Università degli Studi di Padova

Facoltà di Scienze Matematiche, Fisiche e Naturali

Corso di Laurea in Matematica

Teoremi di Mordell e Lutz-Nagell. Relazioni con due classici problemi aritmetici.

Tesi di Laurea Triennale in Matematica

Relatore:
Prof. Maurizio Candilera

Candidato:
Marta Pieropan

Anno accademico 2009-2010

Indice

Introduzione

Trovare soluzioni razionali di equazioni polinomiali è un tipico problema diofanteo: se l'equazione è definita da un polinomio in due variabili ad esso corrisponde un oggetto geometrico, una curva algebrica piana, e risolvere il problema diofanteo significa trovare i punti a coordinate razionali, o più semplicemente i punti razionali, della curva.

Le rette e le coniche sono, rispettivamente, le curve definite da equazioni di primo e secondo grado; su queste curve sappiamo individuare i punti razionali. Se l'equazione è a coefficienti razionali allora un punto della retta ha entrambe le coordinate razionali se e solo se ha una coordinata razionale e l'insieme dei punti razionali di una retta è vuoto oppure isomorfo a $\mathbb{Q}$. Per trovare i punti razionali di una conica si può parametrizzarla con un fascio di rette centrato in un punto razionale della conica. Altrettanto facilmente si trattano le cubiche singolari, che si possono parametrizzare con un fascio di rette avente come centro il punto singolare della cubica.

Una cubica liscia e una retta si intersecano in tre punti distinti, per questa ragione le curve ellittiche non si possono parametrizzare con fasci di rette, ma, con il metodo delle secanti e delle tangenti, si può definire un'operazione di somma tra i punti, detta Somma di Poincaré, che rende l'insieme dei punti razionali della curva un gruppo abeliano.

La legge di gruppo si esprime tramite relazioni algebriche birazionali tra le coordinate, se l'equazione della cubica è in forma di Weierstrass

$$y^2 = x^3 + ax^2 + bx + c$$

le espressioni che descrivono la legge di gruppo sono particolarmente semplici.

Ogni cubica liscia con un punto razionale, o curva ellittica, si può mettere in forma di Weierstrass tramite trasformazioni birazionali, se il punto razionale è un punto di flesso basta una trasformazione proiettiva.

Scopo principale di questo lavoro di tesi è lo studio della struttura del gruppo dei punti razionali di una curva ellittica.

Due curve ellittiche che si esprimono tramite equazioni a coefficienti in un campo $\mathbb{K}$ si dicono equivalenti su $\mathbb{K}$ se si ottengono una dall'altra tramite opportune proiettività di $\mathbb{P}_2(\mathbb{K})$. Su un campo algebricamente chiuso, per esempio $\mathbb{C}$, le curve ellittiche sono classificate dall'invariante j: due curve

con lo stesso invariante j sono equivalenti, nel senso che si ottengono una dall'altra mediante opportune trasformazioni lineari a coefficienti in $\mathbb{C}$ e hanno la stessa struttura di gruppo $E(\mathbb{C})$.

L'invariante j non classifica il gruppo dei punti razionali di una curva ellittica, infatti due curve a coefficienti in $\mathbb{Q}$ hanno lo stesso invariante j se e solo se sono legate da opportune trasformazioni lineari nella chiusura algebrica di $\mathbb{Q}$ e in generale non sono trasformazioni razionali, dunque due curve con lo stesso invariante j non hanno necessariamente lo stesso gruppo $E(\mathbb{Q})$. Lo studio del gruppo dei punti razionali di una curva ellittica risulta dunque qualcosa di più complesso del semplice calcolo di un invariante definito tramite relazioni algebriche tra i suoi coefficienti e, come vedremo, non c'è ancora un metodo standard per determinarlo.

Nel 1922 Mordell dimostrò che il gruppo dei punti razionali $E(\mathbb{Q})$ di una curva ellittica è finitamente generato:

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$$

dove $E(\mathbb{Q})_{\text{tors}}$ è il sottogruppo dei punti di torsione della curva E e r si dice il rango di E.

Il teorema di Mordell ci dice che la conoscenza di un numero finito di punti razionali della curva ellittica è sufficiente a determinarli tutti, così come avere un fascio di parametrizzazione permette di determinare tutti i punti razionali di una conica o di una cubica singolare. Però non dà un metodo per determinare un sistema di generatori, né per calcolare il rango o la struttura del sottogruppo di torsione $E(\mathbb{Q})_{\text{tors}}$.

Negli anni '30 E. Lutz e T. Nagell scoprirono indipendentemente alcune proprietà dei punti di torsione delle curve ellittiche da cui si ricava un algoritmo generale per determinare completamente $E(\mathbb{Q})_{\text{tors}}$ delle curve ellittiche, ovvero calcolarne tutti gli elementi.

Il problema del calcolo del rango di una curva ellittica invece non è ancora stato risolto. Dalla dimostrazione del teorema di Mordell si possono ricavare delle stime superiori, che però di solito non sono sufficienti a stabilire il rango della curva come accade, per esempio, nel caso di $y^2 = x^3 - 4x$. Non ci sono formule semplici per il rango delle curve ellittiche, attualmente la congettura di Birch e Swinnerton-Dyer è ciò che più si avvicina alla soluzione del problema e fa uso delle relazioni tra le curve ellittiche e le funzioni L.

