot (-1)^2 + 2 \cdot (-1) + 6$$
$$= -4 + 7 - 2 + 6$$

é data dalla somma a segni alterni delle cifre.

$$69\,2009\,2009\,2009\,2009 = n^2 \quad ?$$

mod 3: é congruo a 2.

Se n é $\equiv 0 \bmod 3$, $n^2 \equiv 0$

Se n é $\equiv 1 \pmod 3$, $n^2 \equiv 1$

se n é $\equiv 2 \pmod 3$, $n^2 \equiv 4 \equiv 1 \bmod 3$

QUADRATI MODULO M

~~•~~ consideriamo modulo p primo.

$p=7$ $\qquad m = 0, 1, 2, 3, 4, 5, 6$

$\qquad\qquad m^2 = 0, 1, 4, 2, 2, 4, 1$

in generale, modulo p ci sono $\frac{p+1}{2}$ "residui quadratici".

$a^2 = (-a)^2$

$a^2 \equiv b^2 \pmod p$ allora $p \mid a^2 - b^2 \to p \mid (a+b)(a-b)$

$\to a \equiv b$ o $a \equiv -b$

ES. risolvere $15x^2 - 7y^2 = 9$ fattori 3

quindi $3 \mid 7y^2$ quindi $3 \mid y^2 = y \cdot y$ quindi $3 \mid y$

$y = 3y'$

risolvere $15x^2 - 7(3y')^2 = 9$

$15x^2 - 7\cdot 3^2 \cdot y'^2 = 9$

$5x^2 - 7\cdot 3 \cdot y'^2 = 3$

quindi $3 \mid 5x^2 \longrightarrow 3 \mid x$ $\qquad x = 3x'$

risolvere $5(3x')^2 - 7\cdot 3\cdot y'^2 = 3$

$15x'^2 - 7y'^2 = 1$

guardo modulo 3

$\cancel{15x'^2} - 7y'^2 \equiv 1 \pmod 3$

$-y'^2 \equiv 1 \pmod 3$

$y'^2 \equiv -1 \pmod 3$

IMPOSSIBILE.

Se ho un'uguaglianza: $3^n + 1 = 2^n$

una volta che guardo modulo k, resta vera modulo k

UGUAGLIANZA VERA $\longrightarrow$ CONGRUENZA VERA

CONGRUENZA FALSA $\longrightarrow$ UGUAGLIANZA FALSA

DIVISIONI modulo n.

INVERSO DI UN NUMERO

esiste "1/5" modulo 13 ?

$a \cdot 5 \equiv 1 \pmod{13}$ ha soluzione?

$8 \cdot 5 = 40 \equiv 1 \pmod{13}$

5 ha un inverso

$a \cdot 26 \equiv 1 \pmod{13}$ ha soluzione?

NO

~~CASO GENERALE (mod n)~~

$a \cdot 8 \equiv 1 \pmod{12}$ ha soluzione?

NO

CASO GENERALE

$$a \cdot x \equiv 1 \pmod{n} \qquad n \mid ax-1$$

1. Se $(x,n) = d > 1$ $\qquad d \mid ax-1$, ma $d \mid x$, quindi $d \mid 1$, assurdo.

quindi: se $(x,n) > 1$, x NON é invertibile

$$3a \equiv 3b \pmod{6}$$
$$\cancel{a \equiv b \pmod{6}} \qquad \text{NO!!!}$$

ad es. $2 \not\equiv 4$ peró $3 \cdot 2 \equiv 3 \cdot 4 \pmod{6}$

2. Se $(x,n) = 1$ $\qquad kx + jn = 1$ per Bézout

$$kx + 0 \equiv 1 \pmod{n}$$

x é invertibile!!!

