Caratterizzazione della solvibilità dell'equazione di Pell nei polinomi

Dario Balboni

24 Aprile 2017

Indice

1 L'Equazione di Pell - Differenze tra il caso intero e polinomiale

Ci si chiede se, a D fissato, l'equazione

$$P^2 - DQ^2 = 1 \tag{1}$$

abbia soluzione, e se sì, se si riescano a determinare tutte.

Classicamente viene studiata con $P, D, Q \in \mathbb{Z}$, mentre solo recentemente ci si è interessati anche all'equazione polinomiale, ovvero con $P, D, Q \in K[t]$, con K un campo. Iniziamo con qualche osservazione sulle condizioni necessarie per la risolubilità; successivamente vedremo che cosa si riesce a dire sulla struttura delle soluzioni e quanto i fattori quadratici cambino l'esistenza di soluzioni. Inoltre vedremo qualche modo di calcolare esplicitamente le soluzioni attraverso lo strumento delle frazioni continue, ed infine qualche applicazione.

Il risultato principale a cui vogliamo arrivare è il celebrato teorema di Abel, che lega la risolubilità dell'equazione di Pell per $D \in K[t]$ con la periodicità dello sviluppo in frazione continua di $\sqrt{D}$.

1.1 Osservazioni sull'Equazione Polinomiale

Affinchè (1) sia risolvibile notiamo subito che è necessario che il grado di D sia pari, in quanto tra i polinomi Q^2 e DP^2 deve avvenire cancellazione, quindi $\deg D = 2\deg Q - 2\deg P$.

Inoltre, restringendo l'equazione ai coefficienti di testa dei polinomi si ottiene $\alpha^2 - \delta\beta^2 = 0$, ovvero il coefficiente direttivo di D deve essere un quadrato in K.

1.2 Risolvibilità Parziale

Nel caso intero, come è noto, l'equazione (1) ammette soluzioni intere non banali per tutti i discriminanti $D \in \mathbb{Z}$ che non siano quadrati perfetti. Nel caso polinomiale invece i polinomi $D \in K[t]$ che ammettono soluzioni non banali sono "rari".

- Per $D = t^2 - 1$ una soluzione non banale si può trovare con poco sforzo: $P = t$ e $Q = 1$;
- Per $D = t^6 + t$ una soluzione si può verificare essere $P = 2t^5 + 1$ e $Q = 2t^2$. In seguito vedremo come ci si può arrivare senza "indovinarla";
- Per $D = (t^2 + 1)(t - a)^2$ con $a \in \mathbb{R}^+$ non si hanno soluzioni non banali, pur non essendo D il quadrato di alcun polinomio. Vedremo in seguito una dimostrazione di questo fatto.

1.3 Fattori quadratici

Problemi più subdoli per quanto riguarda la risolubilità possono apparire anche attraverso la presenza di fattori quadratici in D. Questa è un'altra differenza con il caso intero, nel quale i fattori quadratici non influivano sull'esistenza di soluzioni. Vediamo qualche esempio di ciò, tratto da Zannier [2014].

- Per ogni dato $\lambda \in K$, per $D = (t - \lambda)^4(t^2 - 1)$ non si hanno soluzioni non banali;
- Data una coppia di polinomi dati $R(t), S(t)$, si può considerare $D = R(t)S(t)^{2k}$. Un'osservazione che fa capire l'importanza dell'ostruzione data dai fattori quadratici è che, per ogni coppia di polinomi fissati, esiste $k \in \mathbb{N}$ tale che l'equazione di Pell con $D = R(t)S(t)^{2k}$ non ammette soluzioni non banali.

Vediamo meglio come si può dimostrare l'ultima affermazione attraverso il Teorema di Mason-Stothers, conosciuto anche come congettura ABC polinomiale:

Teorema 1 (Mason-Stothers)**:** Se A, B, C sono polinomi coprimi su $K[t]$, tali che $A+B=C$, ed almeno una derivata A', B', C' non è completamente nulla allora

$$\max\{\deg A, \deg B, \deg C\} < n(ABC) \tag{2}$$

dove $n(P)$ denota il numero di zeri distinti di P in una chiusura algebrica.

