TEORIA DEI NUMERI 2 - MEDIUM

Titolo nota 08/09/2019

Estensioni quadratiche

d intero, non quadrato

$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \text{ con } a, b \text{ interi}\} \subseteq \mathbb{C}$

$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \text{ con } a, b \text{ razionali}\} \subseteq \mathbb{C}$

Se d non è quadrato mod p,

$\mathbb{F}_p[\sqrt{d}] = \{a + b\sqrt{d} \text{ con } a, b \in \mathbb{F}_p\}$

$\mathbb{F}_p \hookrightarrow \mathbb{Z}/p\mathbb{Z}$

$$(a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) = a_1a_2 + \sqrt{d}(a_1b_2 + b_1a_2) + db_1b_2$$

Pell $x^2 - dy^2 = 1$, d intero fissato $\neq \square$, $d > 0$

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

Norma: dato $z = a + \sqrt{d}\,b$ (con a, b razionali), la sua NORMA è $N(z) = a^2 - db^2 = (a + b\sqrt{d})(a - b\sqrt{d})$

Oss $N(z_1 \cdot z_2) = N(z_1) \cdot N(z_2)$ [ci fidiamo]

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

$$N\left(\frac{1}{z}\right)\cdot N(z) = N(1) = 1$$

$$\Rightarrow N(1/z) = 1/N(z)$$

$$N\left(z_1/z_2\right) = N(z_1 \cdot 1/z_2) = N(z_1)\cdot N(1/z_2)$$

$$= N(z_1)/N(z_2)$$

$$z = a + b\sqrt{d} \qquad \frac{1}{z} = \frac{1}{a+b\sqrt{d}} = \frac{a-b\sqrt{d}}{a^2-db^2}$$

$a^2 - db^2 \neq 0$ perché $d \neq \square$

Idea: se voglio $N(z)=1$, mi basta trovare z_1, z_2 con $N(z_1)=N(z_2)$ e poi prendere $z = z_1/z_2$

Idea 2: $x^2 - dy^2 = 1 \Rightarrow \left(\frac{x}{y}\right)^2 - d = \frac{1}{y^2}$

$$\Rightarrow \left|\frac{x}{y} - \sqrt{d}\right| \cdot \left|\frac{x}{y} + \sqrt{d}\right| = 1/y^2$$

Soluzioni della Pell = approssimazioni razionali molto precise di $\sqrt{d}$

Esempio: BMO 2015/4

Dati 20 interi consecutivi (positivi), ce n'è uno — chiamiamolo d — t.c.

$$n\sqrt{d}\left\{n\sqrt{d}\right\} > 5/2$$

per ogni n.

Soluzione Scriviamo $\{n\sqrt{d}\} = n\sqrt{d} - m > 0$

$$2n\sqrt{d} \cdot \left(n\sqrt{d} - m\right) > 5$$

$$\| \quad (n\sqrt{d} + m)$$

$$d n^2 - m^2$$

$$\left(2n\sqrt{d}\right) > \left(n\sqrt{d} - m\right) \cdot \left(n\sqrt{d} + m\right) = d n^2 - m^2 \overset{?}{\geq} 5$$

$$\left(n\sqrt{d} - m\right)$$

Siamo tristi se $d n^2 - m^2 = 1, 2, 3, 4$

Obiettivo: scegliere d in modo che queste equaz. non abbiano soluzione

Congruenze, e il testo suggerisce mod $\begin{cases} 4 \\ 5 \end{cases}$

Se $5 \mid d$: $\quad -m^2 \equiv 1, \cancel{2}, \cancel{3}, 4 \quad (5)$

Resta da fare una congr. mod 4 per vietare 1, 4.

Vogliamo escludere: -1 è un R.Q. mod d.