È interessante soffermarsi ad esaminare le tecniche dimostrative usate da Mordell, infatti egli definisce prima una funzione altezza h_0 per misurare i punti razionali della curva, basandosi sul fatto che, per la particolare forma di Weierstrass ridotta dell'equazione: $y^2 = x^3 + Ax + B$, essi sono quasi completamente determinati dalla coordinata x, ovvero punti con

la stessa coordinata x hanno lo stesso comportamento secondo la legge di gruppo. Se P ha coordinata $x = \frac{p}{q}$, con p, q interi coprimi, si definisce $h_0(P) = \log \max\{|p|, |q|\}$. A partire dalla mappa h_0 con un'operazione di limite Mordell sviluppa una nozione di altezza canonica h che intuitivamente valuta il comportamento all'infinito delle potenze dei punti:

$$h(P) = \lim_{n \to +\infty} \frac{h_0(2^n P)}{4^n}$$

ed è un indice di quanto restano lontani dall'elemento neutro del gruppo, che è il punto all'infinito. Sebbene perda la connessione diretta con le coordinate del punto che misura, paragonandola alla funzione h_0 l'altezza canonica h ha delle proprietà migliori relativamente alla legge di gruppo di Poincaré ed è dunque più adatta a descrivere il gruppo $E(\mathbb{Q})$.

L'altezza canonica viene usata nella parte finale della dimostrazione per applicare un metodo di discesa infinita e dimostrare con una *reductio ad absurdum* che il gruppo $E(\mathbb{Q})$ ha un numero finito di generatori.

La dimostrazione del teorema è piuttosto lunga e suddivisa in vari passi, che sono descritti in dettaglio all'inizio del capitolo 3, richiede anche notevoli risultati di teoria dei numeri perché per valutare il gruppo dei punti razionali della curva Mordell lavora sul campo di spezzamento del polinomio x^3+ax^2+bx+c.

Gli ultimi due capitoli di questo lavoro sono dedicati allo studio di particolari curve ellittiche legate a classici problemi di aritmetica. Prima si focalizza l'attenzione su due problemi diofantei risolti da Fermat trattando due particolari curve di quarto grado che sono birazionalmente equivalenti a due curve ellittiche; poi si tratta in dettaglio il problema dei numeri congruenti.

I quesiti di Fermat sono due esempi in cui le curve ellittiche forniscono buoni modelli per descrivere problemi di aritmetica, infatti le trasformazioni che le legano alle quartiche traducono la legge di gruppo della curva ellittica nei metodi di discesa usati da Fermat per trovare nuove soluzioni a partire da alcune date. I punti delle curve ellittiche ereditano tramite le trasformazioni birazionali molte proprietà dei punti delle curve di quarto grado e viceversa e si può così costruire un dizionario tra le due curve. Sono due tipi diversi di applicazione del metodo di discesa, il primo riguarda il caso quartico dell'Ultimo Teorema di Fermat e viene usato un argomento di discesa infinita che si può effettuare in modo equivalente sulla quartica o sulla cubica ed è parallelo al ragionamento conclusivo della dimostrazione del teorema di Mordell; il secondo esempio invece usa il metodo di discesa per costruire soluzioni non banali della quartica di Fermat, che equivale a dimostrare che il rango della curva ellittica ad essa associata non è nullo. Mostrare la corrispondenza tra il metodo di discesa e la duplicazione dei punti sulla cubica può coinvolgere calcoli sulle coordinate molto lunghi e complicati, nell'esempio del problema di Fermat a Mersenne è stato possibile verificarli

solo attraverso l'ausilio di un programma informatico di calcolo simbolico, che è stato riportato in Appendice.

Il problema dei numeri congruenti è antico, risale almeno al X secolo d.C. e consiste nel trovare un criterio per stabilire se un numero naturale n è l'area di un triangolo rettangolo con i lati razionali, ovvero se è un numero congruente. Una condizione equivalente è che la curva ellittica $y^2 = x^3 - n^2x$ abbia rango strettamente positivo. Un problema di formulazione elementare come quello dei numeri congruenti si rivela essere della stessa difficoltà del problema di determinare il rango di una curva ellittica: lo sappiamo risolvere in molti casi particolari, per esempio $n = 2(2ab)(a^2 - b^2)$ è congruente per ogni scelta di $a, b \in \mathbb{Z}$ mentre $n = 1$, $n = 2$ e ogni primo $p \equiv 3 \mod 4$ non lo sono, ma non esiste un metodo generale.

Le curve ellittiche di equazione $y^2 = x^3 - n^2x$ hanno tutte invariante $j = 1728$ e sottogruppo di torsione isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, sono dunque un esempio di curve con lo stesso invariante j e sottogruppo di torsione, ma in generale con gruppi $E(\mathbb{Q})$ non isomorfi.

Gli esempi riportati mostrano il legame tra ambiti apparentemente diversi, la geometria delle curve ellittiche e l'aritmetica, e fanno parte della miriade di casi particolari che hanno contribuito e contribuiscono ad accrescere la base per lo studio e la ricerca dei teoremi generali che, prima di essere dimostrati, nascono come congetture dalla manipolazione di singoli esempi.

Capitolo 1

Nozioni Preliminari

In questo capitolo sono ricordati alcuni concetti e risultati generali di teoria delle curve algebriche piane, con particolare attenzione alle cubiche, che verranno utilizzati nelle sezioni successive. Non sono riportate le dimostrazioni, queste si possono trovare nei riferimenti bibliografici indicati.

1.1 Richiami sulle curve piane

Sia $\mathbb{K}$ un campo, in generale $\mathbb{C}$ o $\mathbb{R}$, sarà di nostro interesse considerare in particolare il campo dei numeri razionali $\mathbb{Q}$. Indichiamo con $\mathbb{P}_2(\mathbb{K})$ il piano proiettivo dei punti a coordinate in $\mathbb{K}$.