Dimostrazione. *Omessa.* Per una dimostrazione si può vedere Snyder [2000], benché originariamente il risultato fosse dovuto indipendentemente a Mason [1984] e Stothers [1981]. □

Corollario 1. Sia char $K = 0$ e K algebricamente chiuso per semplicità. Denotiamo con $n(D)$ il numero di zeri distinti di $D \in K[t]$. Se $n(D) \leq \frac{1}{2} \deg D$, allora l'equazione (1) non ha soluzioni non banali in $K[t]$.

Dimostrazione. Si può applicare (2) con $A = P^2$, $B = -DQ^2$ e $C = 1$. Per concludere basta ricordare che $\deg D = 2 \deg P - 2 \deg Q$. □

1.4 Struttura delle soluzioni

Date due soluzioni P_1, Q_1 e P_2, Q_2 (entrambe per il polinomio D fissato), se ne può ottenere una terza "moltiplicandole", ovvero moltiplicando le due espressioni formali $P_1 + \sqrt{D}Q_1$ e $P_2 + \sqrt{D}Q_2$, ovvero

$$P_3 = P_1P_2 + DQ_1Q_2, \qquad Q_3 = Q_1P_2 + Q_2P_1$$

Le soluzioni dell'equazione di Pell formano quindi un gruppo commutativo, dove l'inverso di (P, Q) è dato da $(P, -Q)$ e l'elemento neutro è la soluzione banale $(1, 0)$.

Un risultato piuttosto significativo ed inaspettato è il seguente teorema sulla struttura delle soluzioni dell'equazione polinomiale: esse si comportano esattamente come nel caso intero, ovvero vi è una soluzione minima e tutte le altre si ottengono come potenze di quest'ultima. Inoltre, anche passando ai sottoanelli polinomiali di $K[t]$, la struttura delle soluzioni rimane invariata.

Teorema 2 (Struttura delle soluzioni)**:** Se (1) ha una soluzione non banale in $K[t]$, allora ha precisamente quattro soluzioni minimali. Se (p, q) è una di queste, allora tutte le altre soluzioni non banali sono della forma $(\pm P, \pm Q)$, dove

$$P + Q\sqrt{D} = (p + q\sqrt{D})^n$$

per qualche $n \in \mathbb{N}$.

Inoltre, se $D \in R[t]$, dove R è un sottoanello di K, è tale che (1) ha una soluzione non banale in $R[t]$, allora vi è un intero positivo m tale che ogni soluzione non banale dell'equazione in $R[t]$ è della forma $(\pm P, \pm Q)$, con

$$P + Q\sqrt{D} = (p + q\sqrt{D})^{mn}$$

per qualche $n \in \mathbb{N}$.

Dimostrazione. *Omessa.* A tal proposito si veda Dubickas and Steuding [2004]. □

1.5 Tentativo per le soluzioni

Potrebbe venire in mente che, se fosse disponibile un bound a priori sul grado di una possibile soluzione, si potrebbero pensare i coefficienti della soluzione come incognite e, a D fissato, trattare l'equazione come un sistema di equazioni algebriche in K, la cui risolubilità può essere controllata con metodi noti.

Accade però che, già per D quartico, il grado della soluzione minima può essere arbitrariamente grande, quindi non si hanno bound in termini solo di $\deg D$.

2 Frazioni Continue

Introduciamo ora lo strumento delle frazioni continue anche per lo studio dell'equazione polinomiale.

2.1 Definizioni Principali

Una frazione continua è una scrittura del tipo

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}}$$

che viene solitamente denotata con $\alpha = [a_0; a_1, a_2, a_3, \ldots]$ per brevità.

L'idea è di approssimare il numero α troncando lo sviluppo della frazione continua ad un certo a_n e considerando la successione di razionali r_n che si viene così a formare.

