Teoria dei Numeri 2 - Medium

Titolo nota 04/09/2014

Lemma Sia p un primo, $q(x) \in \mathbb{Z}/p\mathbb{Z}[x]$

Supponiamo che $\deg q \leq p-2$. Allora

$$\sum_{n=0}^{p-1} q(n) \equiv 0 \pmod{p}$$

Dimostrazione

(1) Basta farlo per i monomi (ax^k)

(2) $a = 1$

$$\sum_{n=0}^{p-1} 2n^3 \equiv 0 \pmod{p}$$

(3) $$\sum_{n=0}^{p-1} n^k \equiv \sum_{n=1}^{p-1} n^k \equiv$$

$k > 0$

dove g è un generatore

$$\equiv \sum_{j=0}^{p-2} (g^j)^k$$

$$\equiv \sum_{j=0}^{p-2} (g^k)^j \equiv \frac{(g^k)^{p-1} - 1}{g^k - 1} \equiv 0$$

La formula per la somma della progr geometrica funziona purché $g^k \not\equiv 1 \ (p)$

$\Leftrightarrow \quad (p-1) \nmid k$

(4) Se $k=0$: un polinomio di grado 0 è una costante a. $\sum_{j=0}^{p-1} a = p \cdot a \equiv 0$

Osservazione Per x^{p-1} la somma vale -1

$$\sum_{j=0}^{p-1} j^{p-1} \equiv 0 + \underbrace{1 + \dots + 1}_{(p-1) \quad \text{FLT}} \equiv -1 \ (p)$$

Lemma ++ Se $q(x)$ non ha monomi di grado divisibile per $p-1$ (e non costanti) allora $\sum_{n=0}^{p-1} q(n) \equiv 0 \mod p$

CHEVALLEY - WARNING

Sia
$$\begin{cases} f_1(x_1, \dots, x_n) \equiv 0 \pmod p \\ \vdots \\ f_k(x_1, \dots, x_n) \equiv 0 \pmod p \end{cases}$$
un sistema polinomiale di congruenze.

Supponiamo che $\sum \deg f_k < n$.

Allora se c'è una soluzione ce n'è almeno un altra

Esempio $X^2 - 3y^2 = 47z^2$

Inutile controllare mod p per $p \neq 3, 47$.

Infatti CW (per $p \neq 3, 47$) dice:

- ci sono 3 variabili
- il grado è 2
- c'è una soluzione banale: $(0,0,0)$

$\Rightarrow$ ce n'è anche una non banale

Versione "aritmetica"

Il numero di soluzioni (al sistema...)

è $\equiv 0 \pmod p$

Dimostrazione

$$f_i^{p-1}(x_1, \dots, x_n) \equiv \begin{cases} 0, & \text{se } f_i(x_1, \dots, x_n) = 0 \\ 1 & \text{altrimenti} \end{cases}$$

$$\prod_{i=1}^{k} \left(1 - f_i^{p-1}\right) \equiv \begin{cases} 1, & \text{se } (x_1, \dots, x_n) \text{ è una soluzione} \\ 0 & \text{se anche solo un } f_i(x_1, \dots, x_n) \neq 0 \end{cases}$$

$$\#\text{soluzioni} \equiv \sum_{x_1} \sum_{x_2} \cdots \sum_{x_n} \prod_{i=1}^{k} \left(1 - f_i^{p-1}\right)$$

Esempio 2 variabili, grado 1

$$x_1 + 2x_2 - 5$$

(x_1, x_2) è soluzione $\iff (x_1 + 2x_2 - 5)^{p-1} \equiv 0$

$$\iff 1 - (x_1 + 2x_2 - 5)^{p-1} \equiv 1 \pmod p$$

Se sommiamo $\sum_{x_1=0}^{p-1} \sum_{x_2=0}^{p-1} \left(1 - (x_1 + 2x_2 - 5)^{p-1}\right)$

otteniamo $\sum_{x_1}\sum_{x_2}$ $\begin{cases} 1, & \text{se } (x_1,x_2) \text{ è sol} \\ 0 & \text{altrimenti} \end{cases}$

e cioè il # soluzioni

Fissiamo $p=7$.