Definizione 1.1. Una curva piana proiettiva di grado $d > 0$ su $\mathbb{K}$ è un polinomio omogeneo (non nullo) $F \in \mathbb{K}[z, x, y]$ di grado d.

Due polinomi omogenei di grado d in $\mathbb{K}[z, x, y]$ definiscono la stessa curva se sono uno un multiplo dell'altro. Se $F \in \mathbb{K}[z, x, y]$ è un polinomio omogeneo indichiamo con $F(\mathbb{K}) = \{(z, x, y) : F(z, x, y) = 0\} \subseteq \mathbb{P}_2(\mathbb{K})$ l'insieme dei $\mathbb{K}$-punti razionali della curva F.

Il gruppo delle trasformazioni lineari invertibili di $\mathbb{K}^3$, $GL_3(\mathbb{K})$, agisce transitivamente su $\mathbb{K}^3 \setminus \{(0, 0, 0)\}$. Dunque l'azione di $GL_3(\mathbb{K})$ su $\mathbb{P}_2(\mathbb{K})$ è transitiva. Se $(z_0, x_0, y_0) \in \mathbb{P}_2(\mathbb{K})$ allora esiste $\varphi \in GL_3(\mathbb{K})$ tale che $\varphi(z_0, x_0, y_0) = (1, 0, 0)$, φ è un sistema di coordinate locali affini di $\mathbb{P}_2(\mathbb{K})$ intorno al punto (z_0, x_0, y_0).

Definizione 1.2. Se $F \in \mathbb{K}[z, x, y]$ è una curva piana proiettiva su $\mathbb{K}$, $(z_0, x_0, y_0) \in F(\mathbb{K})$ e $\varphi(z_0, x_0, y_0) = (1, 0, 0)$ è un sistema di coordinate locali affini, $f(x, y) = F(\varphi^{-1}(1, x, y))$ è la curva affine associata a F nel sistema di coordinate locali φ.

f è la curva che si ottiene passando dal piano proiettivo a quello affine scegliendo (z_0, x_0, y_0) come origine. Se F è una curva di grado d su $\mathbb{K}$ e $(z_0, x_0, y_0) \in F(\mathbb{K})$ consideriamo la curva affine $f \in \mathbb{K}[x, y]$ che si ottiene

scegliendo come origine (z_0, x_0, y_0). f è un polinomio, in generale non omogeneo, di grado $\leq d$, scriviamo $f = f_0 + f_1 + \cdots + f_d$ dove $\forall l = 0, 1, \ldots, d$ $f_l \in \mathbb{K}[x, y]$ è un polinomio omogeneo di grado l. Osservo che $f_0 = 0$ perché (z_0, x_0, y_0) appartiene alla curva F. Diciamo che il punto (z_0, x_0, y_0) è singolare per la curva F se $f_1 = 0$, non singolare altrimenti. La definizione di punto singolare non dipende dal sistema di coordinate locali affini scelto, una prova di questo si può trovare in [K], II, §2.

Sia $\overline{\mathbb{K}}$ la chiusura algebrica di $\mathbb{K}$.

Proposizione 1.1 (Criterio differenziale di non singolarità)**.** *Un punto $(z_0, x_0, y_0) \in F(\overline{\mathbb{K}})$ è non singolare per F se e solo se almeno una tra*

$$\frac{\partial F}{\partial z}(z_0, x_0, y_0), \quad \frac{\partial F}{\partial x}(z_0, x_0, y_0), \quad \frac{\partial F}{\partial y}(z_0, x_0, y_0)$$

è non nulla, e in tal caso la retta tangente a F in (z_0, x_0, y_0) ha equazione

$$\frac{\partial F(z_0, x_0, y_0)}{\partial z} z + \frac{\partial F(z_0, x_0, y_0)}{\partial x} x + \frac{\partial F(z_0, x_0, y_0)}{\partial y} y = 0.$$

Per la dimostrazione si veda [K], II, §2, Proposizione 2.6.

Definizione 1.3. Una curva piana F su $\mathbb{K}$ si dice non singolare, o liscia, se ogni punto di $F(\overline{\mathbb{K}})$ è non singolare per F.

Teorema 1.2 (Teorema di Bézout)**.** *Due curve piane proiettive di gradi d e d', senza componenti comuni, si incontrano in esattamente dd' punti, se questi sono contati con le loro molteplicità.*

Per la dimostrazione si veda [C], III, §1, Teorema 1.4.

Se F è una curva piana su $\mathbb{K}$, un punto non singolare $P = (z_0, x_0, y_0) \in F(\mathbb{K})$ si dice punto di flesso per F se la molteplicità di intersezione nel punto P di F con la retta tangente a F in P è ≥ 3, ovvero, usando le notazioni precedenti, se $f_1 | f_2$.

Proposizione 1.3 (Criterio differenziale per i flessi)**.** *Sia F una curva piana di grado d su $\mathbb{K}$, se la caratteristica di $\mathbb{K}$ è diversa da 2 e non divide $d - 1$ allora $(z_0, x_0, y_0) \in F(\mathbb{K})$ è un punto di flesso per F se e solo se* $\det H(z_0, x_0, y_0) = 0$*, dove H è la matrice Hessiana di F.*

Per la dimostrazione si veda [K], II, §3, Proposizione 2.12.

