Equazione di Pell in Interi e Polinomi

Candidato
Dario Balboni

Relatore
Prof. **Roberto Dvornicich**

Argomenti della Tesi

Equazione di Pell polinomiale ed intera

Importanza dell'equazione di Pell

Teoremi sulla struttura delle soluzioni

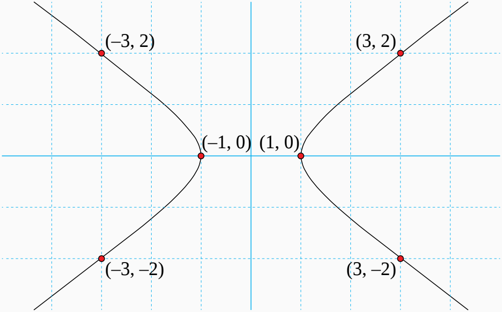
Frazioni continue

Metodo risolutivo con Frazioni Continue

Sistema di riduzioni di Lagrange

Legame con le curve iperellittiche

L’equazione di Pell



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

Cos'è l'equazione di Pell?

Equazione di Pell

$$x^2 - Dy^2 = 1$$

- Classicamente soluzioni con $x, y, D \in \mathbb{Z}$ (per $D > 0$)
- Più recentemente anche $x, y, D \in K[t]$ (K campo)

Equazione di Pell Generalizzata

$$x^2 - Dy^2 = N$$

Curiosità: il ruolo di Pell

Pell non diede alcun contributo alla soluzione dell'equazione. Essa porta il suo nome a causa di un errore di Eulero, che attribuì a Pell il metodo risolutivo di Brouckner (precursore del metodo delle frazioni continue).

Importanza dell’equazione di Pell

Perché è importante?

Rappresenta le unità

$\alpha = x + \sqrt{D}y \in \mathbb{Z}[\sqrt{D}]$ rappresenta un'unità di $\mathbb{Z}[\sqrt{D}]$ se e solo se $\mathcal{N}(\alpha) = (x + \sqrt{D}y)(x - \sqrt{D}y) = x^2 - Dy^2$ è invertibile in $\mathbb{Z}$, ovvero $\mathcal{N}(\alpha) = \pm 1$.

Collegamenti con il class number dei campi quadratici

Attraverso la Class Number Formula: data la soluzione fondamentale per $D > 0$, si può ricavare il class number per $\mathbb{Q}(\sqrt{D})$. [32]

Primitive di funzioni algebriche

Abel notò che è collegata con le primitive di funzioni algebriche: se si ha una soluzione $p(t)^2 - D(t)q(t)^2 = 1$ allora vale

$$\int \frac{p'(x)\mathrm{d}x}{q(x)\sqrt{d(x)}} = \log\left(p(x) + q(x)\sqrt{d(x)}\right).$$

Struttura delle Soluzioni

Struttura delle soluzioni

$$x^2 - Dy^2 = 1$$

Formula di Moltiplicazione delle Soluzioni

Date due soluzioni x_1, y_1 e x_2, y_2 si può definire una terza soluzione attraverso l'operazione

$$(x_1, y_1) \star (x_2, y_2) = (x_1 x_2 + D y_1 y_2,\ x_1 y_2 + x_2 y_1)$$

Ciò equivale a moltiplicare le espressioni del tipo $x_i + \sqrt{D} y_i$.

Le soluzioni formano un gruppo Abeliano

L'elemento neutro è dato dalla soluzione banale $(1, 0)$.

L'inverso di (x, y) è dato da $(x, -y)$.

Esistenza di una soluzione minima

$$x^2 - Dy^2 = 1$$

Soluzioni minime e struttura del gruppo

Se l'equazione di Pell per D è risolubile, il gruppo delle soluzioni è abeliano di rango uno: esiste una soluzione (X, Y), detta minimale, tale che se (P, Q) è un'altra soluzione, allora $P = \pm U, Q = \pm V$ con

$$U + \sqrt{D}V = \left(X + \sqrt{D}Y\right)^n$$

dove $n \in \mathbb{N}$.

La soluzione minima di $D = t^2 + 1$ in $\mathbb{C}[t]$ è $X = it$, $Y = i$, mentre la soluzione minima in $\mathbb{Q}[t]$ è $X = -2t^2 - 1$, $Y = -2t$: la soluzione minima può cambiare a seconda del sottoanello considerato.

