SENIOR 2011 – Teoria dei Numeri 1 (Basic)

Titolo nota 05/09/2011

Esempio 1 $\frac{1}{a}+\frac{4}{b}=1$

$\frac{b+4a}{ab}=1 \qquad b+4a=ab \qquad b(1-a)=-4a$

$b=-\frac{4a}{1-a}=\frac{4a}{a-1}$ (Ho usato che è di 1° grado rispetto alla variabile b)

$=\frac{4a-4+4}{a-1}=\frac{4(a-1)+4}{a-1}=4+\frac{4}{a-1}$

Quindi $a-1$ deve essere un divisore di 4, quindi $\pm 1, \pm 2, \pm 4$.

Esempio 2 Parallelepipedo $a\times b\times c$ (interi)
Parallelepipedo interno $(a-2)(b-2)(c-2)$
voglio che abbia volume metà del precedente

$2(a-2)(b-2)(c-2)=abc$

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

Idea: $\rightarrow$ parte di divisibilità, congruenze, fattorizzazioni
$\hookrightarrow$ disuguaglianze

Domanda: possono a,b,c essere TUTTI enormi?
Possono essere tutti ≥ 10? Sarebbe

$\left(1-\frac{2}{a}\right)\left(1-\frac{2}{b}\right)\left(1-\frac{2}{c}\right)\geq\frac{64}{125}>\frac{1}{2}$

quindi è impossibile. Pertanto almeno una delle 3 è ≤ 9.
Quindi WLOG $c=3,4,5,6,7,8,9$
Non resta che fare 7 comodi casi, che sono equivalenti all'esempio 1.

Esempio 3 Risolvere $a^2 - b^2 = 998$

Impossibile perché $998 \equiv 2 \ (4)$

Fatti generali: ① I $\square$ mod 4 possono essere solo 0, 1
② a^2+b^2 mod 4 non può essere 3
③ a^2-b^2 " " " " 2

Dim: ② e ③ seguono da ①.

* a pari $\Rightarrow a = 2k \Rightarrow a^2 = 4k^2 \equiv 0 \ (4)$
* a dispari $\Rightarrow a = 2k+1 \Rightarrow a^2 = 4k^2+4k+1 = 4(k^2+k)+1 \equiv 1 \ (4)$

Risolvere $a^2 - b^2 = 1.000$

$$(a+b)(a-b) = 1.000$$

Quindi $a+b$ e $a-b$ devono essere divisori di 1000.
Però $a+b$ e $a-b$ hanno la stessa parità, quindi devo scegliere coppie di divisori con la stessa parità, quindi in questo caso pari.

$1.000 = 2^3 \cdot 5^3 \qquad a+b = 2^k \cdot 5^\ell \qquad k = 1, 2$

$\ell = 0, 1, 2, 3$

Quindi ho 8 possibilità positive e 8 negative per $a+b$, e idem per $a-b$.

Oss. Mi riduco al sistema $a+b = S$, $a-b = D$

$2a = S+D \qquad a = \frac{S+D}{2}$

$2b = S-D \qquad b = \frac{S-D}{2}$

Se S e D hanno la stessa parità, il sistema ha sempre soluzione.

Quindi in totale abbiamo 16 coppie (a,b) che risolvono.

Back to 998 $\underbrace{(a+b)(a-b)} = 998$

avendo la stessa parità, il LHS è

* o dispari
* o multiplo di 4.

Esempio 4 ---- $b = \dfrac{a^2+3}{a+1}$

$$b = \frac{a^2+3+a-a}{a+1} = a + \frac{3-a}{a+1} = a + \frac{3+1-1-a}{a+1} = \boxed{a-1} + \frac{4}{a+1}$$

$$\begin{array}{rr|l} a^2 & +3 & a+1 \\ \cline{3-3} -a^2-a & & \boxed{a-1} \\ \hline // \quad -a & +3 & \\ +a & +1 & \\ \hline // & 4 & \end{array}$$

