# TdN Advanced 3 (Pell ...)

Titolo nota 07/09/2018

## Equazione di Pell

$$x^2 - dy^2 = 1 \qquad d \in \mathbb{Z} \qquad d \neq \square$$

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

**Def.** $N(x + y\sqrt{d}) = x^2 - dy^2$

$$N\big((x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d})\big) = N(x_1 + y_1\sqrt{d})\, N(x_2 + y_2\sqrt{d})$$

**Oss** Supponiamo di conoscere una soluz di

$$x_1^2 - dy_1^2 = m \quad \text{e una di} \quad x_2^2 - dy_2^2 = n$$

Allora conosciamo una sol di $x_3^2 - dy_3^2 = mn$

$$N(x_1 + \sqrt{d}\, y_1) = m, \quad N(x_2 + \sqrt{d}\, y_2) = n$$

Posso prendere $x_3 = x_1 x_2 + d y_1 y_2$

$$y_3 = x_1 y_2 + x_2 y_1$$

**TEOREMA** Esistono $\infty$ soluzioni intere di

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

Dim Per Dirichlet esistono infinite coppie $(p, q)$ di interi positivi t.c.

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

Uno vorrebbe prendere $x = p$ e $y = q$

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

$$= \left|y\underbrace{\left(\frac{x}{y} - \sqrt{d}\right)}_{< 1/y^2}\left(x + y\sqrt{d}\right)\right| \leq \frac{x + y\sqrt{d}}{y}$$

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

Per pigeonhole, c'è un qualche intero $k$, con $|k| \leq 2\sqrt{d} + 1$, che si scrive come

$$p^2 - dq^2 = k$$

per infinite coppie $(p, q)$

Prendiamone 2, $(p_1, q_1)$ e $(p_2, q_2)$

$$N\left(\frac{p_1 + q_1\sqrt{d}}{p_2 + q_2\sqrt{d}}\right) = \frac{N(p_1 + q_1\sqrt{d})}{N(p_2 + q_2\sqrt{d})} = \frac{k}{k} = 1$$

$$\| \quad A + B\sqrt{d} \text{ con } A, B \text{ razionali}$$

$$\frac{(p_1+q_1\sqrt{d})(p_2-q_2\sqrt{d})}{(p_2+q_2\sqrt{d})(p_2-q_2\sqrt{d})} = \frac{(p_1p_2-dq_1q_2)+(p_2q_1-q_2p_1)\sqrt{d}}{k}$$

Affinché i coeff. siano interi occorre e basta che

$$\begin{cases} p_1p_2 - d\,q_1q_2 \equiv 0 \ (k) \\ p_2q_1 - q_2p_1 \equiv 0 \ (k) \end{cases} \qquad q_1/q_2 \equiv p_1/p_2 \ (k)$$

Se per caso $p_1 \equiv p_2 \ (k)$ e $q_1 \equiv q_2 \ (k)$

avremmo vinto ( $2^a$ congr. ok; prima congr.:

$$p_1^2 - d\,q_1^2 = k \equiv 0 \ (k) \ )$$

E queste esistono perché originariamente avevamo infinite coppie.

Sia $(x_0, y_0)$ una soluzione, $u = x_0 + \sqrt{d}\,y_0$.

Allora $N(u) = 1 \Rightarrow N(u^k) = 1 \quad \forall k \geq 0$

Non solo: anche $N(u^{-k}) = 1$

$$u^{-1} = \frac{1}{x_0+\sqrt{d}\,y_0} \cdot \frac{x_0-\sqrt{d}\,y_0}{x_0-\sqrt{d}\,y_0} = \frac{x_0-\sqrt{d}\,y_0}{x_0^2 - dy_0^2}$$

$$= x_0 - \sqrt{d}\,y_0 \qquad \square$$

# Struttura di tutte le soluzioni

Esiste $u = x_0 + \sqrt{d}\, y_0$ con $N(u) = 1$

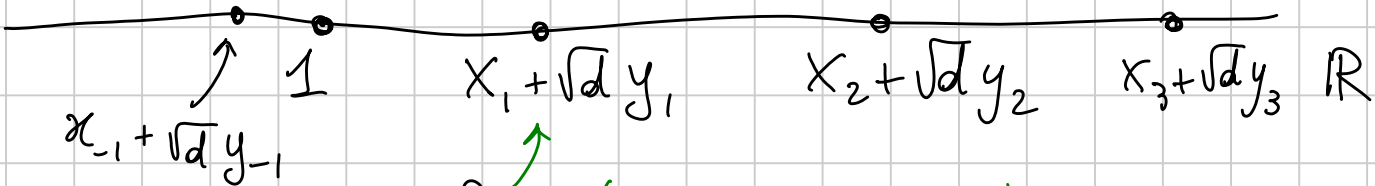
tale che TUTTE le soluzioni "siano" del

tipo $\pm u^k$ con $k \in \mathbb{Z}$

Più precisamente: $x = \dfrac{(x_0+\sqrt{d}\,y_0)^k + (x_0-\sqrt{d}\,y_0)^k}{2}$

$$= \frac{u^k + u^{-k}}{2}$$

e $y = \dfrac{u^k - u^{-k}}{2\sqrt{d}}$




$f$ (fondamentale)