Differenze tra l'equazione intera e l'equazione polinomiale

Differente risolubilità

$$x^2 - Dy^2 = 1$$

Se $D = E^2$ l'equazione di Pell ammette solo la soluzione banale.

Affinché l'equazione polinomiale sia risolubile in $K[t]$ si deve avere $\deg D$ pari e lc $D = a^2$ con $a \in K$.

L'equazione intera è sempre risolubile per i D non quadrati perfetti. [17]

- Per $D = 5$ si ha $9^2 - 5 \cdot 4^2 = 1$.
- Per $D = 11$ si ha $10^2 - 11 \cdot 9^2 = 1$.

L'equazione polinomiale invece non ammette sempre una soluzione:

- $D = (t^2 + 1)(t - a)^2$ al variare di $a \in \mathbb{R}^+$ non ha soluzioni non banali.
- $D = t^6 + t + 1$ non ha soluzioni in $\mathbb{C}[t]$.

Le frazioni continue

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{\ddots}}}}}}$$

Frazioni Continue

Cos'è una frazione continua

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

con $a_0, a_1, \ldots \in \mathbb{N}$ se vogliamo approssimare $\alpha \in \mathbb{R}$.
In maniera compatta viene denotata con $\alpha = [a_0; a_1, a_2, \ldots]$.

Troncando all'n-esimo passo otteniamo una frazione che possiamo scrivere come

$$\frac{x_n}{y_n} = [a_0; a_1, \ldots, a_n]$$

dove $\frac{x_n}{y_n}$ è ridotta ai minimi termini.

Tali frazioni vengono chiamate convergenti.

Teorema di Approssimazione

Convergenti come buone approssimazioni

$\frac{p}{q}$ è una convergente ad F se e solo se si ha $\forall \frac{a}{b} \neq \frac{p}{q}$ con $b \leq q$:

$$|bF - a| \leq |qF - p|$$

Ovvero $\frac{p}{q}$ è un'approssimazione di F migliore di ogni altra frazione con denominatore minore o uguale.

Teorema di approssimazione

Per $F \in \mathbb{R}^+$, $x, y \in \mathbb{N}$ si ha

$$|yF - x| < \frac{1}{|y|}$$

se e solo se $\frac{x}{y}$ è una convergente ad F.

Collegamento con l’equazione di Pell

Legame tra frazioni continue ed equazione di Pell

Le soluzioni della Pell sono convergenti

Se (x, y) è una soluzione per la Pell con parametro D, allora $\pm\frac{x}{y}$ è una convergente di $\sqrt{D}$.

Infatti da $x^2 - Dy^2 = 1$ si ottiene

$$\left(\frac{x}{y}\right)^2 - D = \left(\frac{x}{y} - \sqrt{D}\right)\left(\frac{x}{y} + \sqrt{D}\right) = \frac{1}{y^2}.$$

Supponendo $x, y > 0$ si ha anche $\frac{x}{y} + \sqrt{D} > \sqrt{D}$ da cui

$$\left|\frac{x}{y} - \sqrt{D}\right| < \frac{1}{y^2\sqrt{D}} \leq \frac{1}{y^2}$$

dal teorema precedente si deduce quindi che $\frac{x}{y}$ è una convergente di $\sqrt{D}$.

Problema: Definire $\sqrt{D}$ anche per i polinomi.

Serie di Laurent

Serie di Laurent

Una serie di Laurent a coefficienti in K è un'espressione formale del tipo

$$F = \sum_{h=-m}^{\infty} f_h t^{-h}.$$

Ha finiti termini con esponente positivo ed arbitrari con esponente negativo.

Con la moltiplicazione alla Cauchy formano un anello denotato $K((t^{-1}))$.

Il grado di F è il più piccolo intero h tale che $f_h \neq 0$.

Definiamo anche $\lfloor F \rfloor$ come la sua "parte polinomiale".

Se F è definita come sopra si ha $\lfloor F \rfloor = \sum_{h=-m}^{0} f_h t^{-h} \in K[t]$.