$$-x_1^6$$
$$-\binom{6}{2}x_1^2(2x_2)^4$$
$$\vdots$$

Trucco $\sum_{x_1=0}^{p-1}\sum_{x_2=0}^{p-1} x_1^a x_2^b \equiv 0 \mod p$

- Se $a \le p-2$,

$$\sum_{x_2=0}^{p-1}\sum_{x_1=0}^{p-1} x_1^a x_2^b \equiv$$

$$\equiv \sum_{x_2=0}^{p-1} x_2^b \left(\sum_{x_1=0}^{p-1} x_1^a\right)$$

$$\equiv \sum_{x_2=0}^{p-1} x_2^b \cdot 0 \equiv 0 \mod p$$

- Uguale se $b \le p-2$
- Può essere $a \ge p-1$, $b \ge p-1$? Certamente no, perché altrimenti $\deg (x_1+2x_2-5)^{p-1}$

$\geq 2(p-1)$ ASSURDO

In generale Sviluppando

$$\sum_{x_1} \cdots \sum_{x_n} \prod \left(1 - f_i(x_1, \ldots, x_n)^{p-1}\right)$$

possiamo trovare un termine $x_1^{a_1} \cdots x_n^{a_n}$ con tutti gli $a_i > 0$ e $\equiv 0 \ (p-1)$?

No, perché altrimenti $\sum (\deg f_i)(p-1) \geq (p-1) \cdot n$, assurdo per ipotesi. □

Corollario Se gli $f_i(x_1, \ldots, x_n)$ sono omogenei (o senza termine noto), allora ci sono almeno $(p-1)$ soluz. non banali ($+1$ banale, che è $(0, 0, \ldots, 0)$)

Esercizio Per ogni primo p esiste $k < p$ e x, y, z tali che $x^2 + y^2 + z^2 = kp$

Soluzione con CW Il polinomio $x^2 + y^2 + z^2$ è omogeneo, in 3 variabili, di grado 2

Quindi la congruenza $x^2+y^2+z^2 \equiv 0 \ (p)$ ha una soluz. non banale

Scegliamo $0 \le x, y, z \le \frac{p-1}{2}$; allora

$$x^2+y^2+z^2 < 3\left(\frac{p}{2}\right)^2 = \left(\tfrac{3}{4}p\right) \cdot p$$

IMO ~ 2008 (SL)

p primo. A è un insieme di interi positivi, $q_1, \dots, q_{p-1}$ sono primi

* Ogni intero in A si scrive come prodotto dei q_i (detto meglio: tutti i fattori primi sono tra i q_i)

* Ogni prodotto di elementi di A non è una potenza p-esima perfetta

Qual è al massimo $|A|$?

Elementi di A = vettori di lunghezza $(p-1)$

$(e_1, \dots, e_{p-1})$

Condizione : la somma di alcuni di questi vettori non ha tutte le coordinate $\equiv 0 \ (p)$

$p=2 \rightsquigarrow$ * tutti gli elementi di A sono

della forma q^j

* c'è al più un elem: dev'essere q^{dispari}, ma se ce ne sono 2 il prodotto è un quadrato

$p=3 \rightsquigarrow$ $2,\ 3,\ 6=2\cdot 3,\ 2\cdot 3^3$ ④

q_1	q_1^{1+p}	q_1^{1+2p}	...	$(p-1)$
⋮				⋮
q_{p-1}	q_{p-1}			$(p-1)$

Totale $(p-1)^2$

Tentativo: se sono $> (p-1)^2$?

$(e_{1,1}; \dots, e_{1,p-1})$
$(e_{2,1}; \dots; e_{2,p-1})$
⋮

} Sono k almeno $(p-1)^2+1$

Cerco $a_1, \dots, a_k \in \{0,1\}$ in modo che $\sum a_i (e_{i,1}; \dots; e_{i,p-1})$ abbia tutte le coord. $\equiv 0 \ (p)$

$$\begin{cases} a_1^{p-1} e_{1,1} + a_2^{p-1} e_{2,1} + \dots + a_k^{p-1} e_{k,1} \equiv 0 \ (p) \\ a_1^{p-1} e_{1,2} + a_2^{p-1} e_{2,2} + \dots + a_k^{p-1} e_{k,2} \equiv 0 \ (p) \\ \vdots \end{cases}$$

Numero di incognite : k

" " equazioni $= p-1$

Grado totale: $(p-1)^2$

Se $k > (p-1)^2$, siccome c'è la soluzione banale $(0, 0, \dots, 0)$, ce n'è anche una non banale. Quindi trovo un sottoins di A il prodotto dei cui elementi è una potenza p-esima, MALE.