Sarebbe bello: d è un primo $\equiv 3\ (4)$

Basta: d è divisibile per $p \equiv 3\ (4)$

" : $d \equiv 3\ (4)$

" : $d \equiv 15\ (20)$ □

Teo Se $d>0$, $d \neq \square$, l'equazione

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

ha sempre soluz. (intera) $\neq (\pm 1, 0)$

Dim. Per pigeonhole, dato $\sqrt{d}$ (che è irraz.) so trovare ∞ coppie (x_n, y_n) di interi t.c.

$$\left| \frac{x_n}{y_n} - \sqrt{d} \right| < \frac{1}{y_n^2}$$

$$\left| x_n^2 - d y_n^2 \right| = y_n^2 \left| \left(\frac{x_n}{y_n}\right)^2 - d \right|$$

$$= y_n^2 \cdot \left| \frac{x_n}{y_n} - \sqrt{d} \right| \cdot \left| \frac{x_n}{y_n} + \sqrt{d} \right| < \left| \frac{x_n}{y_n} + \sqrt{d} \right|$$

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

Per pigeonhole trovo ∞ coppie x_n, y_n per cui $x_n^2 - d y_n^2$ assume lo stesso valore N

$$N \left(x_n + \sqrt{d}\, y_n \right)$$

Scegliamo due tali coppie, (x_0, y_0) e (x_1, y_1) con

$$N\left(x_i + \sqrt{d}\, y_i \right) = 1.$$

$$N\left(\frac{x_0 + \sqrt{d}\, y_0}{x_1 + \sqrt{d}\, y_1} \right) = \frac{N\left(x_0 + \sqrt{d}\, y_0\right)}{N\left(x_1 + \sqrt{d}\, y_1\right)} = \frac{N}{N} = 1$$

$a + b\sqrt{d}$ MA A PRIORI a, b razionali

$$\frac{(X_0+\sqrt{d}\,Y_0)(X_1-\sqrt{d}\,Y_1)}{(X_1+\sqrt{d}\,Y_1)(X_1-\sqrt{d}\,Y_1)} = \frac{(X_0X_1-dY_0Y_1)+\sqrt{d}\,(X_1Y_0-X_0Y_1)}{N}$$

Vogliamo fare in modo che $\begin{cases} X_1Y_0 \equiv X_0Y_1 \ (N) \\ X_0X_1 \equiv dY_0Y_1 \ (N) \end{cases}$

Per esempio andrebbe bene se $(*)\begin{cases} X_0 \equiv X_1 \ (N) \\ Y_0 \equiv Y_1 \ (N) \end{cases}$:

allora $X_1Y_0 \equiv X_0Y_1$ è ovvio e

$$X_0X_1 - dY_0Y_1 \equiv X_0^2 - dY_0^2 \equiv N \equiv 0 \ (N)$$

Per pigeonhole di nuovo, trovo due coppie con la stessa norma N e tale che $(*)$ valga ☒

Verso l'infinito e oltre

$$X^2 - 2Y^2 = 1 \qquad 3^2 - 2\cdot 2^2 = 1$$

$$N(3+2\sqrt{2})$$

$$\Rightarrow N\left((3+2\sqrt{2})^2\right) = N(3+2\sqrt{2})^2 = 1$$

$$N(17+12\sqrt{2})$$

Trovo ∞ soluz. considerando $(3+2\sqrt{2})^n$: ∞ soluz sono date da

$$X_n = \frac{1}{2}\left[(3+2\sqrt{2})^n + (3-2\sqrt{2})^n\right]$$

$$Y_n = \frac{1}{2\sqrt{2}}\left[(3+2\sqrt{2})^n - (3-2\sqrt{2})^n\right]$$

Teo Sia $x_0 + \sqrt{d}\, y_0 = f$ la più piccola soluzione di $x^2 - dy^2 = 1$ $\boxed{\begin{matrix} x_0 > 0 \\ y_0 > 0 \end{matrix}}$

└ minimo $x > 1$

Allora ogni soluzione di $x^2 - dy^2$ è della forma $\pm f^k$ per un certo $k \in \mathbb{Z}$.