- Con $F = 2t^{-2} + t + 5t^7$ si ha $\deg F = 7$ e $\lfloor F \rfloor = t + 5t^7$
- Con $F = 6 - t^2$ si ha $\deg F = 2$ e $\lfloor F \rfloor = 6 - t^2$

Radice quadrata di Polinomi

Radice quadrata di Polinomi

$F \in K((t^{-1}))$ è una radice quadrata di $D = \sum_{h=-s}^{0} d_h t^{-h} \in K[t]$ se si ha $F \cdot F = D$. Essa esiste se e solo se D è di grado pari ed il suo coefficiente direttivo è un quadrato in K. Queste restrizioni sono le stesse necessarie affinché l'equazione di Pell di parametro D ammetta soluzione non banale.

$$\begin{aligned} f_{-h}^2 &= d_{-h} \\ 2f_{-h}f_{-(h-1)} &= d_{-(h-1)} \\ 2f_{-h}f_{-(h-2)} + f_{-(h-1)}^2 &= d_{-(h-2)} \\ &\vdots \end{aligned}$$

- Se $D = 4t^6$ allora si ha $F = 2t^3$
- Se $D = t^6 + t$ si ha $F = t^3 + \frac{1}{2}t^{-2} - \frac{1}{2}t^{-7} + \dots$

Frazioni continue per i Polinomi

Frazione continua per i polinomi

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

con $a_0, a_1, \ldots \in K[t]$ se vogliamo approssimare $\alpha \in K((t^{-1}))$.

Teorema di approssimazione

Per $F \in K((t^{-1}))$, $x, y \in K[t]$ si ha

$$\deg(yF - x) < -\deg y$$

se e solo se $\frac{x}{y}$ è una convergente ad F.

Calcolo della frazione continua della radice quadrata

Formula per i resti delle frazioni continue

$$F_0 = F, \quad a_i = \lfloor F_i \rfloor, \quad F_{i+1} = \frac{1}{F_i - a_i}$$

dove $\lfloor F_i \rfloor$ è l'intero più vicino oppure la parte polinomiale.

Forma dei resti di $\sqrt{D}$

Nell'algoritmo per il calcolo della frazione continua, tutti i resti di $\sqrt{D}$ sono esprimibili nella forma $F_i = \dfrac{P_i + \sqrt{D}}{Q_i}$ con $P_i, Q_i \in K[t]$.

Inoltre P_{i+1}, Q_{i+1} soddisfano delle formule per ricorrenza.

Esempio: $D = t^6 + t$

$$F_1 = \frac{t^3 + \sqrt{t^6 + t}}{t}, \quad F_2 = \frac{t^3 + \sqrt{t^6 + t}}{1}$$

Risoluzione dell'equazione di Pell

Misura delle approssimazioni date dalle convergenti

Siano x_h, y_h il numeratore e denominatore della convergente h-esima a $\sqrt{D}$ ridotta ai minimi termini. Allora si ha che

$$x_h^2 - Dy_h^2 = (-1)^{h+1} Q_{h+1}$$

Esempio: $D = t^6 + t$

$$x_0 = t^3, \quad y_0 = 1 \implies x_0^2 - Dy_0^2 = -t$$
$$x_1 = 2t^5 + 1, \quad y_1 = 2t^2 \implies x_1^2 - Dy_1^2 = 1$$

Quindi se sviluppando la frazione continua di $\sqrt{D}$ otteniamo r tale che $Q_r = \pm 1$ abbiamo risolto l'equazione di Pell.

Frazioni continue periodiche

Frazioni continue periodiche

Una frazione continua $\alpha = [a_0; a_1, \ldots]$ si dice periodica se la stringa dei coefficienti a_i è definitivamente periodica, ovvero se

$$\exists l, k \in \mathbb{N} \quad \forall n > k \quad a_{n+l} = a_n$$

Chiamiamo preperiodo i coefficienti precedenti la periodicità $(a_0, a_1, \ldots, a_k)$.

Periodicità di CF$(\sqrt{D})$

Se $\sqrt{D}$ ha frazione continua periodica, il suo preperiodo è di lunghezza uno.

In particolare si ha $\sqrt{D} = [a_0; \overline{a_1, a_2, \ldots, a_n, 2a_0}]$, dove la linea indica la parte periodica dello sviluppo.

Il Teorema di Abel

CF($\sqrt{D}$) è periodica se e solo se $\exists r\ Q_r = \pm 1$ oppure $Q_r \in K[t]^*$.