Esempio 1 ($\star$ Frazione continua di e)**:** Un risultato classico abbastanza noto è lo sviluppo in frazione continua di e:

$$e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, \ldots]$$

Se consideriamo la successione delle convergenti si ottiene:

$$r_0 = \frac{2}{1}, \qquad r_1 = \frac{3}{1}, \qquad r_2 = \frac{8}{3} \simeq 2.67, \qquad r_3 = \frac{11}{4} \simeq 2.75$$

e vediamo che si avvicinano sempre più ad $e \simeq 2.718$.

Di seguito indicheremo quindi con $\frac{x_n}{y_n}$ la frazione corrispondente ad $r_n = [a_0; a_1, \ldots, a_n]$ ridotta ai minimi termini.

In maniera analoga a quanto viene fatto classicamente con i numeri reali, possiamo porci nel campo delle serie di Laurent $K((X^{-1}))$, ovvero l'insieme delle scritture formali $\sum_{h=-m}^{\infty} f_h X^{-h}$ dotate della moltiplicazione alla Cauchy[1].

Per una fissata serie di Laurent F, possiamo allora definire per ricorsione gli a_i nel modo seguente:

$$F_0 = F, \qquad a_i = \lfloor F_i \rfloor, \qquad F_{i+1} = \frac{1}{F_i - a_i} \tag{3}$$

dove se $F(X) = \sum_{h=-m}^{\infty} f_h X^{-h}$ definiamo $\lfloor F_i \rfloor = \sum_{h=-m}^{0} f_h X^{-h}$, ovvero ne prendiamo solo la parte polinomiale.

[1] Corrispondenti tra l'altro all'anello delle serie formali di potenze localizzato per l'insieme $\{X, X^2, X^3, \ldots\}$

Definiamo inoltre il grado di una serie di Laurent come il più piccolo intero h tale che $f_h \neq 0$. In questo modo se consideriamo un polinomio come serie di Laurent le due definizioni di grado vengono a coincidere.

Esempio 2: Se $F(X) = X^{-2} + 4 + X^3$ allora $\lfloor F(X) \rfloor = 4 + X^3$.

Poiché $F(X) = X^3(1 + 4X^{-3} + X^{-5})$ si ha $\deg F(X) = 3$.

2.2 ⋆ Proprietà Aritmetiche

Si può facilmente osservare che numeratore e denominatore dell'approssimante $r_h = \frac{x_h}{y_h}$ si ottengono dall'identità matriciale

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} a_h & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} x_h & x_{h-1} \\ y_h & y_{h-1} \end{pmatrix} \tag{4}$$

dove conveniamo che il prodotto di matrice vuoto è la matrice identità.

Prendendo il determinante della (4) si ottiene

$$x_h y_{h-1} - y_h x_{h-1} = (-1)^{h+1} \tag{5}$$

Ricordando che $F = [a_0; a_1, \ldots, a_h, F_{h+1}]$ si ottiene, attraverso l'identità (4) che

$$F = \frac{x_h F_{h+1} + x_{h-1}}{y_h F_{h+1} + y_{h-1}} \tag{6}$$

2.3 Convergenti come migliori approssimazioni

Le convergenti, anche nel caso polinomiale, possono essere caratterizzate come buone approssimazioni della serie di Laurent in considerazione:

Teorema 3 (Delle migliori approssimazioni)**:** Siano x, y due polinomi coprimi. Allora

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

se e solo se la funzione razionale $\frac{x}{y}$ è una convergente di F.

Dimostrazione. $\boxed{\Leftarrow \star}$ Notiamo che dall'equazione (6) si ottiene

$$y_h F - x_h = \frac{y_h x_{h-1} - y_{h-1} x_h}{y_h F_{h+1} + y_{h-1}} = \frac{(-1)^h}{y_h} \frac{1}{(F_{h+1} + y_{h-1}/y_h)}$$

che mostra la notevole capacità di approssimazione delle convergenti. Passando ai gradi si conclude.
$\boxed{\Rightarrow}$ *Omessa.* Si veda van der Poorten [2000]. □

2.4 Radice quadrata di una serie di Laurent

Data una serie di Laurent $D \in K((X^{-1}))$, diciamo che $F \in K((X^{-1}))$ è una sua radice quadrata se $F \cdot F = D$. Notiamo che, affinché essa esista, è necessario e sufficiente che il coefficiente di testa di D sia un quadrato in K e che il grado di D sia pari.