es. $\qquad a \cdot 5 \equiv 1 \pmod{13}$

$$MCD(13, 5) = (13 - 2\cdot 5, 5) = (3, 5) = (3, 5-3) =$$

$$= (3, 2) = (3-2, 2) = (1, 2) = 1$$

$3 - 2 = 1$

$3 - (5-3) = 1 \qquad 2\cdot 3 - 5 = 1 \qquad 2\cdot(13 - 2\cdot 5) - 5 = 1$

$2\cdot 13 - 5\cdot 5 = 1$

mod 13: $\quad (-5)\cdot 5 \equiv 1$

$8 \cdot 5 \equiv 1$

$$476a \equiv 476b \pmod{101}$$

$$\downarrow$$

$$a \equiv b \pmod{101}$$

OK ✓ (perché $(476, 101) = 1$)

RESIDUI QUADRATICI

mod 3 $\longrightarrow$ 0, 1

mod 5 $\longrightarrow$ 0, 1, 4

mod 7 $\longrightarrow$ 0, 1, 2, 4

mod 8 $\longrightarrow$ 0, 1, 4 perché?

- i pari mi danno 0 o 4
- n dispari: $n = 2k+1$ $\quad n^2 = 4k^2 + 4k + 1$

$$= \underbrace{4k(k+1)}_{\text{mul. di } 8} + 1 = 8z+1$$

risolvere $y^2 = x^5 - 4$.

guardando mod 11:

$y^2 = 0, 1, 4, 9, 5, 3,$ mod 11

$x^5 = 0, 1, -1$

non ha soluzioni.

IMO 2009 / 1 $\quad a_1, \dots, a_k \overset{\text{distinti}}{\in} \{1, \dots, n\} \quad k > 1$

$\forall i = 1, \dots, k \quad n \mid a_i (a_{i+1} - 1) \qquad (a_{k+1}$ è $a_1)$

Th: è impossibile.

$a_i(a_{i+1} - 1) \equiv 0 \pmod n$

$a_i a_{i+1} \equiv a_i \pmod n$

$$\begin{cases} a_1 \equiv a_1 a_2 \\ a_2 \equiv a_2 a_3 \\ a_3 \equiv a_3 a_4 \\ \vdots \\ a_k \equiv a_k a_1 \end{cases}$$

$a_1 \equiv a_1 a_2 \equiv a_1 (a_2 a_3) \equiv a_1 a_2 a_3 \equiv a_1 a_2 (a_3 a_4) \equiv$

$\equiv a_1 a_2 a_3 a_4 \equiv \dots \equiv a_1 a_2 a_3 a_4 a_5 \equiv \dots$

$\dots \equiv \dots \equiv \dots \equiv a_1 a_2 a_3 \cdots a_k a_1$

$a_1 \equiv a_1 (a_1 a_2 \cdots a_k) \mod n$

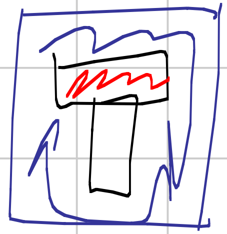
$n \mid a_1 (a_1 a_2 \cdots a_k - 1)$

OSS. $\text{MCD}(a_1, \; a_1 \cdots a_{k-1}) = 1$

IN GENERALE:

se $n \mid ab$ e $(n, a) = 1$

allora $n \mid b$



$a_1 \equiv a_1 \cdots a_{k-1}$ *

$a_1 \equiv a_1 \cdots a_{k-1} \cdot a_k \equiv a_1 a_k \equiv a_k$

$\cancel{a_1 \cdots a_{k-1} \equiv a_1 \cdots a_k}$

QUINDI $a_1 \equiv a_k$, Però $a_i \in \{1, \dots, n\}$

QUINDI $a_1 = a_k$

ASSURDO.

IMO 2006 /4

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

x, y interi.
il caso $x<0$ si esclude facilmente
caso $x=0 \rightarrow (0,2)$ soluzione
ora assumiamo $x, y > 0$.

$$2^x+2^{2x+1}=y^2-1$$

$$2^x(2^{x+1}+1) = (y+1)(y-1)$$

y é dispari $\longrightarrow$ $y=2k+1$

$$2^x(2^{x+1}+1) = (2k+2)(2k)$$

$$2^{x-2}(2^{x+1}+1) = k(k+1)$$

DUE CASI:

1. k é pari.