- La Pell ha soluzione $x, y \implies \frac{x}{y} = \frac{x_h}{y_h}$ è una convergente
- Approssimazione delle convergenti: $x_h^2 - Dy_h^2 = (-1)^{h+1} Q_{h+1}$
- Quindi La Pell ha soluzione $\Leftrightarrow \exists r\ Q_r = \pm 1$
- CF($\sqrt{D}$) è periodica $\Leftrightarrow$ La Pell ha soluzione

Teorema di Abel

L'equazione di Pell $X^2 - DY^2 = 1$ ha soluzioni non banali se e solo se la frazione continua di $\sqrt{D}$ è periodica.

$$\sqrt{t^6 + t} = [t^3; 2t^2, 2t^3, 2t^2, \ldots]$$

Risoluzione dell'equazione di Pell

Teorema di Lagrange sugli irrazionali quadratici

$\alpha \in \mathbb{R}$ ha frazione continua periodica se e solo se α è irrazionale quadratico.

Ciò vale anche per $\alpha \in \mathbb{F}_p[t]$. In questi casi l'equazione di Pell è sempre risolubile, per i D non quadrati perfetti.

Effettività del Teorema di Abel

Se D è Pelliano, sviluppando $\sqrt{D}$ in frazione continua si arriva alla periodicità. A quel punto si può calcolare la soluzione minima.

Se invece D non è Pelliano (ricordiamo che ciò può accadere solo per i polinomi), lo sviluppo di $\sqrt{D}$ con metodi ingenui continua all'infinito senza che vi sia periodicità. Al passo n-esimo però non possiamo sapere se $\sqrt{D}$ abbia periodo molto lungo oppure se sia aperiodico.

Argomenti Collegati

- Sistema di riduzioni di Lagrange
- Equazione di Pell negativa
- Legame con le curve iperellittiche

Sistema di riduzioni di Lagrange

$$x^2 - Dy^2 = N$$

Struttura delle soluzioni

Le soluzioni di $x^2 - Dy^2 = N$ (con N fissato) sono generate da un numero finito di soluzioni fondamentali, moltiplicate per soluzioni della Pell standard.

Lemma di riduzione di Lagrange

Se $x, y > 0$ è una soluzione di $x^2 - Dy^2 = N$ allora $\exists X, Y, K$ tali che

$$0 \leq K \leq \frac{|N|}{2}, \qquad h = \frac{K^2 - D}{N} \in \mathbb{Z}, \qquad X^2 - DY^2 = h$$

Inoltre si ha

$$x = \left|\frac{KX \pm DY}{h}\right|, \;\; y = \left|\frac{KY \pm X}{h}\right|$$

Risoluzione dell'equazione generalizzata

$$x^2 - Dy^2 = N$$

Problema: Determinare tutte le soluzioni fondamentali per un dato N

Utilizzo del sistema di riduzioni di Lagrange

Per trovare le soluzioni fondamentali di $x^2 - Dy^2 = N$:

- Se $N \geq \sqrt{D}$ utilizziamo le riduzioni di Lagrange e sappiamo che per conoscere le soluzioni bisogna risolvere altre equazioni di Pell generalizzate con N minore di quello attuale (ma con stesso D).
- Se $N < \sqrt{D}$ sappiamo già che le soluzioni intere dell'equazione sono da cercare tra le convergenti in frazione continua di $\sqrt{D}$.

Unità di norma negativa

Determinare per quali $D \in \mathbb{Z}$ la Pell

$$x^2 - Dy^2 = -1$$

ammetta soluzione è un problema attualmente aperto.

- È noto in alcuni casi speciali (Esempio: no soluzioni per $D \equiv 3 \pmod 4$).
- Esistono alcuni criteri a D fissato, che però richiedono di aver risolto la Pell standard. Quindi sono “lenti” e non funzionano per famiglie di D.
- Non si ha una descrizione soddisfacente dei D che la rendono risolubile.

Criterio di risolubilità (Mollin-Srinivasan 2010)

Sia (x_0, y_0) la soluzione minima della Pell standard. Allora l’equazione di Pell negativa ha soluzione se e solo se $x_0 \equiv 1 \pmod{2D}$.

Divisori e curve iperellittiche

$$\mathcal{C}: \ u^2 = D(t)$$

Pellianità e divisori di torsione

Dato $D(t)$ squarefree, sia $\tilde{\mathcal{C}}$ il completamento proiettivo della curva

$$u^2 = D(t),$$

che ha due punti all'infinito: siano essi ∞_- e ∞_+.