Ritorno su $y^2 = x^3 + 7$

Affermazione: questa ha soluzioni mod p per ogni primo p.

(x,y) è soluzione mod $p \iff$

$$1 - (y^2 - x^3 - 7)^{p-1} \equiv 1 \mod p$$

$$\#\text{soluzioni mod } p \equiv \sum_x \sum_y \left[1 - (y^2 - x^3 - 7)^{p-1}\right]$$

$$\equiv -\sum_x \sum_y \sum_{j=0}^{p-1} \binom{p-1}{j} y^{2j} (-x^3 - 7)^{p-1-j}$$

$$\equiv -\sum_x \sum_j \binom{p-1}{j} (-x^3 - 7)^{p-1-j} \sum_y y^{2j}$$

Chi sopravvive? $j = \frac{p-1}{2}, p-1$

In realtà anche $j = p-1$ somma a zero perché c'è $\sum_x$

$$\equiv -\sum_x \binom{p-1}{\frac{p-1}{2}} \cdot (-1) \cdot (-x^3 - 7)^{\frac{p-1}{2}}$$

$$\equiv +\sum_x \binom{p-1}{\frac{p-1}{2}} \sum_{k=0}^{\frac{p-1}{2}} (-x^3)^k (-7)^{\frac{p-1}{2}-k} \binom{\frac{p-1}{2}}{k}$$

$$\equiv \binom{p-1}{\frac{p-1}{2}} \sum_{k=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{k} (-7)^{\frac{p-1}{2}-k} \sum_{x} (-x)^{3k}$$

I k muoiono tutti, tranne quelli per cui $(p-1) \mid 3k$, $k>0$, cioè solo $\frac{p-1}{3}$

$p \equiv 1 (3)$

$$\equiv \binom{p-1}{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{\frac{p-1}{3}} (-7)^{\frac{p-1}{6}} \cdot (-1)$$

$$\not\equiv 0 \quad \text{se} \quad p \neq 7$$

E gli altri? $y^2 = x^3 + 7$ modulo $p \equiv 2 \pmod 3$

ogni numero è un residuo cubico

$$\left(\#\text{residui cubici} = 1 + \frac{p-1}{(p-1,3)} = p \right)$$

e la radice cubica è unica

$$x = \sqrt[3]{y^2 - 7} \pmod p,$$

quindi le soluzioni sono esattamente p

[$p = 2, 3, 7$ a mano]

Soluzioni modulo p^n (Hensel dei poveri)

$p \neq 2, 3, 7$. Sia x, y una soluzione modulo p.

$$(y + bp)^2 - (x + ap)^3 - 7 \equiv 0 \pmod{p}$$

Vorrei trovare a, b in modo che

$$y^2 + 2byp - (x^3 + 3x^2 \cdot a \cdot p) - 7 \overset{?}{\equiv} 0 \pmod{p^2}$$

$$kp + p(2by - 3ax^2) \overset{?}{\equiv} 0 \pmod{p^2}$$

$$k + 2by - 3ax^2 \overset{?}{\equiv} 0 \pmod{p}$$

(Questa ha una soluz. (a, b) a meno che

$$2y \equiv 0 \pmod{p} \text{ e } -3x^2 \equiv 0 \pmod{p}$$

$\xRightarrow{p \neq 2,3}$ $x \equiv 0 \equiv y \pmod{p}$; sostituendo otteniamo

$$0 \equiv 0 + 7 \mod p$$

assurdo per $p \neq 7$

E da p^n a p^{n+1} ?