$$a^2+3 = (a+1)(a-1)+4$$

$$\frac{a^2+3}{a+1} = a-1+\frac{4}{a+1}$$

— o —

$$b = \frac{a^2+3}{2a+1} = \frac{1}{2}\,\frac{2a^2+6}{2a+1} = \frac{1}{2}\,\frac{2a^2+a-a+6}{2a+1}$$

$$= \frac{1}{2}\left\{a + \frac{-a+6}{2a+1}\right\}$$

$$= \frac{a}{2} + \frac{1}{4}\,\frac{-2a+12-1+1}{2a+1}$$

$$= \frac{a}{2} + \frac{1}{4}\left\{-1+\frac{13}{2a+1}\right\}$$

$$= \frac{a}{2} - \frac{1}{4} + \boxed{\frac{13}{2a+1}}\cdot\frac{1}{4} = \frac{1}{4}\left\{2a-1+\frac{13}{2a+1}\right\}$$

deve essere intero

Di sicuro $2a+1$ deve dividere 13 e resta un numero finito di casi da provare.

— o — o —

Divisione Euclidea Dati 2 interi positivi a e b, esistono q ed r (unici) tali che

$$\boxed{a = q\cdot b + r \qquad 0 \le r < b}$$

Teorema di Bezout Siano a e b due interi (diciamo positivi). Allora esistono due interi m ed n tali che

$$\boxed{am + bn = \text{massimo comun divisore di } a \text{ e } b}$$

Fatto generale Dati a e b interi. Quali sono tutti gli interi che si scrivono come

$$ax + by \qquad x \in \mathbb{Z},\ y \in \mathbb{Z}$$

Sono tutti e soli i multipli di MCD(a,b)

Come calcolare m ed n dati a e b?

Intanto suppongo WLOG che MCD(a,b) = 1.

Divisioni euclidee iterate

$a = 70 \qquad b = 13$

$$\boxed{70} = \boxed{13} \cdot 5 + \boxed{5}$$
$$\boxed{13} = \boxed{5} \cdot 2 + \boxed{3}$$
$$\boxed{5} = \boxed{3} \cdot 1 + \boxed{2}$$
$$\boxed{3} = \boxed{2} \cdot 1 + \boxed{1}$$

Iterando l'algoritmo prima o poi si trova resto = 1.

Adesso procedo al contrario

Mi procuro 1 dall'ultima

$$1 = \boxed{3} - \boxed{2} \cdot 1$$

Mi procuro 2 dalla penultima

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

Mi procuro 3

$$= (13 - 5 \cdot 2) \cdot 2 - 5$$
$$= 13 \cdot 2 - 5 \cdot 5$$

Mi procuro 5

$$= 13 \cdot 2 - (70 - 13 \cdot 5) \cdot 5$$
$$= 13 \cdot 27 - 70 \cdot 5$$

Quindi ho ottenuto che $\quad 13 \cdot 27 - 70 \cdot 5 = 1$

—o—o—

Dati a e b con MCD(a,b) = 1, sono unici m ed n t.c.

$$am + bn = 1 \quad ?$$

Ovviamente NO! Nell'esempio $\quad 13 \cdot (27+70) - 70\,(5+13) = 1$

Come sono fatte TUTTE le soluzioni?

Sia (m, n) una soluzione: $am + bn = 1$
Sia (m_1, n_1) un'altra soluzione: $am_1 + bn_1 = 1$

Differenza: $a(m - m_1) + b(n - n_1) = 0$
$$a(m - m_1) = b(n_1 - n)$$

Poiché $MCD(a,b) = 1$, si ha che $a \overset{\text{divide}}{|} (n_1 - n)$, quindi $n_1 - n = ka$, e di conseguenza $m - m_1 = kb$, cioè

$m_1 = m - kb$ $\qquad n_1 = n + ka$

Basta sostituire per vedere che (m_1, n_1) va bene per ogni $k \in \mathbb{Z}$.