Allora esiste una soluzione all'equazione di Pell $x(t)^2 - D(t)y(t)^2 = 1$ se e solo se il divisore $\delta = \infty_- - \infty_+ \in \mathrm{Jac}\, \tilde{\mathcal{C}}$ è di torsione, ovvero

$$\exists m \in \mathbb{N} \text{ tale che } m(\infty_- - \infty_+) = 0 \in \mathrm{Jac}\, \tilde{\mathcal{C}}.$$

Si può infatti notare che, data una soluzione $x(t), y(t)$ e posta $\varphi = x(t) + uy(t) \in K[\mathcal{C}]$, si ha $\mathrm{div}(\varphi) = m\delta$.

Risolubilità dell'equazione polinomiale

$$\mathcal{C}: \; u^2 = D(t)$$

Algoritmo effettivo per la determinazione della Pellianità

Esiste un algoritmo per determinare se un punto nello Jacobiano Jac $\tilde{\mathcal{C}}$ è di torsione (con $\tilde{\mathcal{C}}$ definita su un campo finitamente generato sul campo primo):

- Per esemplificare sia $D \in \mathbb{Z}[t]$ e chiamiamo $\tilde{\mathcal{C}}_p$ la curva iperellittica che si ottiene per riduzione modulo p.
- La mappa tra le varietà Jacobiane Jac $\tilde{\mathcal{C}} \to$ Jac $\tilde{\mathcal{C}}_p$ preserva i gruppi di torsione coprima con p.
- Riducendo per due primi p, q opportunamente scelti si può capire se il punto originario è di torsione.

Specificazione delle soluzioni minime

- Sistema di riduzioni di Lagrange
- Equazione di Pell negativa
- Legame con le curve iperellittiche

Il problema delle specificazioni

$$x^2 - Dy^2 = 1$$

Supponiamo di avere $D(t) \in \mathbb{Z}[t]$ e di avere una soluzione minima $X(t), Y(t)$ in $\mathbb{Z}[t]$. Allora sappiamo che, preso $t_0 \in \mathbb{Z}$, $X(t_0), Y(t_0)$ è una soluzione in $\mathbb{Z}$ per la Pell intera di parametro $D(t_0)$.

Ci chiediamo quanto spesso essa possa essere una soluzione intera minimale.

Se $X(t_0), Y(t_0)$ non è la minimale allora si ha:

$$X(t_0) + \sqrt{D(t_0)}Y(t_0) = (x + \sqrt{D(t_0)}y)^n$$

con $n \in \mathbb{N}$ dipendente da t_0.

Se $X(t), Y(t)$ è una soluzione minima della polinomiale su $K[t]$, allora

$$\frac{X(t)}{Y(t)} = [A_0(t); A_1(t), \ldots, A_k(t)].$$

Limitatezza dell'esponente

$$x^2 - Dy^2 = 1$$

Idea: "Semplicità" di una frazione continua

Supponiamo di avere una "frazione continua razionale" $\alpha = [a_0; a_1, \ldots, a_k]$ dove $a_i \in \mathbb{Q}^+$. Ovviamente α può essere espressa in frazione continua naturale $\alpha = [b_0; b_1, \ldots, b_m]$ con $b_i \in \mathbb{N}$.

È lecito aspettarsi che m si possa limitare superiormente da k e dai denominatori che compaiono negli a_i. Ciò succede e vi è un algoritmo che consente di convertire una frazione continua razionale in una frazione continua naturale.

Al variare di t_0 vogliamo limitare la lunghezza della frazione continua naturale di $\frac{X(t_0)}{Y(t_0)}$. Per quanto appena detto si riesce a fare, ottenendo quindi che anche l'esponente della non-minimalità è limitato: infatti, come già visto, se una soluzione è multiplo k-esimo della fondamentale, la sua frazione continua ha almeno k termini naturali. [16]

Polinomi di Chebycheff e minimalità

$$x^2 - Dy^2 = 1$$

Polinomi di Chebycheff e minimalità

Data una soluzione $x, y \in \mathbb{Z}$ della Pell, la sua potenza n-esima si può esprimere come

$$(x + \sqrt{D}y)^n = T_n(x) + \sqrt{d}\ yU_n(x)$$

dove T_n e U_n sono polinomi di Chebycheff di primo e secondo tipo.