2.5 Legame con l'equazione di Pell

Supponendo di avere una soluzione della (1) e dividendo per Q^2 si ottiene

$$\frac{1}{Q^2} = \left(\frac{P}{Q}\right)^2 - D$$

che fa intuire come $\frac{P}{Q}$ debba essere un'ottima approssimazione di $\sqrt{D}$.

In effetti si può dare il seguente più preciso enunciato, la cui dimostrazione si appoggia sul Teorema 3:

Teorema 4: Se $x^2 - Dy^2 = z$ e $\deg z < \deg \sqrt{D}$, allora $\pm\frac{x}{y}$ è una convergente in frazione continua di $\sqrt{D}$

Questo risultato ci dice che se abbiamo una buona approssimazione razionale a $\sqrt{D}$, essa deve essere una convergente in frazione continua. Proviamo allora a vedere se effetivamente le convergenti danno delle buone approssimazioni.

2.6 Calcolo delle convergenti della radice quadrata

Enunciamo in breve un generico passaggio del calcolo delle F_i, in parte per fissare la notazione, ed in parte per comprendere meglio lo strumento delle frazioni continue.

Vediamo che potremo sempre supporre che le F_i si scrivano come $F_i = \frac{P_i + \sqrt{D}}{Q_i}$ con $P_i, Q_i \in K[t]$ e $Q_i \mid D - P_i^2$. Se $a_i = \lfloor F_i \rfloor$, otteniamo che l'espressione di $F_{i+1} = \frac{1}{F_i - a_i}$ in termini delle P_i, Q_i è:

$$P_i + P_{i+1} = a_i Q_i, \qquad Q_i Q_{i+1} = D - P_{i+1}^2 \tag{7}$$

dalla quale si possono ricavare P_{i+1} e Q_{i+1}. Inoltre le convergenti soddisfano la ricorrenza

$$\begin{cases} x_{i+1} = a_{i+1} x_i + x_{i-1} \\ y_{i+1} = a_{i+1} y_i + y_{i-1} \end{cases} \tag{8}$$

con $x_{-1} = 1, y_{-1} = 0, x_0 = a_0, y_0 = 1$.

Esempio 3: Calcoliamo i primi termini della frazione continua della radice quadrata di $D = t^6 + t$. Con un veloce conto si scopre che $E = \left\lfloor \sqrt{D} \right\rfloor = t^3$.

i	P_i	Q_i	a_i	x_i	y_i
-1	/	/	/	1	0
0	0	1	t^3	t^3	1
1	t^3	t	$2t^2$	$2t^5+1$	$2t^2$
2	t^3	$\boxed{1}$	$2t^3$	/	/
3	t^3	t	$2t^2$	/	/

Come vedremo più avanti avere $Q_r = 1$ ci indica che la frazione continua è periodica (questo lo potevamo vedere anche osservando che $P_3 = P_1$ e $Q_3 = Q_1$ e, siccome tutto l'algoritmo dipende solo dai Q_i e P_i, si sarebbe dovuto ripetere) e quindi abbiamo ottenuto

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

In particolare, visto che il nostro claim è che le soluzioni della Pell debbano essere buone approssimazioni di $\sqrt{D}$, possiamo provare con le convergenti, calcolando $x_i^2 - Dy_i^2$, ottenendo:

$$x_0^2 - Dy_0^2 = -t, \qquad x_1^2 - Dy_1^2 = 1$$

e quindi abbiamo effettivamente risolto l'equazione di Pell con $D = t^6 + t$.

2.7 Frazione continue Periodiche

Data una frazione continue di $\alpha = [a_0; a_1, a_2, \ldots]$ diciamo che essa è periodica se $\exists k \in \mathbb{N}$ tale che $\forall r \geq r_0$ si ha $a_{r+k} = a_r$, ovvero se la stringa degli a_i è periodica.