— o — o —

Scrittura di un intero positivo in base b

$$n = \underbrace{a_k a_{k-1} \dots a_1 a_0}_{\text{cifre in base } b, \text{ quindi } 0 \le a_i \le b-1}$$
$$= a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0$$

Esempio Scrivere 70 in base 2

$$70 = 1 \cdot 64 + 0 \cdot 32 + 0 \cdot 16 + 0 \cdot 8 + 1 \cdot 4 + 1 \cdot 2 + 0 \cdot 1$$
$$= (1000110)_2$$

Esempio $f: \mathbb{N} \to \mathbb{N}$ $\quad f(0) = f(1) = 0$

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

	In binario	
$f(0) = 0$		$f(0) = 0$
$f(1) = 0$		$f(1) = 0$
$f(2) = 1$		$f(10) = 1$
$f(3) = 0$		$f(11) = 0$
$f(4) = 3$		$f(100) = 11$
$f(5) = 2$		$f(101) = 10$
$f(6) = 1$		$f(110) = 1$
$f(70) =$		$f(1000110) = 111001$

[Si tratta di dim. formalmente per induzione che f "inverte" le cifre in base 2]

$n = [1\,1\,0\,\dots]$ $\qquad 2n+1 = [\qquad\quad]1$ $\quad$ invertito.

$f(n) = [\text{ invertito }]$ $\qquad f(2n+1) = 2f(n)$

$\qquad\qquad\qquad\qquad\qquad = \boxed{[\text{invertito}]\,0}$

— o — o —

<u>Esercizio</u> $\qquad d_n = MCD\,(100+n^2,\ 100+(n+1)^2)$

Quanto può valere al massimo d_n ?

$d_n \mid 100+n^2$

$d_n \mid 100+(n+1)^2 = n^2+2n+101$

$\Rightarrow d_n \mid n^2+2n+101-(100+n^2) = 2n+1$

Ora so che $\quad d_n \mid n^2+100 \Rightarrow d_n \mid 4n^2+400$

$\qquad\qquad\quad d_n \mid 2n+1$

$$
\begin{array}{l|l}
4n^2+400 & 2n+1 \\
\hline
-4n^2-2n & 2n-1 \\
\hline
-2n+400 & \\
+2n\quad +1 & \\
\hline
\qquad 401 &
\end{array}
$$

$4n^2+400 = (2n+1)(2n-1)+401$

$d_n \qquad\qquad d_n$

$\Rightarrow d_n \mid 401$

$\Rightarrow d_n$ può essere solo

1 oppure 401

Devo trovare un esempio in cui effettivamente $d_n = 401$

Dalla condizione $d_n \mid 2n+1$ una possibilità è provare $n = 200$

Devo controllare $\quad 401 \mid 200^2+100 = 4\cdot 100\cdot 100+100 = 401\cdot 100$

$\qquad\qquad\qquad\qquad 401 \mid 201^2+100$

Per la 2^a o si fa il conto scrivendo $201^2 = (200+1)^2$,

oppure si osserva che

$$200 \equiv -201 \pmod{401}$$

$$200^2 \equiv 201^2 \pmod{401}$$

— o — o —

CONGRUENZE

$a \equiv b \pmod{n}$ $\quad$ n intero ≥ 2

$\Leftrightarrow$ a e b hanno stesso resto quando divisi per n
$\Leftrightarrow$ $a-b$ è multiplo di n.

Fatto generale: ogni intero è congruo (mod n) ad un intero in $\{0, 1, \dots, n-1\}$

Si comportano bene rispetto a somma e prodotto

$$\begin{matrix} a_1 \equiv b_1 \\ a_2 \equiv b_2 \end{matrix} \Rightarrow \quad a_1 \pm a_2 \equiv b_1 \pm b_2 \qquad a_1 \cdot a_2 \equiv b_1 \cdot b_2$$

<u>Divisione</u> $\quad 5x \equiv 2 \pmod{13} \qquad x \equiv \text{"}\frac{2}{5}\text{"} \pmod{13}$

Inverso di 5 mod 13 è 8: infatti $5 \cdot 8 = 40 \equiv 1 \ (13)$

$5x \equiv 2 \pmod{13}$ $\quad$ Moltiplico per 8!
$40x \equiv 16 \pmod{13}$ $\quad$ $x \equiv 3 \pmod{13}$

Come si trova l'inverso? Trovare l'inverso di 5 (mod 13) vuol dire trovare un numero m t.c. $5m \equiv 1 \pmod{13}$ cioè $5m = 1 + 13n$, cioè $5m - 13n = 1$, quindi è come in BEZOUT.