Sia $f$ il minimo numero reale $>1$ che si scrive come $x+\sqrt{d}\,y$, $x^2 - dy^2 = 1$

Sia poi $s = a + b\sqrt{d}$ una soluzione.

Anche $s \cdot f^k$, $k \in \mathbb{Z}$, sono soluzioni.

Scelgo $k$ in modo che

$$1 \leq \underbrace{s \cdot f^k}_{\text{soluzione!}} < f$$

Per minimalità di $f$, $e^{\cdot} = 1$

$$\Rightarrow s = f^{-k}$$

□

## FRAZIONI DI FAREY

$$x^2 - 5y^2 = 1$$

$$\frac{2}{1} < \sqrt{5} < \frac{3}{1} \rightsquigarrow \frac{2+3}{1+1} = 5/2$$

$$\frac{2}{1} < \sqrt{5} < \frac{5}{2} \rightsquigarrow \frac{2+5}{1+2} = 7/3$$

$$\frac{2}{1} < \sqrt{5} < \frac{7}{3} \rightsquigarrow \frac{2+7}{1+3} = 9/4 \quad \text{ECCOLA!}$$

Soluzione fondamentale: $9 + 4\sqrt{5}$

## Pell generalizzate

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

Supponiamo che almeno una soluzione $(x_0, y_0)$ esista. Allora $(x_0 + y_0\sqrt{d}) \cdot f^k$ sono ancora soluzioni

① Bound su una soluzione

Sia $s = x_0 + y_0\sqrt{d}$ una soluzione. Allora posso scegliere $k$ t.c. $S = s f^k \in \left[\frac{\sqrt{a}}{\sqrt{f}}, \sqrt{a}\cdot\sqrt{f}\right]$

$$x = \frac{S + \text{coniugato}(S)}{2} = \frac{S + a/S}{2}$$

$$\leq \frac{1}{2} \max\left\{\sqrt{\frac{a}{f}} + \sqrt{a}\cdot\sqrt{f},\ \sqrt{a}\cdot\sqrt{f} + \frac{\sqrt{a}}{\sqrt{f}}\right\}$$

$$= \frac{1}{2}\sqrt{a}\left(\sqrt{f} + \frac{1}{\sqrt{f}}\right) \qquad (a > 0 \dots)$$

② Famiglie di soluzioni

Vorremmo prendere due solez. $N(s_1) = N(s_2) = a$ e dividere una per l'altra

$$\frac{x_1+\sqrt{d}\,y_1}{x_2+\sqrt{d}\,y_2}\cdot\frac{x_2-\sqrt{d}\,y_2}{x_2-\sqrt{d}\,y_2}=\frac{(x_1x_2-dy_1y_2)+\sqrt{d}(x_2y_1-x_1y_2)}{a}$$

Facciamo il caso $(x_1, a)=(x_2, a)=1$

$$(y_1, a)=(y_2, a)=1$$

$$\begin{cases} x_1x_2-dy_1y_2 \equiv 0 \mod a \\ y_1/x_1 \equiv y_2/x_2 \mod a \end{cases}$$

$$0\equiv x_1-dy_1(y_2/x_2)\equiv x_1-dy_1(y_1/x_1)$$

$$\equiv \frac{1}{x_1}(x_1^2-dy_1^2)\equiv 0 \ (a)$$

Due soluz. stanno nella stessa famiglia se e solo se hanno lo stesso $(Y/X \mod a)$

$\Rightarrow$ # famiglie $\leq \varphi(|a|)$

ESERCIZI

- $X^4-2y^2=17$ con le Pell
- $p\equiv 1\ (4) \Rightarrow x^2-py^2=-1$ ha $\infty$ soluz

  $p=a^2+b^2$ con $a$ dispari $\Rightarrow x^2-py^2=a$ si risolve
- $X^2-5183y^2=2$ : si risolve?