Teorema 1.4 (Euclide)**.** *In ogni terna pitagorica (a, b, c), con a, b coprimi, esattamente uno tra a e b è dispari. Se a è dispari e $c > 0$ allora esistono due interi m, n coprimi, non entrambi dispari, tali che*

$$a = m^2 - n^2 \qquad b = 2mn \qquad c = m^2 + n^2$$

Dimostrazione. Siano a', b', c' le classi di congruenza modulo 4 di a, b, c rispettivamente, allora si ha

$$a'^2 + b'^2 \equiv c'^2 \mod 4$$

Siccome a, b sono coprimi, non sono entrambi pari, se fossero entrambi dispari, allora sarebbero congrui a 1 o 3 modulo 4, e si otterrebbe $a'^2 + b'^2 \equiv 2 \mod 4$, ma 2 non è un quadrato in $\mathbb{Z}_4$, dunque sono uno pari e uno dispari, supponiamo a dispari e b pari. Supponiamo anche $c > 0$.

Se $x = a/c$, $y = b/c$ allora $a^2 + b^2 = c^2 \iff x^2 + y^2 = 1$, parametrizzando il cerchio unitario con il fascio di rette $x = ty - 1$ di centro $(-1, 0)$ tutti i punti razionali si ottengono al variare del parametro $t = \frac{m}{n}$, con $m, n \in \mathbb{Z}$ coprimi:

$$(x, y) = \left(\frac{t^2 - 1}{t^2 + 1}, \frac{2t}{t^2 + 1}\right) = \left(\frac{m^2 - n^2}{m^2 + n^2}, \frac{2mn}{m^2 + n^2}\right)$$

Dunque $(a, b, c) = \frac{u}{v}(m^2 - n^2, 2mn, m^2 + n^2)$ con $m, n \in \mathbb{Z}$ coprimi e $u, v \in \mathbb{Z}$ coprimi. Siccome u, v coprimi si ha che u divide a, b, c ma $GCD(a, b) = 1$ dunque $u = \pm 1$ scegliamo $u = 1$. Allora $c > 0$ dà $v > 0$. Se un primo dispari dividesse v allora dividerebbe $m^2 - n^2$ e $m^2 + n^2$ e dunque dividerebbe m e n contro il fatto che siano coprimi. Se 2 dividesse v allora 4 dividerebbe $2mn$ quindi 2 dividerebbe o m o n, perché m, n coprimi, dunque$va = m^2 - n^2$ sarebbe dispari contro il fatto che v sia divisibile per 2. Dunque v positivo e senza fattori primi, quindi $v = 1$. Così abbiamo dimostrato la tesi, m, n non sono entrambi dispari perché a è dispari. □

1.2 Cubiche

Una cubica su $\mathbb{K}$ è una curva piana di grado 3 su $\mathbb{K}$. D'ora in poi eviteremo di specificare ogni volta il campo $\mathbb{K}$, a meno che non risulti necessario.

Proposizione 1.5. *Su un campo algebricamente chiuso una cubica non singolare F ha almeno un punto di flesso.*

Dimostrazione. I punti di flesso di F sono tutti e soli i punti di intersezione tra F e $\det H$, perché F è non singolare, dunque basta applicare il Teorema di Bézout, 1.2, a queste due curve. □

Definizione 1.4. Una cubica F si dice in forma di Weierstrass se ha equazione

$$y^2 z + a_1 xyz + a_3 yz^2 = x^3 + a_2 x^2 z + a_4 xz^2 + a_6 z^3. \tag{1.1}$$

La forma di Weierstrass affine di F è

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \tag{1.2}$$

e si ottiene scegliendo $z = 0$ come retta all'infinito.

Proposizione 1.6. *Se F è una cubica con un punto di flesso in $F(\mathbb{K})$, allora esiste una trasformazione proiettiva φ di $\mathbb{P}_2(\mathbb{K})$ tale che $F \circ \varphi^{-1}$ sia in forma di Weierstrass.*

Per la dimostrazione si veda [K], II, §4, Proposizione 2.14.

Infatti se $P \in F(\mathbb{K})$ è un punto di flesso per la cubica F, con opportune trasformazioni proiettive si può scegliere un sistema di coordinate in cui $P = (0, 0, 1)$ e la retta tangente a F in P sia $z = 0$, quindi

$$F(z, x, y) = c_{zyy}zy^2 + c_{zxy}zxy + c_{zzy}z^2y + c_{xxx}x^3 + c_{zxx}zx^2 + c_{zzx}z^2x + c_{zzz}z^3$$

con $c_{zyy} \neq 0$ e $c_{xxx} \neq 0$, riscalando si può rendere l'equazione di F in forma di Weierstrass.

Sia F una cubica in forma di Weierstrass affine (1.2), se la caratteristica del campo $\mathbb{K}$ è $\neq 2$ allora, completando il quadrato a primo membro, si può ridurre l'equazione ottenendo

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \tag{1.3}$$

dove

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \end{aligned} \tag{1.4}$$

Se la caratteristica di $\mathbb{K}$ è diversa da 2 e da 3, nell'equazione (1.3) si può completare il cubo in modo da eliminare il termine di secondo grado e si ottiene la forma di Weierstrass ridotta

$$y^2 = x^3 - 27c_4x - 54c_6 \tag{1.5}$$

con

$$\begin{aligned} c_4 &= b_2^2 - 24b_4 \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \end{aligned} \tag{1.6}$$

Definizione 1.5. Qualunque sia la caratteristica del campo $\mathbb{K}$, data una cubica in forma di Weierstrass (1.2), si definisce il discriminante della curva

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \tag{1.7}$$

dove b_2, b_4, b_6 sono definiti in (1.4) e $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$. Se $\mathbb{K}$ non ha caratteristica 2 o 3, allora si ottiene:

$$\Delta = \frac{c_4^3 - c_6^2}{1728}$$

Dato un polinomio di terzo grado $f(x) = (x - r_1)(x - r_2)(x - r_3)$ il discriminante di f è $d = (r_1 - r_2)^2(r_2 - r_3)^2(r_3 - r_1)^2$, in particolare per i polinomi $f(x) = x^3 + px + q$ si ha $d = -4p^3 - 27q^2$. Se $\mathbb{K}$ ha caratteristica $\neq 2$, per una cubica che ammette forma di Weierstrass definiamo d_b e d_c i discriminanti del polinomio di terzo grado a secondo membro nelle equazioni ridotte (1.3) e (1.5) rispettivamente.