Lemma 5: Una frazione continua è periodica se e solo se esiste r tale che $Q_r = 1$.

Dimostrazione. $\boxed{\Leftarrow}$ Se $Q_r = 1$, si può vedere eseguendo i calcoli come visto precedentemente che $P_{r+1} = P_1$ e $Q_{r+1} = Q_1$, il che ci dà quindi la periodicità.
$\boxed{\Rightarrow}$ *Omessa.* □

3 Il Teorema di Abel

Motivati dal legame tra frazioni continue ed equazione di Pell, ci si potrebbe chiedere effettivamente "quanto bene" le convergenti a $\sqrt{D}$ risolvano l'equazione di Pell. Significativamente si ottiene:

Lemma 6: Consideriamo lo sviluppo in frazione continua di $\sqrt{D}$: allora, per ogni h vale

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

Abbiamo già visto che se l'equazione di Pell ammette soluzioni non banali, allora esse sono convergenti alla frazione continua di $\sqrt{D}$. Dal lemma precedente, se una convergente risolve l'equazione di Pell, deve essere $Q_{h+1} = \pm 1$. Se si ottiene $Q_{h+1} = -1$, come già notato precedentemente, basta elevare la soluzione al quadrato per ottenerne una con $Q_{h+1} = 1$.

Per la caratterizzazione precedente della periodicità delle frazioni continue otteniamo quindi un noto teorema di Abel:

Teorema 7 (di Abel di caratterizzazione dei polinomi Pelliani)**:** L'equazione di Pell per il polinomio $D(t) \in K[t]$

$$P(t)^2 - D(t)Q(t)^2 = 1$$

è risolubile in $K[t]$ se e solo se lo sviluppo in frazione continua di $\sqrt{D(t)}$ è periodico.

Benché molto bello, il teorema di Abel non è effettivo: dato un polinomio $D(t)$ non sappiamo dire se esso sia Pelliano oppure no. Infatti si può provare a sviluppare la frazione continua di $\sqrt{D(t)}$. Se è periodica allora sappiamo che la soluzione esiste e la sappiamo anche trovare. In caso contrario si può correre il rischio di continuare a svilupparla, senza sapere se non si è ancora raggiunta la lunghezza del periodo oppure se l'equazione non è solvibile.

4 Applicazioni ed Approfondimenti

4.1 Utilità dello studio dell'equazione

Vediamo ora qualche applicazione dell'equazione di Pell nel caso polinomiale.

4.1.1 Integrazione di differenziali esatti

Abel [1826] notò, qualche secolo fa, che se $p(x)$ e $q(x)$ risolvono l'equazione di Pell con $d(x)$, allora vale che

$$\int \frac{p'(x)\mathrm{d}x}{q(x)\sqrt{d(x)}} = \log\left(p(x) + q(x)\sqrt{d(x)}\right) \tag{9}$$

espressione che generalizza il ben noto integrale

$$\int \frac{\mathrm{d}x}{\sqrt{x^2 + 2bx + c}} = \log\left(x + b + \sqrt{x^2 + 2bx + c}\right)$$

Ciò è piuttosto sorprendente, poiché in generale ci si aspetterebbe di ottenere funzioni ellittiche inverse o peggio, piuttosto che un logaritmo di una funzione algebrica.

4.1.2 Riduzione della generica equazione in due variabili

Attraverso semplici cambi di variabili per completamento dei quadrati, si può portare la generica equazione quadratica

$$ax^2 + bxy + cy^2 + dx + ey + f = 0, \qquad a, b, c, d, e, f \in K[t]$$

nella forma dell'equazione (generica, ovvero $P^2 - DQ^2 = G$) se char $K \neq 2$ e $D = b^2 - 4ac \neq 0, a \neq 0$. Ciò è particolarmente utile poiché, come abbiamo visto, sulle soluzioni dell'equazione di Pell molto è noto.