# SOLUZIONI

$x^2 - 5183y^2 = 2$ $\qquad$ $5183 = 71 \cdot 73$

$= (72+1)(72-1)$

$\frac{71}{1} < \sqrt{5183} < \frac{72}{1}$ $\qquad$ Fondamentale: $72 + \sqrt{5183}$

$\approx 144$

$$|x| \leq \frac{1}{2}\sqrt{a}\left(\sqrt{f} + \frac{1}{\sqrt{f}}\right) = \frac{1}{2}\sqrt{2}\left(12+1\right) < 13$$

quindi no soluz perché $x^2 - 5183y^2 \leq$

$$\leq x^2 - 5183 < 0$$

Più in generale: $x^2 - (n^2-1)y^2 = m$

allora o $m = \square$ oppure $|m|$ è "grandicello" rispetto a $n$.

- $x^2 - py^2 = -1$ $\qquad$ $N(s) = -1$

  $p \equiv 1 \ (4)$ $\qquad$ $N(s^2) = 1$

  $f = a + b\sqrt{p}$ la fondamentale

Se $\sqrt{f} = x + y\sqrt{p} \implies N(\sqrt{f}) = -1$

$1 \leq \sqrt{f} \leq f$

$$\begin{cases} x^2 + py^2 = a \\ 2xy = b \end{cases}$$

$$a^2 - pb^2 = 1$$

$$\Downarrow$$

$$(a+1)(a-1) = pb^2$$

$a^2 - b^2 \equiv 1 \mod 4 \Rightarrow$ $a$ disp, $b$ pari

$b = 2c$

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

$p\square \quad \square$

$\square \quad p\square$

$$\frac{a \pm 1}{2} = \underset{x^2}{\square}, \quad \frac{a \mp 1}{2} = p\underset{y^2}{\square} \Rightarrow a = \square + p\square = x^2 + py^2$$

e $\quad 2xy = 2\sqrt{\left(\frac{a\pm1}{2}\right)\left(\frac{a\mp1}{2p}\right)} = \sqrt{\frac{a^2-1}{p}} = b$

$x^2 - py^2 = a \qquad p = a^2 + b^2$

$$\begin{cases} b^2 - p \cdot 1 = -a^2 \\ x^2 - py^2 = -1 \text{ ha soluz} \end{cases} \Rightarrow x^2 - py^2 = +a^2$$

- $x^4 - 2y^2 = 17 \quad \rightsquigarrow \quad z^2 - 2y^2 = 17$

Famiglie di soluzioni: determinate da $z/y \mod 17$

$$(z/y)^2 \equiv 2 \mod 17 \Rightarrow z/y \equiv \pm 6 \mod 17$$

$z^2 - 2y^2 = 1$ $\qquad$ $f = 3 + 2\sqrt{2}$

Soluzione di $z^2 - 2y^2 = 17$ : $z = 5,\ y = 2$

$z = -5,\ y = 2$

Tutte le soluz sono del tipo

$$z = \pm \frac{1}{2}\left[ (\pm 5 + 2\sqrt{2}) \cdot (3+2\sqrt{2})^k + (\pm 5 - 2\sqrt{2})(3-2\sqrt{2})^k \right]$$

$z = \square \Rightarrow z > 0 \Rightarrow$ o $+, +$ o $-, -$

$$z = \frac{1}{2}\left[ (5 \pm 2\sqrt{2})(3+2\sqrt{2})^k + \text{coniugato} \right]$$

$$\begin{cases} z_{k+1} = 6z_k - z_{k-1} \\ z_0 = 5 \ / \ 5 \\ z_1 = 23 \ / \ 7 \end{cases}$$

Modulo 8! $z_k \bmod 8$ è $5, 7, 5, 7, \ldots$

$2 + 2\sqrt{28n^2+1}$ intero $\Rightarrow$ quadrato

$$y^2 = 28n^2 + 1 \qquad y^2 - 7 \cdot 2^2 n^2 = 1$$

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

$$y = 8, \; x = 3 \qquad 8 + 3\sqrt{7} = f$$

Conto $\Rightarrow$ in $\dfrac{f^k + f^{-k}}{2}$ il coeff di $\sqrt{7}$ è

pari se e solo se $k$ è pari

$$2 + 2\sqrt{28n^2+1} = 2 + 2y = 2 + f^{2m} + f^{-2m}$$

$$= \left(f^m + f^{-m}\right)^2$$

$$f_{28} : \quad 127 + 24\sqrt{28} = \left(8 + 3\sqrt{7}\right)^2$$

$x^2+1 = 5^n$ $\quad$ $n$ pari $\quad$ OK

$n = 2k+1$

$x^2+1 = 5\cdot y^2$ $\qquad$ $y = 5^k$

$x^2 - 5y^2 = -1$ $\qquad$ Soluzione: $2+\sqrt{5}$

Fondam: $9+4\sqrt{5} = (2+\sqrt{5})^2$

Tutte le solez: $(2+\sqrt{5})^{2r+1}$

$$y = \frac{1}{2\sqrt{5}}\left( (2+\sqrt{5})^{2r+1} - (2-\sqrt{5})^{2r+1} \right)$$