Se (x,y) è soluz mod p^n, ne so costruire una mod p^{n+1} della forma

$$x + a \cdot p^n, \quad y + b \cdot p^n$$

PELL, PELL, PELL (LE 6 L)

Fissiamo $d > 0$ e cerchiamo di risolvere

$$x^2 - dy^2 = 1$$

Oss. 1 Se $d = \square$ si fattorizza e non è interessante

Oss 2 Si può supporre d libero da quadrati

Claim Se $d \neq \square$ ci sono infinite soluz.

$$x^2 - dy^2 = (x + \sqrt{d}\, y)(x - \sqrt{d}\, y)$$

Norma $N(x + \sqrt{d}\, y) = x^2 - dy^2$

$$N\big((x + \sqrt{d}\, y)(w + \sqrt{d}\, z)\big) =$$

$$= N(x + \sqrt{d}\, y)\, N(w + \sqrt{d}\, z)$$

"Pell" = "$N(x + \sqrt{d}\, y) = 1$"

Idea Per trovare una soluzione della Pell (= una cosa di norma 1)

cerchiamo due cose con la stessa norma

e facciamo il rapporto

$$\frac{x + \sqrt{d}\, y}{z + \sqrt{d}\, w} = \frac{(x + \sqrt{d}\, y)(z - \sqrt{d}\, w)}{z^2 - d w^2}$$

$$= \frac{(xz - dwy) + \sqrt{d}\,(yz - xw)}{N(z + \sqrt{d}\, w)}$$

Supponiamo di avere $x + \sqrt{d}\, y$, $z + \sqrt{d}\, w$ con la stessa norma N.

Ci serve $N \mid (xz - dwy)$

$N \mid yz - xw$

" $y/x \equiv w/z$ $\Leftarrow$ (*) $\boxed{\begin{matrix} y \equiv w \\ x \equiv z \end{matrix}}$ mod N

$x^2 - dy^2 \equiv 0 \ (N)$ "

Meglio: se ne troviamo infiniti con la stessa norma, allora due rispettano (*) e il rapporto è intero.

Dirichlet: se α è irrazionale, $\exists$ infiniti p/q : $|\alpha - p/q| < 1/q^2$

Applichiamolo ad $\alpha = \sqrt{d}$

$$(x - \sqrt{d}y)(x + \sqrt{d}y) = N$$

tende a 0 · tende a ∞

$x - \sqrt{d}y \approx 0 \iff x/y \approx \sqrt{d}$

Dirichlet $\Rightarrow$ esistono infiniti p/q t.c.

$$|\sqrt{d} - p/q| < 1/q^2$$

$$|N(p+\sqrt{d}\,q)| = |(p+\sqrt{d}\,q)(p/q - \sqrt{d})\cdot q|$$

$$< 1/q^2 \cdot q \cdot |p+\sqrt{d}\,q|$$

$$= |p/q + \sqrt{d}| \leq 2\sqrt{d} + 1/q^2$$

$$\leq 2\sqrt{d} + 1$$

Per Pigeonhole, trovo infinite coppie (p,q) t.c. $N(p+\sqrt{d}\,q) = N$, per almeno un N tra $-2\sqrt{d}-1$ e $2\sqrt{d}+1$.

Tra questi, $\exists\ (p_1, q_1)$ e (p_2, q_2) con $p_1 \equiv p_2$ e $q_1 \equiv q_2 \pmod N$: il loro rapporto è intero ed ha norma 1.

$(p_1, q_1) \neq (p_2, q_2)$ $\quad p_1, q_1, p_2, q_2 > 0$

Se z è una soluzione $\neq 1$, allora

$\| \quad x + \sqrt{d}\, y$

$$N(z^n) = N(z)^n = 1$$

e quindi z^n è una soluzione.

Lo stesso vale per $(-z^n)$: infatti

$$N(-z^n) = N(-1)\, N(z^n) = N(-1 + 0\sqrt{d}) = 1$$

Soluzione fondamentale f

è il minimo $z > 1$ tale che $N(z) = 1$

Oss: $\frac{1}{z} = \frac{1}{x+\sqrt{d}\,y} \cdot \frac{x-\sqrt{d}\,y}{x-\sqrt{d}\,y} = \frac{x-\sqrt{d}\,y}{1}$

Hope Tutte le soluzioni sono della forma $\pm f^n$, dove n è un intero (non necessariamente positivo)

Dim. Sia z una soluz. Sostituendo z con $-z$ possiamo supporre $z > 0$.

Esiste un unico n t.c. $f^n \le z < f^{n+1}$

$N(\underbrace{z \cdot f^{-n}}_{a+b\sqrt{d},\ a \in \mathbb{Z},\ b \in \mathbb{Z}}) = 1$

$|a+b\sqrt{d}| = |z| \cdot |f|^{-n} < f$

≤ 1

Per definiz. di f, $z \cdot f^{-n} = 1 \Rightarrow z = f^n$ ∎

Esempio $x^2 - 3y^2 = 1$

Cerchiamo (x,y) più piccoli possibile.