$k = a \cdot 2^{x-2}$ (a deve essere dispari)

$$\cancel{2^{x-2}}(2^{x+1}+1) = a\cdot\cancel{2^{x-2}}(a\cdot 2^{x-2}+1)$$

$$2^{x+1}+1 = a^2\cdot 2^{x-2}+a$$

2^{x-2} deve essere pari $\rightarrow x = x'+2$ con $x'>0$

$$2^{x'+3}+1 = a^2 \cdot 2^{x'}+a$$

$$2^{x'}(a^2-8) = 1-a$$

Se $a \geq 3$, LHS > 0, RHS < 0, impossibile

restano $\cancel{a=1}$, $\cancel{a=2}$ che si fanno a mano

II CASO: $k+1$ é pari

$$2^{x-2}(2^{x+1}+1) = k(k+1)$$

$$k+1 = a \cdot 2^{x-2}$$

$$\cancel{2^{x-2}}(2^{x+1}+1) = (a \cdot 2^{x-2}-1) \cdot a \cdot \cancel{2^{x-2}}$$

$$2^{x+1}+a+1 = a^2 \cdot 2^{x-2}.$$

a é dispari, quindi $x-2>0$

$x = x'+2$ con $x'>0$

$$2^{x'+3}+a+1 = a^2 \cdot 2^{x'}$$

$$2^{x'}(a^2-8) = a+1 \qquad 2^{x'} \geq 2$$

$$\Longrightarrow \quad 2(a^2-8) \leq a+1$$

$$2a^2-a-17 \leq 0$$

soluzioni dispari: 1, 3, basta

con $a = 1$: $\quad 2^{x+1} + 1 = 2^{x-2}$

con $a = 3$: $\quad 2^{x+1} + 4 = 9 \cdot 2^{x-2}$

$$2^{x-1} + 1 = 9 \cdot 2^{x-4} = (2^3 + 1)\, 2^{x-4}$$

$$= 2^{x-1} + 2^{x-4}$$

$2^{x-4} = 1 \qquad x = 4 \longrightarrow y =$

FINE

$$x^2+x+1 = n^2$$

$$x^2 < x^2+x+1 < (x+1)^2$$

nessuna soluzione (tranne $x=0$)

$a, b, c \geq 0$

$$4^a+4^b+4^c = n^2$$

$a \leq b \leq c$

$$4^a\left(1+4^{b-a}+4^{c-a}\right) = n^2$$

CASO $a=b=c \longrightarrow 3\cdot 4^a = n^2$ impossibile

$$1+4^{b-a}+4^{c-a} = \left(\frac{n}{2^a}\right)^2$$

se $\left(\frac{a}{b}\right)^2 \in \mathbb{Z}$ $\quad \frac{a}{b} \in \mathbb{Z}$

BASTA RISOLVERE (posto $x=b-a$ e $y=c-a$)

$$1+4^x+4^y = n^2 \qquad \text{con } x \leq y$$

$$4^x(4^{y-x}+1)=(n+1)(n-1)$$

CASO $x=0$ a parte e caso $x=y$ a parte,

possiamo porre $z=y-x>0$, e $n=2k+1$:

$$4^{x-1}(4^z+1)=k(k+1)$$

CASO 1: k é pari

$$k=a\cdot 4^{x-1}$$

$$\cancel{4^{x-1}}(4^z+1)=a\cdot\cancel{4^{x-1}}(a\cdot 4^{x-1}+1)$$

$$4^z+1=a^2 4^{x-1}+a$$

DUE QUADRATI

$$2^z+a\cdot 2^{x-1}\leq a-1$$

e da qui si conclude ...

(LEMMA: $|x^2-y^2|\geqslant|x+y|$)