$v_5(y) = v_5(2r+1)$ per una opportuna versione di LTE

$$\frac{(2+\sqrt{5})^{2r+1}}{2\sqrt{5}} \lesssim y = 5^{v_5(y)} = 5^{v_5(2r+1)}$$

LTE "generale"

$$\frac{(2+\sqrt{5})^k - (2-\sqrt{5})^k}{2\sqrt{5}} \quad \text{con } (k,5)=1:$$

$$= \frac{1}{2\sqrt{5}}\left( 2^k + k\cdot 2^{k-1}\sqrt{5} + \binom{k}{2}2^{k-2}\cdot 5 + \binom{k}{3}2^{k-3}\cdot 5\cdot\sqrt{5} + \dots \right.$$
$$\left. -2^k + k\cdot 2^{k-1}\sqrt{5} - \binom{k}{2}2^{k-2}\cdot 5 + \binom{k}{3}2^{k-3}\,5\sqrt{5} \right)$$

Stesso conto quando $K=5$.

## Risolubilità di $x^2 - 2y^2 = p$

Necessario: $\left(\frac{2}{p}\right) = +1 \iff p \equiv \pm 1 \ (8)$

$(x - \sqrt{2}\,y)(x + \sqrt{2}\,y) = p \rightsquigarrow \mathbb{Z}[\sqrt{2}]$

FATTORIZZAZIONE UNICA

Siccome $\left(\frac{2}{p}\right) = +1$, esiste $n$ t.c. $p \mid n^2 - 2$

$\Rightarrow p \mid (n - \sqrt{2})(n + \sqrt{2})$

$n + \sqrt{2} = p \cdot (a + b\sqrt{2})$ NO!

$\Rightarrow p$ non è primo $\Rightarrow p$ non è irriducibile

$p = (a + b\sqrt{2})(c + d\sqrt{2})$

$N(p + 0\sqrt{2}) = N(a + b\sqrt{2})\,N(c + d\sqrt{2})$

$p^2 = (a^2 - 2b^2)(c^2 - 2d^2)$

$\neq \pm 1 \qquad \neq \pm 1$

Quindi sono $\pm p$!

$$p = ac + 2bd + \sqrt{2}(bc + ad)$$

$$bc = -ad \qquad a^2 - 2b^2 = c^2 - 2d^2 = \pm p$$

$(a,b) = (c,d) = 1$ e quindi $a = \pm c$, $b = \mp d$

Stesso ragionamento con $x^2 + 2y^2 = p$: si risolve se e solo se $\left(\frac{-2}{p}\right) = +1$

Come si dimostra la fattorizz. unica?

Lemma chiave Se "funziona" la divisione con resto c'è fattorizzazione unica

"Funziona": c'è una funzione "grandezza" (a valori interi)
t.c. $\forall\, x, y \neq 0$ esistono $q, r \in$ (dove serve)

t.c. $x = q \cdot y + r$ E grandezza(resto) < grandezza($y$)

Nei casi facili, GRANDEZZA = NORMA

Esempio $\mathbb{Z}[i]$

Voglio dividere con resto $a+bi$ per $c+di$.

Calcolo $\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{c^2+d^2} = (A + r_1) + (B + r_2)i$

dove $A, B$ sono interi e $r_1, r_2$ sono razionali di $|\cdot| \leq 1/2$

$$a+bi = (A+Bi)(c+di) + \underbrace{(r_1+r_2 i)(c+di)}_{\text{resto} \in \mathbb{Z}[i] \text{ per differenza}}$$

$$N(\text{resto}) = N(c+di)\, N(r_1+r_2 i)$$

$$\leq N(c+di) \cdot \frac{1}{2} < N(c+di)$$

Applicazione $\qquad A \quad B = x^2$

$$y^2+2 = x^3 \quad \rightsquigarrow \quad (y+\sqrt{-2})(y-\sqrt{-2}) = x^3$$

$y$ dispari $\Rightarrow (y+\sqrt{-2}, y-\sqrt{-2}) =$

$$= (y+\sqrt{-2}, 2\sqrt{-2}) = 1$$

$$\Rightarrow y+\sqrt{-2} = A^3 = (a+b\sqrt{-2})^3$$

$$= a^3 + 3a^2 b\sqrt{-2} + 3ab^2(-2) + b^3(-2)\sqrt{-2}$$

Coeff. di $\sqrt{-2}$ : $\quad 1 = 3a^2 b - 2b^3 = b(3a^2 - 2b^2)$

$\Rightarrow b = \pm 1, \; a = \pm 1$ (e in realtà $b = +1$)

$$y + \sqrt{-2} = \left(\pm 1 + \sqrt{-2}\right)^3$$

$$\Rightarrow \quad y = a^3 - 6a = \pm 5$$