4.1.3 Unità degli anelli quadratici

Come per l'equazione intera, le soluzioni dell'equazione polinomiale rappresentano le unità negli anelli quadratici $K[t, \sqrt{D(t)}]$ e quindi è relazionata alle corrispondenti formule per il Class Number.

Infatti se prendiamo un qualunque elemento $\alpha \in K[t, \sqrt{D(t)}]$, non è difficile rendersi conto che α si scrive in modo unico come $\alpha = p + \sqrt{D}q$, dove $p, q \in K[t]$. Allora α è un'unità in $K[t, \sqrt{D(t)}]$[2] se e solo se la sua norma come estensione di campi (di $K(t, \sqrt{D(t)})$ come estensione quadratica di $K(t)$) è un elemento invertibile di $K[t]$ e quindi se e solo se è una costante.

Nel caso di K algebricamente chiuso si può facilmente vedere che si ha soluzione a

$$P^2 - DQ^2 = \mu, \qquad \mu \in K^*$$

se e solo se si ha soluzione alla Pell con $\mu = 1$. Infatti $\exists \lambda \in K$ tale che $\lambda^2 = \mu$ e quindi

$$\left(\frac{1}{\lambda}P\right)^2 - D\left(\frac{1}{\lambda}Q\right)^2 = 1$$

[2]Tra l'altro, $K[t, \sqrt{D(t)}]$ è la chiusura integrale di $K[t]$ in $K(t, \sqrt{D(t)})$

4.2 $\star$ Polinomi di basso grado

Caso quadratico

Se D ha grado due e K è algebricamente chiuso, l'equazione di Pell è risolubile se e solo se D ha due radici distinte: infatti dette α, β le due radici di $D = c(t-\alpha)(t-\beta)$, le soluzioni si possono scrivere esplicitamente come

$$P = \frac{2t - (\alpha+\beta)}{\alpha - \beta}, \qquad Q = \frac{2}{\sqrt{c}(\alpha-\beta)}$$

Dimostrazione della non solubilità per $D = (t^2+1)(t-a)^2$

Notiamo innanzitutto che $D = (t^2+1)(t-a)^2 \in \mathbb{C}[t]$, con $a \in \mathbb{R}^+$ non è un quadrato perfetto e non possiamo nemmeno applicare il Corollario 1 poiché $\deg D = 4$ e $n(D) = 3$.

Allora osserviamo che se P e Q sono tali che $P(t)^2 - D(t)Q(t)^2 = 1$, allora deve essere che $P(t)^2 - (t^2+1)[(t-a)Q(t)]^2 = 1$, ovvero detto $Q'(t) = (t-a)Q(t)$ la coppia $(P(t), Q'(t))$ deve essere soluzione della pell per $D'(t) = (t^2+1)$, ovvero in particolare $Q'(a) = 0$.

Per quanto osservato sopra, le soluzioni di questa sono tutte della forma

$$P + \sqrt{D'}Q' = \left(it + \sqrt{D'}i\right)^n$$

per qualche $n \in \mathbb{N}$.

Scrivendo esplicitamente si ottiene che

$$Q' = i^n \sum_{\substack{k=0 \\ k \text{ dispari}}}^{n} \sqrt{D'}^{k-1} t^{n-k} \binom{n}{k}$$

ma, poiché a è reale positivo $Q'(a) > 0$, violando così l'esistenza di soluzioni.

Caso quartico

Se $K = \mathbb{Q}$, già Schinzel [1961/1962] dimostrò che il periodo della frazione continua di $\sqrt{D}$ per $\deg D = 4$ è ≤ 22. Successivamente risultati di Malyschev, e la tesi di dottorato di Scherr [2013] risolsero la questione di determinare esattamente quali periodi possono presentarsi.

Il modo in cui viene dimostrato è di usare la corrispondenza tra solvibilità della Pell e punti di torsione nella varietà Jacobiana (che per $\deg D = 4$ è una curva ellittica) e successivamente di utilizzare il celebrato teorema di Mazur sui possibili gruppi di torsione per una curva ellittica.