Proposizione 1.7. *Se $\mathbb{K}$ ha caratteristica $\neq 2$ allora per una cubica che ammette forma di Weierstrass si hanno le seguenti uguaglianze:*

$$d_c = 2^{12}3^{12}d_b \qquad \Delta = 2^4 d_b.$$

Per la dimostrazione si veda [K], III, §2, Proposizione 3.6.

Proposizione 1.8. *Una cubica che ammette forma di Weierstrass (1.1) è singolare se e solo se $\Delta = 0$.*

Per la dimostrazione si veda [K], III, §2, Teorema 3.2.

Consideriamo ora le trasformazioni affini $\varphi \in GL_3(\mathbb{K})$ che mantengono le cubiche in forma di Weierstrass: sono della forma

$$x = u^2x' + r \qquad y = u^3y' + su^2x' + t \tag{1.8}$$

ovvero

$$\begin{pmatrix} z \\ x \\ y \end{pmatrix} = \varphi^{-1} \begin{pmatrix} z' \\ x' \\ y' \end{pmatrix} \quad \text{con} \quad \varphi^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ r & u^2 & 0 \\ t & su^2 & u^3 \end{pmatrix} \tag{1.9}$$

con $r, s, t, u \in \mathbb{K}$. Naturalmente sono cambi di coordinate che tengono fisso il punto $(0, 0, 1)$ e lasciano unita la retta all'infinito, $z = 0$.

Se F è una cubica in forma di Weierstrass 1.2 e φ è una trasformazione che mantiene la cubica in forma di Weierstrass allora $a_i' = u^{-i}A_i$, dove A_i sono espressioni polinomiali in $r, s, t, a_1, a_2, a_3, a_4, a_6$ non dipendenti da u, sono i coefficienti della forma di Weierstrass della trasformata di F. Si dice che il coefficiente a_i ha peso i, che corrisponde alla potenza negativa di u presente in a_i'. Anche i coefficienti b_i e c_i hanno peso i e in particolare si ha che $c_i' = u^{-i}c_i$ cioè i coefficienti della forma di Weierstrass ridotta 1.5 non dipendono da r, s, t, da questo di ottiene che, se la caratteristica di $\mathbb{K}$ non è 2 o 3, il discriminante Δ non dipende da r, s, t e ha peso 12.

1.3 Somma di Poincaré

Per il teorema di Bézout su un campo algebricamente chiuso una cubica e una retta si incontrano esattamente in tre punti, contati con le opportune molteplicità. Se $\mathbb{K}$ non è algebricamente chiuso una cubica non singolare e una retta si intersecano in 0, 1 o 3 punti a coordinate in $\mathbb{K}$, per una dimostrazione di questo fatto si veda [K], II, §4, Proposizione 2.15. Dunque se F è una cubica non singolare tale che $F(\mathbb{K}) \neq \emptyset$ e $P, Q \in F(\mathbb{K})$, la retta passante per P e Q interseca la cubica in un terzo punto che indicheremo con $P \cdot Q$. In questo modo resta ben definita su $F(\mathbb{K})$ un'operazione

$$\begin{aligned} F(\mathbb{K}) \times F(\mathbb{K}) &\to F(\mathbb{K}) \\ (P, Q) &\mapsto P \cdot Q \end{aligned}$$

che è commutativa, ma non associativa.

Proposizione 1.9. *Per ogni scelta di punti $P, Q, P', Q' \in F(\mathbb{K})$ si ha*

$$(P \cdot P') \cdot (Q \cdot Q') = (P \cdot Q) \cdot (P' \cdot Q'). \tag{1.10}$$

Per la dimostrazione si veda [K], III, §3, Lemma 3.9.

Definizione 1.6. Fissato un punto $O \in F(\mathbb{K})$ si definisce la somma di Poincaré:

$$\begin{aligned} F(\mathbb{K}) \times F(\mathbb{K}) &\to F(\mathbb{K}) \\ (P, Q) \quad &\mapsto P + Q = O \cdot (P \cdot Q) \end{aligned}$$

Teorema 1.10. *Se F è una cubica non singolare e $O \in F(\mathbb{K})$, la somma di Poincaré rende $(F(\mathbb{K}), +)$ un gruppo abeliano con O come elemento neutro e l'opposto definito da $-P = P \cdot (O \cdot O)$.*

Se si sceglie un diverso punto origine $O' \in F(\mathbb{K})$ le due strutture di gruppo $(F(\mathbb{K}), +)$ e $(F(\mathbb{K}), +')$ sono isomorfe e le due operazioni sono legate dalla relazione $P +' Q = P + Q - O'$.

Se $\mathbb{K}'$ è un'estensione di $\mathbb{K}$ allora l'inclusione $F(\mathbb{K}) \subseteq F(\mathbb{K}')$ è un omomorfismo di gruppi

Per la dimostrazione si veda [K], III, §3, Teorema 3.8, oppure [C], II, §7, Teorema 7.5.3.