L'inverso esiste se e solo se ciò che voglio invertire ed il modulo hanno MCD = 1.

Inverso di 7 mod 13 : 2 $\quad (7 \cdot 2 \equiv 1 \pmod{13})$
di 7 mod 16 : 7 $\quad (7 \cdot 7 \equiv 1 \pmod{16})$
di 7 mod 12 : 7 $\quad (7 \cdot 7 \equiv 1 \pmod{12})$

Inverso di 7 mod 36:

$$7 \cdot 5 = 35 \equiv -1 \pmod{36}$$
$$7 \cdot (-5) = -35 \equiv 1 \pmod{36}$$
$$7 \cdot 31 \equiv 1 \pmod{36}$$

Fatto generale: voglio risolvere $ax \equiv b \pmod n$
OK se $\text{MCD}(a, n) = 1$.

Se a ed n non sono primi tra loro, può esistere o non esistere x.

$$3x \equiv 5 \pmod{12}$$

Impossibile perché $\underset{3}{\underset{\uparrow}{3x}} = \underset{\text{NO } 3}{\underset{\uparrow}{5}} + \underset{3}{\underset{\uparrow}{12k}}$

$$\overset{2}{\cancel{6}}x \equiv \overset{3}{\cancel{9}} \pmod{\overset{4}{\cancel{12}}} \iff 2x \equiv 3 \pmod 4$$

$$6x = 9 + 12k \iff 2x = 3 + 4k \iff 2x \equiv 3 \pmod 4$$

Occhio a semplificare nelle congruenze.

— o — o —

<u>Criteri di congruenza</u>

Un numero è congruo modulo 2 alla sua cifra delle unità
" " " 3 alla somma delle sue cifre
" " " 4 al numero costituito dalle ultime 2 cifre
" " modulo 9 alla somma delle cifre
" " modulo 11 alla somma delle cifre a segno alterno, in modo che la cifra delle unità abbia segno +.

$$a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0 \overset{\text{mod } 3 \text{ o } 9}{\equiv} a_k + a_{k-1} + \dots + a_1 + a_0$$
$$\underset{\text{mod } 11}{\equiv} a_0 - a_1 + a_2 - a_3 + \dots$$

Esercizio $\boxed{18}\boxed{2}$ $\quad \boxed{18} - \boxed{2} \cdot 2 = 14$ divisibile per 7, allora divisibile per 7 all'inizio

$\boxed{200}\boxed{3} \rightsquigarrow 200 - 3 \cdot 2 = 182 \rightsquigarrow 14 \rightsquigarrow$ ok

$2072 \rightsquigarrow 207 - 2 \cdot 2 = 203 \rightsquigarrow 20 - 3 \cdot 2 = 14 \rightsquigarrow$ ok

Questo è un criterio di DIVISIBILITÀ, ma non di congruenza.
Perché funziona?

Enunciato: $\quad 10A + B \equiv 0 \pmod 7 \iff A - 2B \equiv 0 \pmod 7$

Dim. Prendo $10A + B$ e moltiplico per 5 (inverso di 10)

$$50A + 5B \equiv A - 2B \pmod 7$$

Viceversa: se $A - 2B \equiv 0 \pmod 7$ moltiplico per 10 e ottengo

$$10A - 20B \equiv 0 \pmod 7$$

$$10A + B \equiv 0 \quad \text{"}\quad .$$

—o—o—

C'è lo stesso modulo 13? $\quad 10A + B \equiv 0 \pmod{13}$

$$\Updownarrow$$

$$A + kB \equiv 0 \pmod{13}$$

Sol: $k = 4$. Basta prendere la 1ª e moltiplicare per 4 (inverso di 10 modulo 13).

—o—o—

Residui quadratici $\quad$ Risolvere $x^2 \equiv a \pmod m$

Si dice che a è residuo quadratico mod m se riesco a risolvere.
Appena $m \geq 3$ esistono valori di a per cui non si risolve.