Dim Sia (u, v) una soluzione, sia $g = u + \sqrt{d}\, v$

Posso supporre wlog $g > 0$, e voglio dim $g = f^k$.

Osservo che $f^{-1} = x_0 - \sqrt{d}\, y_0$ $\quad (N(f) = 1)$

Scegliamo k in modo che

$$f^k \leq g < f^{k+1} \qquad (f > 1)$$

$$\Downarrow$$

$$1 \leq \underbrace{f^{-k} g}_{\in \mathbb{Z}[\sqrt{d}],\ N(f^{-k} g) = 1} < f$$

cioè $f^{-k} g$ è una soluz. della Pell. Siccome f era la più piccola soluzione > 1, questo vuol dire che $f^{-k} g = 1$ □

Oss f è detta la SOLUZIONE FONDAMENTALE

ALGORITMO PER TROVARE LA SOLUZ. FONDAM.

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

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

$$\frac{5}{2} = \frac{2+3}{1+1}$$

$5^2 - 7\cdot 2^2 = -3$ NO

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

$$\frac{5+3}{2+1} = 8/3$$

$8^2 - 7\cdot 3^2 = 1$: la fondam. e' $(8,3)$, o in modo equivalente $8 + 3\sqrt{7}$

Esempio: $p \equiv 1 \ (4)$. L'eqz $x^2 - py^2 = -1$ ha ∞ soluzioni

Infinite soluz sono gratis a partire da una: se (u,v) e' soluz e $g = u + v\sqrt{p}$, allora g^{2k+1} e' ancora soluz.

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

Ma anche $g \cdot f^k$ sono soluzioni ... ispirazione: magari $g = \sqrt{f}$

(e in effetti e' l'unica speranza: $N(g) = -1$

$\Rightarrow N(g^2) = 1 \Rightarrow g^2 = f^n$, e n deve essere dispari ...)

Sia $f = a + b\sqrt{p}$, $g = c + d\sqrt{p}$: sto cercando di risolvere $\begin{cases} c^2 + pd^2 = a \\ 2cd = b \end{cases}$, e so $\boxed{a^2 - pb^2 = 1}$

$$(a+1)(a-1) = pb^2$$
$$\| \qquad\qquad \|$$
$$4 \qquad\quad 4pe^2$$

Oss: $1 = a^2 - pb^2 \equiv a^2 - b^2 \pmod 4$

$\Rightarrow$ a dispari, b pari $= 2e$

$$\left(\frac{a+1}{2}\right)\left(\frac{a-1}{2}\right) = p\cdot e^2$$

$$\begin{cases} \frac{a\pm 1}{2} = \ell^2 \\ \frac{a\mp 1}{2} = p m^2 \end{cases} \Rightarrow \begin{array}{l} a = \ell^2 + p m^2 \\ b = 2e \end{array}$$

Siamo riusciti a far vedere che $\sqrt{f} \in \mathbb{Z}[\sqrt{p}]$, e ci siamo. □

Oss Se $x^2 - dy^2 = a$ ha una soluz, allora ne ha ∞: se c'è soluzione (u,v), allora $N(\underbrace{u+v\sqrt{d}}_{g}) = a$, e quindi $N(g\cdot f^k) = a \ \forall k$.

Esempio: $y^2 - 5183x^2 = 2$

Vorremmo far vedere che non ne esistono.

Sia (u,v) una soluz, $g = u + v\sqrt{5183}$ e f una soluz. fondam.

$$5183 = 72^2 - 1$$

La fondam. è quindi $f = 72 + \sqrt{5183} \approx 144$

$$f^{-1} = 72 - \sqrt{5183}$$

Morale: vorrei aggiustare g con potenze di f per avere informaz. su quanto è grande x.