1.4 Richiami sui numeri algebrici

Definizione 1.7. Un numero $z \in \mathbb{C}$ si dice intero algebrico se è una radice di un polinomio monico a coefficienti in $\mathbb{Z}$. Indichiamo con $\mathcal{O}$ l'insieme degli interi algebrici.

Proposizione 1.11. *$\mathcal{O}$ è un sottoanello di $\mathbb{K}$*

Dimostrazione. Siano $\alpha, \beta \in \mathcal{O}$, consideriamo il sottoanello $\mathbb{Z}[\alpha, \beta]$ di $\mathbb{K}$, osserviamo che come gruppo additivo è abeliano e finitamente generato, dunque $\mathbb{Z}[\alpha, \beta] = \mathbb{Z}u_1 \oplus \cdots \oplus \mathbb{Z}u_n$ con $u_1, \ldots, u_n \in \mathbb{K}$.
Se $\gamma \in \mathbb{Z}[\alpha, \beta]$ allora $u_j\gamma = \sum_{i=1}^{n} a_{ij}u_i$ con $a_{ij} \in \mathbb{Z} \quad \forall i, j = 1, \ldots, n$, sia $A = (a_{i,j})_{i,j=1,\ldots,n}$, abbiamo

$$A \begin{pmatrix} u_1 \\ \vdots \\ v_n \end{pmatrix} = \gamma \begin{pmatrix} u_1 \\ \vdots \\ v_n \end{pmatrix}$$

dunque γ è un autovalore di A e quindi uno zero del polinomio caratteristico di A che è $\det(x\mathbb{I}_n - A)$, polinomio monico di grado n e a coefficienti in $\mathbb{Z}$. Allora γ è un intero algebrico e $\mathbb{Z}[\alpha, \beta] \subseteq \mathcal{O}$, abbiamo così provato che $\mathcal{O}$ è un sottoanello di $\mathbb{K}$. □

Sia $\mathbb{K}$ un'estensione algebrica di grado finito su $\mathbb{Q}$. Definiamo $\mathcal{O}_\mathbb{K} = \mathcal{O} \cap \mathbb{K}$ l'anello degli interi algebrici di $\mathbb{K}$.

$\mathbb{K}$ è un'estensione di Galois di $\mathbb{Q}$, perché è un'estensione di grado finito. Allora per ogni $\alpha \in \mathbb{K}$ resta ben definita la norma di α

$$\mathrm{N}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(\mathbb{K}|\mathbb{Q})} \sigma(\alpha) \qquad \in \mathbb{Q}$$

Proposizione 1.12. $\mathrm{N} : \mathbb{K}^\times \to \mathbb{Q}^\times$ *è un omomorfismo di gruppi moltiplicativi e* $\mathrm{N}(\mathcal{O}_\mathbb{K}) \subseteq \mathbb{Z}$

Dimostrazione. Se $\alpha, \beta \in \mathbb{K}^\times$ allora poiché i $\sigma \in \mathrm{Gal}(\mathbb{K}|\mathbb{Q})$ sono omomorfismi

$$\begin{aligned}\mathrm{N}(\alpha\beta) = \prod_{\sigma \in \mathrm{Gal}(\mathbb{K}|\mathbb{Q})} \sigma(\alpha\beta) = \prod_{\sigma \in \mathrm{Gal}(\mathbb{K}|\mathbb{Q})} (\sigma(\alpha)\sigma(\beta)) = \\ = \prod_{\sigma \in \mathrm{Gal}(\mathbb{K}|\mathbb{Q})} \sigma(\alpha) \prod_{\sigma \in \mathrm{Gal}(\mathbb{K}|\mathbb{Q})} \sigma(\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)\end{aligned}$$

dunque N è un omomorfismo di gruppi moltiplicativi. Osserviamo anche che $\mathrm{N}(\alpha)$ è il termine noto del polinomio minimo di α, dunque se $\alpha \in \mathcal{O}_\mathbb{K}$ si ha $\mathrm{N}(\alpha) \in \mathbb{Z}$. □

Indichiamo con $\mathcal{O}_\mathbb{K}^\times$ il gruppo delle unità di $\mathcal{O}_\mathbb{K}$.

Proposizione 1.13. *Le unità di* $\mathcal{O}_\mathbb{K}$ *sono gli elementi* $u \in \mathcal{O}_\mathbb{K}$ *tali che* $\mathrm{N}(u) \in \{\pm 1\}$.

Dimostrazione. Per la proposizione precedente, se $u \in \mathcal{O}_\mathbb{K}$ è invertibile allora $\mathrm{N}(u) \in \mathbb{Z}$ e $\mathrm{N}(u^{-1}) = \mathrm{N}(u)^{-1} \in \mathbb{Z}$, dunque $\mathrm{N}(u) \in \{\pm 1\}$. Se invece $u \in \mathcal{O}_\mathbb{K}$ con $\mathrm{N}(u) \in \{\pm 1\}$ allora

$$\begin{aligned}&\mathrm{N}(u) = \prod_{\sigma \in \mathrm{Gal}(\mathbb{K}|\mathbb{Q})} \sigma(u) = u \prod_{\substack{\sigma \in \mathrm{Gal}(\mathbb{K}|\mathbb{Q}) \\ \sigma \neq \mathrm{id}}} \sigma(u) \\ \Rightarrow \quad &u^{-1} = \mathrm{N}(u)^{-1} \prod_{\substack{\sigma \in \mathrm{Gal}(\mathbb{K}|\mathbb{Q}) \\ \sigma \neq \mathrm{id}}} \sigma(u) \quad \in \mathcal{O}_\mathbb{K}\end{aligned}$$

□

Teorema 1.14 (Dirichlet)**.** $\mathcal{O}_\mathbb{K}^\times$ *è un gruppo abeliano finitamente generato.*

Per la dimostrazione si veda [M], V, Teorema 38.