$$\begin{aligned}
(x + \sqrt{D}y)^3 &= (x^3 + 3x\underline{Dy^2}) + \sqrt{D}(\underline{Dy^3} + 3yx^2) \\
&= (x^3 + 3x(x^2 + 1)) + \sqrt{D}\ y((x^2 + 1) + 3x^2) \\
&= (4x^3 + 3x) + \sqrt{D}\ y(4x^2 + 1)
\end{aligned}$$

Condizione equivalente alla minimalità

$$x^2 - Dy^2 = 1$$

Condizione equivalente alla minimalità

La soluzione specificata $P(t_0), Q(t_0)$ è la potenza n-esima di una qualche soluzione intera se e solo se esistono $x, y \in \mathbb{Z}$ soluzioni delle seguenti equazioni:

$$P(t_0) - T_n(x) = 0, \quad Q(t_0) - U_n(x)y = 0, \quad x^2 - D(t_0)y^2 - 1 = 0$$

In particolare possiamo assumere n primo, a meno di spezzare n in fattori.

Abbiamo già mostrato che n è limitato. Ora mostriamo che per ogni n primo non possono esserci infinite soluzioni intere se la soluzione polinomiale dalla quale vengono ottenute è minimale.

Strumenti utilizzati

$$x^2 - Dy^2 = 1$$

Teorema di Bilu e Tichy

Siano $f(t), g(t) \in \mathbb{Q}[t]$ due polinomi non costanti e consideriamo l'equazione

$$f(x) = g(y).$$

Se essa ha infinite soluzioni razionali con denominatore limitato deve essere

$$f = \phi \circ f_1 \circ \lambda, \qquad g = \phi \circ g_1 \circ \mu$$

dove $\lambda(t), \mu(t) \in \mathbb{Q}[t]$ sono polinomi lineari, $\phi(t) \in \mathbb{Q}[t]$ polinomio qualunque e $(f_1(t), g_1(t))$ è una coppia standard su $\mathbb{Q}$.

Le *coppie standard* non sono altro che cinque famiglie di soluzioni parametriche all'equazione di cui sopra.

Minimalità delle soluzioni

$$x^2 - Dy^2 = 1$$

Utilizzando il teorema di Bilu e Tichy con $P(t) = T_n(x)$ e che $n = \deg T_n$ è primo (quindi T_n è indecomponibile), otteniamo (analizzando caso per caso le coppie standard) che se vi sono infinite soluzioni intere a $P(t) = T_n(x)$ si ha che esiste $A(t) \in \mathbb{Q}[t]$ tale che $P(t) = T_n(A(t))$.

Da questo $A(t)$ si riesce poi a costruire una soluzione polinomiale in $\mathbb{Q}[t]$ dell'equazione di Pell che elevata alla n-esima potenza dà $P(t), Q(t)$, violando così la minimalità.

Minimalità delle soluzioni

Se $D(t) \in \mathbb{Z}[t]$ è squarefree e la soluzione minima in $\mathbb{Q}[t]$ $P(t), Q(t)$ sta in $\mathbb{Z}[t]$, allora per tutti i $t_0 \in \mathbb{Z}$ tranne un numero finito, la soluzione $P(t_0), Q(t_0)$ è la soluzione minima in $\mathbb{Z}$ per $D(t_0)$.

Esempi e Controesempi

$$x^2 - Dy^2 = 1$$

Non tutte le specificazioni sono minime

Consideriamo $D(t) = t^4 + 6t^3 + 9t^2 + t + 3$: con il metodo delle frazioni continue si ottiene la soluzione minima $X(t) = 2t^3 + 6t^2 + 1$ e $Y(t) = 2t$.

Valutando in $t = -4$ si ottiene $D(-4) = 15$, $|X(-4)| = 31$, $|Y(-4)| = 8$, mentre la soluzione fondamentale per $D = 15$ è $X = 4$ e $Y = 1$.

Tutte le specificazioni sono minime

Se troviamo un polinomio $D(t)$ tale che abbia solo polinomi a coefficienti in $\mathbb{Z}[t]$ nell'espansione della radice quadrata, si hanno anche dei bound (molto stretti) per eliminare i punti con soluzione non-minima.

Purtroppo nel caso generale non si hanno dei bound effettivi sul massimo t_0 tale che $P(t_0), Q(t_0)$ sia non minimale.