$$y = \frac{g \cdot f^k + 2g^{-1} f^{-k}}{2} \qquad \text{(No, ma quasi)}$$

$$g \cdot f^k = a + b\sqrt{5183}$$

$$a - b\sqrt{5183} = \frac{2}{a + b\sqrt{5183}}$$

Per ottimizzare vorrei che $g \cdot f^k$ e $2g^{-1} f^{-k}$ fossero "dello stesso ordine di grandezza"

$$\times f^k \in \left[\frac{\sqrt{a}}{\sqrt{f}}, \sqrt{a}\sqrt{f} \right]$$

$$X \cdot f^k + \frac{a}{X \cdot f^k} \leq \max \left\{ \frac{\sqrt{a}}{\sqrt{f}} + \frac{a\sqrt{f}}{\sqrt{a}}, \sqrt{af} + \frac{\sqrt{a}}{\sqrt{f}} \right\}$$

$$= \sqrt{a} \cdot \left(\sqrt{f} + \frac{1}{\sqrt{f}} \right)$$

Nel nostro caso particolare: se c'è una soluz, ce n'è una con $|y| \leq \frac{1}{2}\sqrt{2}\left(\sqrt{f} + \frac{1}{\sqrt{f}}\right)$

$$\leq \frac{\sqrt{2}}{2}\left(12 + 1\right) < 13$$

$y^2 - 5183X^2 = 2$ il membro sinistro sarebbe negativo!

Oss OVVIAMENTE il primo tentativo DOVEVA essere modulo $71 \cdot 73 = 5183$ (ma non funziona)

Lemma Se $x^2 - dy^2 = a$ ha una soluzione, ne ha una con $|x| \leq \frac{1}{2}\sqrt{a}\left(\sqrt{f} + 1/\sqrt{f}\right)$

Esempio: IMO SL 2016/N5

Sia $a>0$ intero, $a \neq \square$, e consideriamo, per $K>0$, l'equazione $K = \dfrac{x^2-a}{x^2-y^2}$. Siano

$A = \{ K \mid$ c'è una soluz con $x > \sqrt{a} \}$

$B = \{ K \mid$ ——————— $0 \leq x < \sqrt{a} \}$

Dim. che $A = B$

Soluzione $K(x^2-y^2) = x^2-a$

$(K-1)x^2 - Ky^2 = -a$

$\Rightarrow \quad ((K-1)x)^2 - K(K-1)y^2 = -a(K-1)$

$w^2 - K(K-1)y^2 = -a(K-1)$

$\boxed{B \subseteq A}$ Idea di base: prendere una soluz "piccola" e moltiplicarla per una potenza della fondamentale

Parto da $(w_0 + y_0\sqrt{K(K-1)})$ e moltiplico per la fondam. $(u + v\sqrt{K(K-1)}) = f$

$= \left(\underbrace{w_0 u}_{\equiv 0 (K-1)} + \underbrace{y_0 v K(K-1)}_{\equiv 0 (K-1)} + \sqrt{K(K-1)}(w_0 v + u y_0) \right)$

Moltiplicando per f^n con n grande trovo una soluz. grande (con $\dfrac{w}{K-1}$ intero)

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

$3 + 2\sqrt{2} = f$

$3 - 2\sqrt{2} = f^{-1}$

$17 - 8\sqrt{2} = f^{-2}$

$\vdots$

i coefficienti crescono!

$\boxed{A \subseteq B}$ Bisogna davvero capire chi è la fondamentale

Cerchiamo davvero f: $\quad y^2 - k(k-1)x^2 = 1$

Una soluzione è $(2k-1, 2)$. È la fondam.

perché $x = 1$ non è soluz $\left(k^2 - k + 1 = \square \dots \right)$

$(k-1)y^2 - kx^2 = 1$: con -1 la so fare,

e la soluz. è $(1,1)$ "$\rightsquigarrow$" $\sqrt{k-1} + \sqrt{k}$

$\square$

$\rightsquigarrow 2k - 1 + 2\sqrt{k(k-1)}$

Applichiamo il macchinario: la Pell

$$w^2 - k(k-1)x^2 = -a(k-1),$$

che per hp ha una soluz, ne ha anche una con

$$|w| \leq \frac{1}{2}\sqrt{a(k-1)} \cdot \left(\sqrt{f} + \frac{1}{\sqrt{f}} \right)$$