$y = 0 \Rightarrow x = 1$ NO

$y = 1 \Rightarrow x = \pm 2$ $\quad f = 2 + \sqrt{3}$

f^2 è soluzione: $\quad f^2 = 4 + 3 + 4\sqrt{3}$

$(x, y) = (7, 4)$

Tutte le soluzioni sono della forma

$$\pm (2+\sqrt{3})^n$$

ovvero

$$x = \frac{(2+\sqrt{3})^n + (2-\sqrt{3})^n}{2}$$

$$y = \frac{(2+\sqrt{3})^n - (2-\sqrt{3})^n}{2\sqrt{3}}$$

Trovare la fondamentale

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

$$\frac{2}{1} < \sqrt{7} < \frac{3}{1}$$

$$\frac{2}{1} \oplus \frac{3}{1} = \frac{5}{2} \qquad \frac{5}{2} < \sqrt{7} < \frac{3}{1}$$

$$\frac{5}{2} \oplus \frac{3}{1} = \frac{8}{3} \qquad 8^2 - 7 \cdot 3^2 = 1$$

$$\frac{a}{b} \oplus \frac{c}{d} = \frac{a+c}{b+d} \quad \text{(FAREY)}$$

Algoritmo Si parte da $\frac{n}{1} < \sqrt{d} < \frac{n+1}{1}$, con n intero.

Ad ogni passo abbiamo una disuguaglianza $a/b < \sqrt{d} < e/f$. Proviamo se

$$a^2 - db^2 = 1 \quad \text{o} \quad e^2 - df^2 = 1$$

Se sì, fine. Se no, consideriamo $\frac{a+e}{b+f}$ e otteniamo una nuova disug.

$$\frac{a+e}{b+f} < \sqrt{d} < \frac{e}{f} \quad \text{oppure} \quad \frac{a}{b} < \sqrt{d} < \frac{a+e}{b+f}$$

Esercizio Se $(m+1)^3 - m^3 = n^2$, allora

$2n-1$ è un quadrato

$3m^2+3m+1 = n^2$

$3\left(m+\frac{1}{2}\right)^2 + \frac{1}{4} = n^2$

$3(2m+1)^2 + 1 = (2n)^2$

$(2n, 2m+1)$ è una soluz. di $x^2 - 3y^2 = 1$

$2n + (2m+1)\sqrt{3} = (2+\sqrt{3})^k$

k è dispari, altrimenti $\dfrac{(2+\sqrt{3})^k + (2-\sqrt{3})^k}{2}$

è dispari

$$2n-1 = \frac{(2+\sqrt{3})^k + (2-\sqrt{3})^k - 2}{2}$$

$$= \frac{2(2+\sqrt{3})(2+\sqrt{3})^{k-1} + 2(2-\sqrt{3})(2-\sqrt{3})^{k-1} - 2\cdot 2}{2\cdot 2}$$

Oss $(1+\sqrt{3})^2 = 4 + 2\sqrt{3} = 2(2+\sqrt{3})$

$$2n-1 = \left(\frac{(1+\sqrt{3})(2+\sqrt{3})^{(k-1)/2} + (1-\sqrt{3})(2-\sqrt{3})^{\frac{k-1}{2}}}{2}\right)^2$$

Pell generalizzate

(*) $x^2 - dy^2 = m \iff N(x + \sqrt{d}\, y) = m$

E' comunque importante studiare $x^2 - dy^2 = 1$.

Sia f la fondamentale.

(1) Se z e' una soluzione di (*), allora $\pm z \cdot f^n$ sono tutte soluzioni:

$$N(z \cdot f^n) = \underbrace{N(z)}_{m} \cdot \underbrace{N(f)^n}_{1} = m$$

(2) $z = x + \sqrt{d}\, y \rightsquigarrow$ **$x/y \bmod m$**

Esistono al piu' $\varphi(|m|)$ soluzioni

$z_1, \dots, z_k \quad (k \le \varphi(|m|))$

tali che ogni soluzione sia della forma

$$\pm z_i \cdot f^n$$

(3) $x/y \bmod m$ ha senso solo se $1 = (y, m)$

Altrimenti c'e' p che divide x, y, m

Se $m = -1$ o ± 2 c'e' al piu' una famiglia di soluzioni.