Grazie per l'attenzione

Riferimenti Bibliografici:

A. Y. Khinchin, "Continued Fractions", *The University of Chicago Press, Chicago, Ill.-London* 1964, pp. xi+95

M. J. Jacobson e H. C. Williams, "Solving the Pell equation", *CMS Books in Mathematics, Springer, New York* 2009, pp. xx+495

A. J. van der Poorten e X. C. Tran, "Quasi-elliptic integrals and periodic continued fractions", In: *Monatshefte für Mathematik* 131.2 (2000), pp. 155-169

A. Dubickas e J. Steuding, "The polynomial Pell equation", In: *Elemente der Mathematik* 59.4 (2004), pp. 133-143

U. Zannier, "Unlikely Intersections and Pell's equations in polynomials", In: *Trends in contemporary mathematics* 8 (2014), pp. 151-169

O. Merkert, “Reduction and specialization of hyperelliptic continued fractions”, Ph.D. Thesis, Scuola Normale Superiore 2016

N. H. Abel, “Über die Integration der Differential-Formel $\frac{\varrho\,\mathrm{d}x}{\sqrt{R}}$, wenn R und ϱ ganze Functionen sind”, In: *Journal für die Reine und Angewandte Mathematik* 1 (1826), pp. 185-221

K. Matthews, “The diophantine equation $X^2 - DY^2 = N$, $D > 0$”, In: *Expositiones Mathematicæ* 18.4 (2000), pp. 323-332

R. A. Mollin e A. Srinivasan, “A Note on the negative pell equation”, In *International Journal of Algebra* 19.4 (2010), pp. 919-922

R. C. Mason, “Diophantine equations over function fields”, *London Mathematical Society Lecture Note Series, Cambridge University Press, Cambridge* 1984 vol. 96, pp. x+125

W. W. Stothers, “Polynomial identities and Hauptmoduln”, In: *The Quarterly Journal of Mathematics. Oxford. Second Series* 32.127 (1981), pp. 349-370

N. Snyder, “An alternate proof of Mason’s theorem”, In: *Elemente der Mathematik* 55.3 (2000), pp. 93-94

L. van den Dries e K. Schmidt, “Bounds in the theory of polynomial rings over fields. A nonstandard approach”, In: *Inventiones mathematicæ* 76.1 (1984), pp. 77-91

J. Yu, “On arithmetic of hyperelliptic curves”, In: *Manuscript marked Aspects of Mathematics, Hong Kong University* (1999), pp. 4-6

Y. Bilu e R. Tichy, “The Diophantine equation $f(x) = g(y)$”, In: *Acta Arithmetica* 95.3 (2000), pp. 261-288

A. Schinzel, “On some problems of the arithmetical theory of continued fractions. II”, In: *Acta Arithmetica* 7 (1961/1962), pp. 287-298

Class Number Formula

Class Number Formula

$$h(d) = \frac{\sqrt{d}}{\ln \varepsilon} L(1, \chi)$$

dove $h(d)$ è il class number di $\mathbb{Q}(\sqrt{d})$, ε viene detta unità fondamentale, e $L(s, \chi)$ è la L-serie di Dirichlet del campo.

Finitezza della L-serie

Dirichlet mostrò che la L-serie per questi campi si può scrivere in forma finita, ovvero supponendo che χ sia un carattere primitivo con conduttore primo q si ha

$$L(1, \chi) = \begin{cases} -\frac{\pi}{q^{\frac{3}{2}}} \sum_{m=1}^{q-1} m \left(\frac{m}{q} \right) & \text{se } q \equiv 3 \pmod{4} \\ -\frac{1}{q^{\frac{1}{2}}} \sum_{m=1}^{q-1} \left(\frac{m}{q} \right) \ln(2) \sin\left(\frac{m\pi}{q} \right) & \text{se } q \equiv 1 \pmod{4} \end{cases}$$

Calcolabilità del Class Number

Visto che $h(d)$ è un numero naturale ed $L(1,\chi)$ si può calcolare dalle formule precedenti con precisione arbitraria, se fosse noto $\ln \varepsilon$ con sufficiente precisione, si potrebbe determinare il class number di $\mathbb{Q}(\sqrt{d})$.

Legame con l'equazione di Pell

L'unità fondamentale ε si può caratterizzare come

$$\varepsilon = \frac{a + b\sqrt{d}}{2}$$

dove (a,b) è la soluzione più piccola a

$$x^2 - dy^2 = \pm 4$$

negli interi positivi.