Esercizio I residui quadratici mod 401 sono 201.
Calcolo $0^2, 1^2, 2^2, \dots, 400^2$. Tranne 0^2, tutti gli altri $(\pm k)^2 = k^2$. Ci possono essere più sovrapposizioni?

$x^2 \equiv y^2 \pmod{401}$ vuol dire per forza che $x \equiv \pm y \ (401)$?

$(x+y)(x-y) = 401k$. Essendo 401 primo abbiamo che o $401 \mid x-y$ (quindi $x \equiv y$) o $401 \mid x+y$ (quindi $x \equiv -y$).

STRUTTURA MOLTIPLICATIVA — p PRIMO

Come si comportano $a^0, a^1, a^2, a^3, \ldots \pmod p$ nel caso $MCD(a,p) = 1$.

Le potenze sono periodiche !!

__Esempio__ $p = 7$

$$2^0 \equiv 1 \qquad 2^3 \equiv 1$$
$$2^1 \equiv 2 \qquad 2^4 \equiv 2^3 \cdot 2 \equiv 2 \qquad (\text{mod } 7)$$
$$2^2 \equiv 4 \qquad 2^5 \equiv 4$$

Le potenze di 2 si ripetono con periodo 3.

$3^0 \equiv 1$

$3^1 \equiv 3$ — Le potenze di 3 si ripetono con periodo 6

$3^2 \equiv 2$

$3^3 \equiv 6 \equiv (-1)$ — Le potenze di 6, cioè le potenze di -1,

$3^4 \equiv 4 \equiv (-3)$ — si ripetono con periodo 2.

$3^5 \equiv 5$

$3^6 \equiv 1$

__Definizione__ Si chiama ordine moltiplicativo di a mod p il periodo (più piccolo) delle potenze di a mod p. Si indica con

$$\boxed{\text{ord}_p(a)}$$

__Esempi__ $\text{ord}_7(2) = 3$ $\quad \text{ord}_7(3) = 6$ $\quad \text{ord}_7(6) = 2$

$\text{ord}_7(1) = 1$

__Dim. della periodicità.__ Considero $a^0, a^1, a^2, \ldots, a^p, \ldots$

Sono infiniti oggetti che possono essere solo $1, 2, \ldots, p-1$.

Quindi prima o poi c'è una ripetizione, cioè esistono $m < n$ t.c. $a^m \equiv a^n \pmod p$, cioè $a^n - a^m = kp$, cioè $a^m(a^{n-m} - 1) = kp$. Essendo $MCD(a,p) = 1$, devo avere $p \mid (a^{n-m} - 1)$, cioè $a^{n-m} \equiv 1 \ (p)$, quindi c'è una potenza con esp $\neq 0$ che fa 1.

Corollario Fino a quando non si ripete la classe 1, nessuna classe si ripete.

Quindi $a^0 = 1$, poi tutti diversi fino a quando per un certo k si ha che $a^k \equiv 1$, da lì in poi si ripete. Chi è k? $k = \text{ord}_p(a)$.

Applicazione 1 Supponiamo che $a^n \equiv 1 \pmod{p}$.
Allora $\text{ord}_p(a) \mid n$

Applicazione 2 Supponiamo che $a^n \equiv a^m \pmod{p}$
Allora $\text{ord}_p(a) \mid m-n$

PICCOLO TEOREMA DI FERMAT

Versione 1 : $a^{p-1} \equiv 1 \pmod{p}$ se $\text{MCD}(a,p) = 1$
Versione 2 : $a^p \equiv a \pmod{p}$ per ogni a

Corollario $\text{ord}_p(a)$ è sempre un divisore di $p-1$.