Problema: come decido se $x^2 - 82y^2 = 2$ ha o meno soluzioni?

Prendiamo uno z t.c. $N(z) = m$

Moltiplicando per f^n con n opportuno trovo un'altra soluzione nell'intervallo

$$\left[\sqrt{\frac{|m|}{f}}, \sqrt{|m|} \cdot \sqrt{f} \right]$$

$$x = \text{"}\frac{z+\bar{z}}{2}\text{"} = \frac{z + m/z}{2}$$

$z = x + y\sqrt{d}$

$\bar{z} = x - y\sqrt{d}$

$$z\bar{z} = N(z) = x^2 - dy^2 = m$$

Diciamo $m > 0$. La funzione

$$z \longmapsto \frac{z + m/z}{2}$$

è convessa, quindi il suo massimo sta in un estremo. Negli estremi questa funzione vale $\frac{1}{2}\left(\sqrt{|m| \cdot f} + \sqrt{\frac{|m|}{f}}\right)$

$$= \frac{f+1}{2\sqrt{f}} \cdot \sqrt{|m|}$$

Caso concreto $\quad x^2 - 82y^2 = 2$

$$x^2 - 82y^2 = 1$$

$$N(9+\sqrt{82}) = (9+\sqrt{82})(9-\sqrt{82})$$

$$= 81 - 82 = -1$$

$$\Rightarrow N\left((9+\sqrt{82})^2\right) = +1$$

$$\| $$

$$N\left(81+82+18\sqrt{82}\right) = N\left(163+18\sqrt{82}\right)$$

$$f < 343$$

Fatto di pagina prima $\Rightarrow$ se c'è una soluz., ce n'è una in cui $x \leq \dfrac{f+1}{2\sqrt{f}}\sqrt{2}$

$$\leq \frac{1}{2}\frac{\cancel{344}^{172}}{\cancel{18}^{6}}\cancel{\frac{3}{2}} < 15$$

Mod $41 \Longrightarrow \quad x^2 - 82y^2 \equiv 2 \quad (41)$

$$x^2 \equiv 2 \quad (41)$$

$$\Downarrow$$

$$x \equiv \pm 17 \quad (41)$$

Un tale x non esiste!

Aside Se $p \equiv 3 \ (4)$ e $\left(\frac{a}{p}\right) = +1$, allora le radici quadrate di a mod p sono date da $\pm a^{\frac{p+1}{4}}$

$$\left(a^{\frac{p+1}{4}}\right)^2 \equiv a^{\frac{p+1}{2}} \equiv a^{\frac{p-1}{2}+1} \equiv \underbrace{a^{\frac{p-1}{2}}}_{\left(\frac{a}{p}\right) = +1} \cdot a$$

Sia $a \in \mathbb{N}$ e $d = a^2 - 1$. Se x, y sono tali che $m = x^2 - dy^2$ e' (in valore assoluto) $< 2a+2$, allora $|m|$ e' un quadrato perfetto.

Prendiamo dei tali x, y con x il piu' piccolo possibile.

Fondamentale = soluz. di $x^2 - (a^2-1)y^2 = 1$ più piccola $= a + \sqrt{d}$

$$x \leq \frac{f+1}{2\sqrt{f}} \cdot \sqrt{|m|} = \sqrt{\frac{a+1}{2}} \sqrt{|m|}$$

$$\Leftrightarrow \frac{(f+1)^2}{4f} = \frac{a+1}{2}$$

$$\Leftrightarrow \left(a^2 + a^2 \cancel{-1} + 2a\sqrt{d} \cancel{+1} + 2a + 2\sqrt{d}\right) \stackrel{?}{=} 2f(a+1)$$

$$\Leftrightarrow 2a^2 + 2a\sqrt{d} + 2a + 2\sqrt{d} \stackrel{?}{=} 2f(a+1)$$

□

$$x \le \sqrt{\frac{a+1}{2}}\sqrt{|m|} < \sqrt{\frac{a+1}{2}}\sqrt{2(a+1)}$$

$$= a+1$$

$$x^2 - dy^2 = 1$$

$$dy^2 = x^2 - 1 \le a^2 - 1$$

$$y^2 \le \frac{a^2-1}{d} = 1$$

Quindi esistono $x \le a$ e $y \in \{0,1\}$ t.c.