$|w| = |(k-1)x|$

$$\Rightarrow |x| \leq \frac{1}{2}\sqrt{a}\,\frac{1}{\sqrt{k-1}}\left(\sqrt{f} + \frac{1}{\sqrt{f}} \right) \overset{?}{\leq} \sqrt{a}$$

$$\iff \sqrt{f} + \frac{1}{\sqrt{f}} \leq 2\sqrt{k-1}$$

$\iff \quad f + \frac{1}{f} + 2 \leq 4(k-1)$

$4k - 2 + 2 \leq 4k - 4$ che è un po' falsa..

Riproviamo: $\boxed{A \subseteq B}$

Riscriviamo in termini di x, y la trasformazione "soluz $\longrightarrow$ soluz $\times$ fondam^{-1}" che abbiamo nelle var. (w, y)

$$\left(w + \sqrt{k(k-1)}\, y\right) \cdot \left((2k-1) - 2\sqrt{k(k-1)}\right) =$$

$$= \left((2k-1)w - 2k(k-1)y + \sqrt{k(k-1)}\left(-2w + (2k-1)y\right)\right)$$

Siccome $w = (k-1)x$ abbiamo che se (x,y) è soluz, anche $\begin{cases} x' = (2k-1)x - 2ky \\ y' = 2(k-1)x - (2k-1)y \end{cases}$ è soluz.

Sia (x,y) la soluz MINIMA con $x > \sqrt{a}$, wlog $y > 0$

Se $|x'| < x$, allora (x', y') deve risp. $|x'| < \sqrt{a}$

- $x' < x$: $\quad (2k-1)x - 2ky < x$

$$\frac{k-1}{k}x < y \iff \left(\frac{k-1}{k}\right)^2 x^2 < y^2$$

testo $\rightarrow$ $= \dfrac{(k-1)x^2 + a}{k}$

$\iff (k-1)^2 x^2 < k(k-1)x^2 + ka$, vera perché $k, a > 0$

- $x' > -x \qquad (2k-1)x - 2ky > -x$

$$\iff \quad 2kx > 2ky \quad (=) \quad x^2 > y^2$$

$$0 < K = \frac{X^2 - a}{X^2 - y^2} \begin{matrix} > 0 \\ > 0 \end{matrix}$$

II

Diamo un senso alle congruenze mod p con $\sqrt{d}$

Esempio $F_0 = 0$, $F_1 = 1$, ..., $F_{n+1} = F_n + F_{n-1}$.

Dim che $F_* \equiv 0 \ (p)$ per ogni p primo, $p \neq 5$

$*$ ↝ una qualche funzione semplice di p

$$F_n = \frac{1}{\sqrt{5}} \left[\varphi^n - \left(-\frac{1}{\varphi}\right)^n \right] \qquad \varphi = \frac{1+\sqrt{5}}{2}$$

$$-1/\varphi = \frac{1-\sqrt{5}}{2}$$

$$F_n \equiv 0 \ (p) \iff \boxed{\varphi^n \equiv (-1/\varphi)^n \mod p}$$

Caso 1: $p \neq 2$ e 5 è un quadrato mod p

Scelgo $a \in \mathbb{Z}$ con $a^2 \equiv 5 \mod p$

$$\left(\frac{a+1}{2}\right)^n \equiv \left(\frac{1-a}{2}\right)^n \mod p$$

è verificata per $n \equiv 0 \ (p-1)$

Caso 2: $p \neq 2$ e 5 NON è un quadrato mod p

Diamo alla congruenza mod p il seguente significato:

$a + b\sqrt{5} \equiv c + d\sqrt{5} \mod p$ (con $a, b, c, d \in \mathbb{Z}$)

se e solo se $a \equiv c$, $b \equiv d \mod p$

Oss Se 5 fosse $\equiv n^2 \bmod p$, le due espressioni

$$n + 0\sqrt{5} \quad \text{e} \quad 0 + 1\sqrt{5}$$

"avrebbero voglia" di essere congrue mod p, ma è difficile formalizzarlo.

$$F_n \equiv 0 \ (p) \iff 2^n F_n \equiv 0 \ (p)$$

$$\iff (1+\sqrt{5})^n \equiv (1-\sqrt{5})^n \bmod p$$

$$\iff (1+\sqrt{5})^{2n} \equiv (1-5)^n \bmod p$$

Se $a_1 + b_1\sqrt{5} \equiv a_2 + b_2\sqrt{5}$ (p) e

$c_1 + d_1\sqrt{5} \equiv c_2 + d_2\sqrt{5}$ (p)

allora $(a_1 + b_1\sqrt{5})(c_1 + d_1\sqrt{5}) \equiv (a_2 + b_2\sqrt{5})(c_2 + d_2\sqrt{5})$ (p)

La dim è scrivere $a_2 = a_1 + kp_1$ etc e sviluppare !

Il piccolo teo di Fermat "fallisce":

$$X = 1 + \sqrt{5} \bmod 3$$

$$X^2 = 6 + 2\sqrt{5} \equiv -\sqrt{5} \bmod 3$$

Teo (Fermat ++) $(a + b\sqrt{d})^{p^2-1} \equiv 1 \bmod p$, $p > 2$

Dim. Basta far vedere che $(a+b\sqrt{d})^{p+1} \equiv c + 0\sqrt{d}$ (p)

Calcoliamo $(a + b\sqrt{d})^p \equiv a^p + \binom{p}{1} a^{p-1} b\sqrt{d} + \dots$

$$+ \binom{p}{p-1} a (b\sqrt{d})^{p-1} + b^p \sqrt{d}^{\,p-1} \cdot \sqrt{d}$$

$$\equiv a^p + b^p d^{\frac{p-1}{2}} \sqrt{d} \equiv a + b d^{\frac{p-1}{2}} \sqrt{d} \quad (p)$$

└ piccolo di Fermat

Per Eulero, $d^{\frac{p-1}{2}} \equiv -1 \ (p)$, quindi

$$(a+b\sqrt{d})^p \equiv a - b\sqrt{d} \mod p$$

$$\Rightarrow (a+b\sqrt{d})^{p+1} \equiv a^2 - db^2 \mod p$$

$$\Rightarrow (a+b\sqrt{d})^{p^2-1} = (\underbrace{a^2-db^2}_{\neq 0})^{p-1} \equiv 1 \mod p$$

└ FLT

□

Esempio $(1+\sqrt{2})^k \mod 3$

$k=2$: $3+2\sqrt{2} \equiv -\sqrt{2} \mod 3$

$k=4$: $2 = (1+\sqrt{2})(1-\sqrt{2}) \equiv 1-2 \equiv 2 \ (3)$

$k=8$: 1

$(1+\sqrt{5})^n \equiv (1-\sqrt{5})^n \mod p$: sicuramente vera per $n = p^2-1$, perché entrambi i membri sono $\equiv 1 \mod p$, ma è vera anche per $n = p+1$ perché allora sono entrambi congrui a $N(1+\sqrt{5}) \equiv N(1-\sqrt{5}) \equiv -4 \ (p)$

Esempio $a_0 = 2$, $a_{n+1} = 2a_n^2 - 1$. Sia p un primo che divide a_n $(n>0)$. Allora

$$p \equiv \pm 1 \mod 2^{n+2}$$

Soluzione $\cos(2\theta) = 2\cos^2\theta - 1$

Se per caso $a_0 = \cos(\theta_0)$, $a_1 = 2\cos^2(\theta_0) - 1 = \cos(2\theta_0)$,