— o — o —

DIM FLT 1 $a^p \equiv a \pmod{p}$
Per induzione su a : banale per $a=0$ o per $a=1$
P.I. Hp: $a^p \equiv a \pmod{p}$ Tesi: $(a+1)^p \equiv a+1 \pmod{p}$

$$(a+1)^p = a^p + \underbrace{\binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \dots + \binom{p}{p-1} a}_{\text{multipla di } p} + 1 = (\star)$$

dove $\binom{p}{k} = \dfrac{p!}{k!\,(p-k)!}$ ← Tutti multipli di p, tranne per $k=0$ e $k=p$

uso Hp induttiva.

$$(\star) \equiv a^p + 1 \equiv a+1$$

$\boxed{\text{DIM FLT 2}}$ $\quad a^{p-1} \equiv 1 \pmod p$

$\{1, 2, \dots, p-1\}$ = tutte classi non nulle mod p

$\{a, 2a, \dots, (p-1)a\}$ = nuovamente tutte le classi mod p

Perchè? Sono $(p-1)$ oggetti e sono tutti distinti perchè se fosse $ma = na \pmod p$

vorrebbe dire che $a\,\underbrace{(m-n)}$ è multiplo di p

no multiplo di p per ipotesi — troppo piccolo per essere multiplo di p

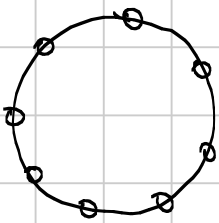
Allora

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

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

cioè $(p-1)!\,[a^{p-1}-1] = kp \Rightarrow$ p sta per forza in $(a^{p-1}-1)$

$\boxed{\text{DIM FLT 3}}$



Collana con p palline che voglio colorare con a colori. Considero equivalenti 2 collane che si ottengono l'una dall'altra mediante rotazioni.

Quante sono le possibili collane NON monocromatiche?

$\overset{\text{TUTTE}}{a^p} - \overset{\text{MONOCROMATICHE}}{a}$

Devo dividere per tener conto della rotazione.

Una certa colorazione, quante altre diverse ne genera RUOTANDO?

Se ne genera p ho che $\dfrac{a^p - a}{p}$ è intero e ho finito.

Se una collana ruotando di k torna in sè vuol dire che la 0 è colorata come la k, la 2k, la 3k, ..., $(p-1)k$, ma queste sono tutte distinte, quindi sarebbe monocromatica.

— o — o —

IMO 2009 – 1 $\quad a_1, \dots, a_k$ interi in $\{1, \dots, n\}$ distinti

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

Tesi: $\quad n \nmid a_k (a_1 - 1)$

Ipotesi:
$$n \mid a_1 (a_2 - 1)$$
$$n \mid a_2 (a_3 - 1)$$
$$n \mid a_3 (a_4 - 1)$$
$$\vdots$$
$$n \mid a_{k-1} (a_k - 1)$$

Tesi: $n \nmid a_k (a_1 - 1)$

Dim Supponiamo che oltre all' ipotesi valga anche $n \mid a_k (a_1 - 1)$ e cerchiamo un assurdo.

$$n \mid a_1 (a_2 - 1) \iff a_1 (a_2 - 1) \equiv 0 \pmod{n} \iff a_1 \equiv a_1 a_2 \ (n)$$

$$\left.\begin{array}{l} \left.\begin{array}{ll} a_1 \equiv a_1 a_2 & \pmod{n} \\ a_2 \equiv a_2 a_3 & \pmod{n} \end{array}\right\} a_1 \equiv a_1 a_2 a_3 \\ a_3 \equiv a_3 a_4 \quad \pmod{n} \end{array}\right\} a_1 \equiv a_1 a_2 a_3 a_4$$
$$\vdots$$

Per induzione ottengo che $\quad a_1 \equiv a_1 \cdot \ldots \cdot a_k \pmod{n}$

Oss.: Fin qui ho usato l' ipotesi, ma non la tesi negata.

Nel momento in cui assumo che la tesi sia falsa, l' ipotesi diventa ciclica, quindi posso partire da un qualunque a_i

Ottengo $\quad a_i \equiv$ prodotto di tutti $\quad$ per ogni $i = 1, \dots, k$.

Quindi tutti gli a_i hanno la stessa classe (mod n) ed essendo in $\{1, \dots, n\}$ dovrebbero coincidere. Assurdo.