Questo ad esempio dà un algoritmo effettivo per dire se un polinomio di quarto grado in $\mathbb{Q}[t]$ è Pelliano.

Bound di questo genere si possono in teoria ottenere per arbitrari campi di numeri, utilizzando al posto del teorema di Mazur il teorema di Merel che dice che l'ordine dei gruppi di torsione di curve ellittiche su campi di numeri è limitato da una costante dipendente solo dal grado dell'estensione. Essi non sono però effettivi, perché non sono attualmente note le costanti in questione.

4.3 $\star$ Determinazione della Pellianità

Per poter determinare algoritmicamente se un dato polinomio $D \in K[t]$ è pelliano, si può utilizzare la seguente osservazione:

Dato $D(t) \in K[t]$ squarefree definiamo la curva $\mathcal{C} : u^2 = D(t)$ dentro $\mathbb{A}^2_K$, il cui proiettivizzato ha due punti all'infinito, denotati con ∞_- e ∞_+. La differenza $\delta = \infty_+ - \infty_-$ è un divisore di grado zero, e quindi definisce un punto nello Jacobiano $J = \mathrm{Pic}^0\mathcal{C}$.

Lemma 8: Sia K algebricamente chiuso e D squarefree; Allora l'equazione di Pell $P^2 - D(t)Q^2 = 1$ ha una soluzione polinomiale non costante se e solo se δ è un punto di torsione di J, nel qual caso il suo ordine coincide con il grado $\deg P(t)$ della soluzione minimale.

Dimostrazione. Presa una soluzione non banale $(p(t), q(t))$ si possono considerare le due funzioni $\varphi_\pm = p \pm uq \in K(\mathcal{C})$, che sono regolari e non costanti sulla parte affine, con $\varphi_+\varphi_- = 1$. Il loro divisore allora è tutto contenuto nei punti all'infinito, ed avendo grado zero deve essere $\mathrm{div}\varphi_+ = m\delta$. Ma per definizione di Pic^0, $m\delta = 0$ poiché è principale. E valgono anche le implicazioni al contrario. $\square$

In particolare, esistono degli algoritmi per capire se un dato punto è di torsione nello Jacobiano sfruttando le buone riduzioni modulo primi e, per il lemma appena enunciato, ciò permette di comprendere se l'equazione di Pell ha soluzione. Si veda ad esempio Yu [1998], dove viene fornito un algoritmo per dire se un polinomio è o non è pelliano (e nel caso calcolare la soluzione fondamentale) nel caso in cui K sia un campo di numeri.

Riferimenti bibliografici

N. H. Abel. Ueber die Integration der Differential-Formel $\frac{\varrho d.x}{\sqrt{R}}$, wenn R und ϱ ganze Functionen sind. *J. Reine Angew. Math.*, 1:185–221, 1826.

Artūras Dubickas and Jörn Steuding. The polynomial Pell equation. *Elem. Math.*, 59(4):133–143, 2004.

R. C. Mason. *Diophantine equations over function fields*, volume 96 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1984.

Zachary L. Scherr. *Rational Polynomial Pell Equations.* PhD thesis, 2013.

A. Schinzel. On some problems of the arithmetical theory of continued fractions. II. *Acta Arith.*, 7: 287–298, 1961/1962.

Noah Snyder. An alternate proof of Mason's theorem. *Elem. Math.*, 55(3):93–94, 2000.

W. W. Stothers. Polynomial identities and Hauptmoduln. *Quart. J. Math. Oxford Ser. (2)*, 32(127): 349–370, 1981.

Xuan Chuong van der Poorten, Alfred J. e Tran. Quasi-elliptic integrals and periodic continued fractions. *Monatsh. Math.*, 131(2):155–169, 2000.

Jing Yu. On arithmetic of hyperelliptic curves. 1998.

Umberto Zannier. Unlikely intersections and Pell's equations in polynomials. In *Trends in contemporary mathematics*, volume 8 of *Springer INdAM Ser.*, pages 151–169. Springer, Cham, 2014.