Proposizione 1.15. *Proprietà degli ideali di* $\mathcal{O}_\mathbb{K}$*:*

i) ogni ideale non nullo $I \subseteq \mathcal{O}_\mathbb{K}$ *è un gruppo abeliano libero di rango* $n = [\mathbb{K} : \mathbb{Q}]$ *e* I *genera* $\mathbb{K}$ *come spazio vettoriale su* $\mathbb{Q}$*;*

ii) ogni ideale non nullo di $\mathcal{O}_\mathbb{K}$ contiene un elemento non nullo di $\mathbb{Z}$;

iii) ogni ideale non nullo di $\mathcal{O}_\mathbb{K}$ ha indice finito in $\mathcal{O}_\mathbb{K}$;

iv) $\mathcal{O}_\mathbb{K}$ è un anello Noetheriano, cioè ogni catena ascendente di ideali è stazionaria;

v) ogni ideale non banale primo di $\mathcal{O}_\mathbb{K}$ è massimale.

Per la dimostrazione si veda [M], II e III.

Sull'insieme degli ideali non nulli di $\mathcal{O}_\mathbb{K}$ si definisce un'operazione di prodotto: se I, J sono ideali non nulli di $\mathcal{O}_\mathbb{K}$

$$IJ = \{\sum_{i=1}^{n} a_i, b_i : a_i \in I, b_i \in J\}$$

tale prodotto è associativo, commutativo e ha come elemento neutro l'ideale $\mathcal{O}_\mathbb{K}$. Tramite questo prodotto possiamo ora definire sull'insieme degli ideali non nulli di $\mathcal{O}_\mathbb{K}$ una relazione di equivalenza: I, J ideali non nulli di $\mathcal{O}_\mathbb{K}$ si dicono equivalenti se esistono $\alpha, \beta \in \mathcal{O}_\mathbb{K}$ tali che $(\alpha)I = (\beta)J$. Allora:

- l'operazione di prodotto definita sopra rispetta le classi di equivalenza, infatti: se $(\alpha)I = (\beta)I'$ e $(\gamma)J = (\delta)J'$ si ha

$$(\alpha\gamma)IJ = (\alpha)I(\gamma)J = (\beta)I'(\delta)J' = (\beta\delta)I'J'$$

- gli ideali principali formano un'unica classe che agisce come identità per il prodotto tra le classi.

Il numero delle classi di equivalenza degli ideali non nulli di $\mathcal{O}_\mathbb{K}$ si dice il numero di classi di $\mathbb{K}$, lo indichiamo con $h_\mathbb{K}$.

Teorema 1.16. *Il numero di classi di un'estensione finita di $\mathbb{Q}$ è finito.*

Per la dimostrazione si veda [M], V, Teorema 35, Corollario 2.

Proposizione 1.17. *L'insieme delle classi di ideali non nulli di $\mathcal{O}_\mathbb{K}$ è un gruppo con l'operazione di prodotto tra ideali ed elemento neutro la classe degli ideali principali. Tale gruppo si dice il gruppo delle classi di ideali di $\mathbb{K}$ e il suo ordine è $h_\mathbb{K}$.*

Dimostrazione. Basta dimostrare che ogni classe di ideali non nulli ammette inversa rispetto al prodotto. Sia I un ideale non nullo di $\mathcal{O}_\mathbb{K}$, sia $\alpha \in I$, $\alpha \neq 0$, allora $J = \{\beta \in \mathcal{O}_\mathbb{K} : \beta I \subseteq (\alpha)\}$ è un ideale non nullo di $\mathcal{O}_\mathbb{K}$ e si ha $IJ \subseteq (\alpha)$. Dunque la classe di I ammette una classe inversa rispetto al prodotto. Poichè il numero di classi di $\mathbb{K}$ è finito, esiste $i \in \mathbb{N}$, $i \geq 2$, tale che I e I^i sono equivalenti, $(\alpha)I = (\beta)I^i$ con $\alpha, \beta \in \mathcal{O}_\mathbb{K}$, allora $(\beta)I^{i-2}I = (\alpha)$ e la classe di I^{i-2} è l'inverso della classe di I. □

Teorema 1.18. *Ogni ideale proprio I di $\mathcal{O}_{\mathbb{K}}$ si scrive in modo unico come prodotto di ideali primi propri di $\mathcal{O}_{\mathbb{K}}$*

$$I = \prod_{i=1}^{N} P_i^{k_i}$$

dove i k_i sono numeri interi positivi tali che $I \subset P_i^{k_i}$, ma $I \not\subset P_i^{k_i+1}$.

Dimostrazione. Esistenza. Iniziamo con due osservazioni.

Se A, B sono due ideali non nulli di $\mathcal{O}_{\mathbb{K}}$ e $A \subset B$ allora esiste un ideale non nullo $C \subset \mathcal{O}_{\mathbb{K}}$ tale che $A = BC$, basta prendere $C = \{\beta \in \mathcal{O}_{\mathbb{K}} : \beta B \subset A\}$.