—o —o —

$\boxed{\text{IMO 2006} - 4}$ $\quad 1 + 2^x + 2^{2x+1} = y^2 \qquad x, y$ interi

Bisognerebbe trattare il caso di $x \leq 0$, che è facile ma richiede qualche considerazione (e vengono soluzioni)
D'ora in poi $x > 0$, quindi LHS dispari, quindi y dispari
$y = 2n+1$

$$\cancel{1} + 2^x + 2^{2x+1} = 4n^2 + 4n + \cancel{1}$$

$$2^x (1 + 2^{x+1}) = 4n(n+1) \qquad \text{quindi } x \geq 2$$

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

Ora il 2^{x-2} deve andare tutto nello stesso fattore del RHS

- Caso 1: $\quad n = k \cdot 2^{x-2}$: $\quad \cancel{2^{x-2}}(1 + 2^{x+1}) = k \cdot \cancel{2^{x-2}}(k \cdot 2^{x-2} + 1)$

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

Per ragioni di disuguaglianze k può essere solo 1 oppure 2

Se $k \geq 3$, allora $\quad k^2 2^{x-2} + k \geq 9 \cdot 2^{x-2} + 3$

$$> 8 \cdot 2^{x-2} + 3$$
$$> 2^{x+1} + 1$$

Sostituito $k=1$ o $k=2$, c'è una sola incognita...

- Caso 2: $\quad n+1 = k \cdot 2^{x-2}$: $\quad \cancel{2^{x-2}}(1 + 2^{x+1}) = k\, \cancel{2^{x-2}}(k 2^{x-2} - 1)$

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

Ancora una volta k non può essere troppo grande, ma va detto bene

$k^2 \geq k + 8$ vera per ogni $k \geq 4$, quindi se $k \geq 4$ ho che

$$k^2 2^{x-2} - k \geq (k+8) 2^{x-2} - k = k\, 2^{x-2} + \cancel{2^{x+1}} - k \overset{?}{\geq} \cancel{2^{x+1}} + 1$$
$$= k(2^{x-2} - 1) \overset{?}{\geq} 1$$

vera appena $x \geq 3$ (controllare $x = 2$ a mano).

— o — o —

$\boxed{\text{IMO 2005}-4}$ Per ogni primo p esiste un intero positivo n t.c.
$$p \mid 2^n+3^n+6^n-1$$

$p=2$ $\quad 2 \mid 2^n+3^n+6^n-1 \iff 2 \mid 3^n-1$ basta $n=1$
$p=3$ $\quad 3 \mid$ " $\iff 3 \mid 2^n-1$ " $n=2$

Oss. "border line": $n=-1$ in un certo senso va bene
$$\frac{1}{2}+\frac{1}{3}+\frac{1}{6}-1=0$$

Oss. "più seria": se $p \neq 2,3$, allora

$$(\text{inverso di } 2)+(\text{inverso di } 3)+(\text{inverso di } 6) \equiv 1 \quad (p)$$

$a=$ inv. di 2
$b=$ inv. di 3
$c=$ inv. di 6

$$\begin{aligned} 6(a+b+c) &\equiv 6a+6b+6c \\ &\equiv 3\cdot 2a+2\cdot 3b+6c \\ &\equiv 3+2+1 \\ &\equiv 6 \pmod p \end{aligned}$$

Essendo $p \neq 2,3$ posso "semplificare il 6"

FLT $\Rightarrow$ elevare alla $p-1$ è come elevare alla 0, quindi
" " $p-2$ " " " " -1, cioè come
fare l'inverso.

Quindi basta prendere $n=p-2$.

Per $p \neq 2,3$ considero $n=p-2$

$$\begin{aligned} 6\left(2^{p-2}+3^{p-2}+6^{p-2}\right) &= 3\cdot 2^{p-1}+2\cdot 3^{p-1}+6^{p-1} \overset{(FLT)}{\equiv} \\ &\equiv 3+2+1 \\ &\equiv 6 \pmod p \end{aligned}$$

Essendo $p \neq 2,3$ ho che $2^{p-2}+3^{p-2}+6^{p-2} \equiv 1 \pmod p$.

— o — o —