$\dots, \quad a_n = \cos\left(2^n \theta_0\right)$

Ma $\cos\theta_0 = \dfrac{e^{i\theta_0} + e^{-i\theta_0}}{2}$ e

$$a_n = \cos\left(2^n\theta_0\right) = \frac{\left(e^{i\theta_0}\right)^{2^n} + \left(e^{-i\theta_0}\right)^{2^n}}{2} = \frac{A^{2^n} + A^{-2^n}}{2}$$

Scritta bene: se $a_n = \frac{1}{2}\left(A^{2^n} + A^{-2^n}\right)$, allora

$$a_{n+1} = 2a_n^2 - 1 = 2\frac{1}{4}\left(A^{2^{n+1}} + A^{-2^{n+1}} + 2\right) - 1.$$

Basta quindi scegliere A in modo t.c.

$$A + A^{-1} = 4 \qquad (a_0 = 2)$$

$$A^2 - 4A + 1 = 0 \iff A = 2 \pm \sqrt{3}$$

$$2a_n = \left(2+\sqrt{3}\right)^{2^n} + \left(2-\sqrt{3}\right)^{2^n} \overset{?}{\equiv} 0 \ (p)$$

$$\left(2+\sqrt{3}\right)^{2^n} \equiv -\left(2-\sqrt{3}\right)^{2^n} \pmod p$$

$$\left(2+\sqrt{3}\right)^{2^{n+1}} \equiv -1 \pmod p$$

$$\Rightarrow \operatorname{ord}_p\left(2+\sqrt{3}\right) = 2^{n+2}$$

- Se 3 è un residuo quad. mod p, allora posso applicare il piccolo Teo Fermat "usuale" per ottenere $2^{n+2} \mid \varphi(p) = p-1$
- Se 3 NON è res. quad. mod p, il FLT "potenziato" dà $2^{n+2} \mid p^2 - 1 = (p-1)(p+1)$, che fornisce solo $p \equiv \pm 1 \ (2^{n+1})$

MA possiamo osservare che $(2+\sqrt{3})^{p+1} \equiv (2+\sqrt{3})(2-\sqrt{3})$

$\equiv 1 \ (p) \implies 2^{n+2} \mid p+1$ □

Combiniamo tutto!

Sia $n>0$. Dim. che esistono a,b interi >1 t.c.

$a^2+1 = 2b^2$ e $a \equiv b \pmod{n}$

Soluzione $a^2 - 2b^2 = -1$ ha come soluzioni

- $(1,1)$ è soluz $\rightsquigarrow$ $g = 1+\sqrt{2}$
- Infinite soluzioni: $(1+\sqrt{2})(3+2\sqrt{2})^k = (1+\sqrt{2})^{2k+1}$

$$a_k = \frac{1}{2}\left[(1+\sqrt{2})^{2k+1} + (1-\sqrt{2})^{2k+1}\right]$$

$$b_k = \frac{1}{2\sqrt{2}}\left[(1+\sqrt{2})^{2k+1} - (1-\sqrt{2})^{2k+1}\right]$$

Cerchiamo di imporre $a_k \equiv b_k \mod n$

$$\iff \frac{1}{2}\left[(1+\sqrt{2})^{2k+1} + (1-\sqrt{2})^{2k+1}\right] \equiv \frac{1}{2\sqrt{2}}\left[(1+\sqrt{2})^{2k+1} - (1-\sqrt{2})^{2k+1}\right] \mod n$$

Idea chiave: la congruenza è vera per $k=0$ e i due membri sono periodici.

Come si dimostra la periodicità?

$x^0, x^1, x^2, \dots, x^t \mod n$

Ce ne sono 2 congrue, diciamo $x^r \equiv x^s \mod n$

con $r<s$. SICCOME x è INVERTIBILE

MOD n, LA PRIMA CHE SI RIPETE È 1

La cosa funziona anche qui, perché $1+\sqrt{2}$ è invertibile mod n, visto che l'inverso è $\sqrt{2}-1$