$$m = x^2 - dy^2$$

Per $y = 0 \Rightarrow m = x^2$

Per $y = 1 \Rightarrow \begin{cases} m = x^2 - (a^2-1) \\ x = a \end{cases} \Rightarrow m = 1$

□

$3^n - 2$ è un quadrato $\iff$ $n = 1, 3$

Mod 4 $\Rightarrow$ n è dispari

$$3^n - 2 = y^2 \qquad 3x^2 - 2 = y^2$$

$$(*)\ y^2 - 3x^2 = -2$$

$\varphi(|-2|) = 1$: una famiglia di soluzioni

$$N(1+\sqrt{3}) = -2$$

Fondamentale: $y^2 - 3x^2 = 1$ $\qquad f = 2+\sqrt{3}$

Tutte le soluzioni (positive) della (*) sono

$$y + x\sqrt{3} = (1+\sqrt{3})(2+\sqrt{3})^\ell$$

x dev'essere una potenza di 3. Guardiamo mod 9.

$$x_\ell = \frac{(1+\sqrt{3})(2+\sqrt{3})^\ell - (1-\sqrt{3})(2-\sqrt{3})^\ell}{2\sqrt{3}}$$

$$= \frac{(1+\sqrt{3})^{2\ell+1} - (1-\sqrt{3})^{2\ell+1}}{2\sqrt{3}\cdot 2^\ell}$$

$$b_\ell = 2^\ell x_\ell$$

$$X \equiv (2\ell+1) + \frac{(2\ell+1)(2\ell)(2\ell-1)}{6}\cdot 3 \bmod 9$$

$$\equiv (2\ell+1)\underbrace{\left(1 + \ell(2\ell-1)\right)}_{\not\equiv 0 \ (3)} \bmod 9$$

$$\Rightarrow \ell \equiv 4 \bmod 9$$

b_ℓ è una potenza di 3 $\Rightarrow \ell \equiv 4 \ (9)$

$$\Rightarrow b_9 \mid b_\ell$$

Se b_9 non è una potenza di 3, lo stesso vale per X_ℓ.

(e non per colpa dei fattori 2!)

Sia $a = (1+\sqrt{3})^9$ e $b = (1-\sqrt{3})^9$

Mi chiedo se $\frac{a-b}{2\sqrt{3}}$ divida $\frac{a^n - b^n}{2\sqrt{3}}$

Funziona perché il rapporto è

$$\underbrace{a^{n-1} + a^{n-2}b + \dots + b^{n-1}}_{\text{intero}}$$

$$a^{n-2}b + b^{n-2}a = \text{intero}$$

$$(1+\sqrt{3})^3 = (1+3\cdot 3) + \sqrt{3}\,(3+3)$$

$$= (10 + 6\sqrt{3})$$

$$(10+6\sqrt{3})^3 = 8\,(5+3\sqrt{3})^3 = \dots$$

Alla fine, $X_g = 9 \cdot 17$, quindi X_ℓ non è una potenza di 3

$$\sum_{k|n} \varphi(k) = n$$

Verifichiamola se $n = p^m$

$$\sum_{k|p^m} \varphi(k) = \sum_{j=0}^{m} \varphi(p^j) =$$

$$= 1 + \sum_{j=1}^{m} (p-1)\, p^{j-1}$$

$$= 1 + (p-1) \sum_{j=0}^{m-1} p^j =$$

$$= 1 + (p-1)\, \frac{p^m - 1}{p-1} = p^m$$

$$\sum_{k \mid ab} \varphi(k) = \sum_{\substack{k_1 \mid a \\ k_2 \mid b}} \varphi(k_1 k_2)$$

$(a,b) = 1$

$$= \sum_{\substack{k_1 \mid a \\ k_2 \mid b}} \varphi(k_1)\,\varphi(k_2)$$

$$= \underbrace{\left(\sum_{k_1 \mid a} \varphi(k_1) \right)}_{a} \underbrace{\left(\sum_{k_2 \mid b} \varphi(k_2) \right)}_{b}$$