Ogni ideale massimale M di $\mathcal{O}_{\mathbb{K}}$ è primo. Supponiamo per assurdo che non sia vero, siano $a, b \notin M$ tali che $ab \in M$, abbiamo due inclusioni strette: $M \subset M + a\mathcal{O}_{\mathbb{K}}$ e $M \subset M + b\mathcal{O}_{\mathbb{K}}$, essendo M un ideale massimale otteniamo $\mathcal{O}_{\mathbb{K}} = M + a\mathcal{O}_{\mathbb{K}} = M + b\mathcal{O}_{\mathbb{K}}$, dunque $1 = n + ar = m + bs$ con $n, m \in M$ e $r, s \in \mathcal{O}_{\mathbb{K}}$ e $1 = 1 \cdot 1 = nm + bns + amr + abrs \in M$, cioè $M = \mathcal{O}_{\mathbb{K}}$ contro il fatto che sia un ideale massimale.

Sia S l'insieme degli ideali di $\mathcal{O}_{\mathbb{K}}$ che non si fattorizzano come prodotto di ideali primi. Poichè $\mathcal{O}_{\mathbb{K}}$ è un anello Noetheriano, S ammette un elemento massimale M, $M \neq \mathcal{O}_{\mathbb{K}}$ perché $\mathcal{O}_{\mathbb{K}} \notin S$ essendo il prodotto di ideali vuoto. M è un ideale proprio, dunque esiste un ideale massimale $P \subset \mathcal{O}_{\mathbb{K}}$ tale che $M \subseteq P$ ed esiste un ideale $I \subset \mathcal{O}_{\mathbb{K}}$ tale che $M = PI$, $M \subsetneq I$ altrimenti, se $M = I$, avremmo $\mathcal{O}_{\mathbb{K}} M = PM$ e $P = \mathcal{O}_{\mathbb{K}}$ contro il fatto che P è un ideale massimale, e dunque proprio, di $\mathcal{O}_{\mathbb{K}}$. Allora $I \notin S$ quindi I è un prodotto di ideali primi e anche $M = PI$ è un prodotto di ideali primi, contro il fatto che $M \in S$, possiamo concludere che $S = \emptyset$ e ogni ideale proprio di $\mathcal{O}_{\mathbb{K}}$ si fattorizza come prodotto di ideali primi.

Unicità. Lo mostriamo per induzione. Siano $P_1 \cdot \cdots \cdot P_r = Q_1 \cdot \cdots \cdot Q_s$ con P_i, Q_i ideali primi di $\mathcal{O}_{\mathbb{K}}$, non necessariamente distinti. Se $r = s = 1$ non c'è niente da dimostrare, se $\max\{r, s\} > 1$ allora $Q_1 \cdot \cdots \cdot Q_s \subseteq P_1 \cdot \cdots \cdot P_r$ dunque $Q_1 \cdot \cdots \cdot Q_s \subseteq P_1$ e P_1 contiene qualche Q_i, infatti supponendo il contrario avremmo che $\forall i = 1, \ldots, s$ esiste $a_i \in Q_i \setminus P_1$ e $a_1 \cdot \cdots \cdot a_s \in Q_1 \cdot \cdots \cdot Q_s \subseteq P_1$, ma P_1 è un ideale primo dunque esiste un indice i tale che $a_i \in P_1$ contro il fatto che $a_i \in Q_i \setminus P_1$. A meno di riordinare i fattori possiamo supporre che $Q_1 \subseteq P_1$ e dunque $Q_1 = P_1$ perchè ogni ideale primo è massimale. Allora $Q_2 \cdot \cdots \cdot Q_s = P_2 \cdot \cdots \cdot P_r$ e il risultato di ottiene per ipotesi induttiva. □

Teorema 1.19. *Se $\mathbb{K}$ è un'estensione finita di $\mathbb{Q}$ e $\mathcal{O}_{\mathbb{K}}$ è l'anello degli interi algebrici di $\mathbb{K}$, allora esiste un sottoanello R di $\mathbb{K}$ contenente $\mathcal{O}_{\mathbb{K}}$ tale che:*

i) R è un dominio a ideali principali,

ii) il gruppo delle unità di R è finitamente generato.

Dimostrazione. Sia h il numero di classi di $\mathbb{K}$, siano $I_1, \dots, I_h$ rappresentanti di ciascuna classe e sia $I_1 = (1)$ l'identità. $\forall j = 1, \dots, h$ sia $u_j \in I_j$ e sia $u = u_1 \cdots u_h$, dunque $u \in I_j \forall j = 1, \dots, h$.

Sia $S = \{1, u, u^2, \dots\}$, abbiamo che $S \neq \emptyset$ e S è chiuso rispetto al prodotto, allora $S^{-1}\mathcal{O}_\mathbb{K} = \{s^{-1}\alpha : s \in S, \alpha \in \mathcal{O}_\mathbb{K}\}$ è un anello. Mostriamo che $S^{-1}\mathcal{O}_\mathbb{K}$ è un dominio a ideali principali con gruppo delle unità finitamente generato.

Se I è un ideale di $\mathcal{O}_\mathbb{K}$ allora $\tilde{I} = S^{-1}I$ è un ideale di $S^{-1}\mathcal{O}_\mathbb{K}$ e ogni ideale di $S^{-1}\mathcal{O}_\mathbb{K}$ ha questa forma, infatti se I_S è un ideale di $S^{-1}\mathcal{O}_\mathbb{K}$ allora $I = I_S \cap \mathcal{O}_\mathbb{K}$ è un ideale di $\mathcal{O}_\mathbb{K}$ e $\tilde{I} = S^{-1}I = S^{-1}(I_S \cap \mathcal{O}_\mathbb{K}) = I_S$. Se I è un ideale di $\mathcal{O}_\mathbb{K}$ indichiamo con $I_S = S^{-1}I$.

Sia $I = I_S \cap \mathcal{O}_\mathbb{K}$, dove I_S è un ideale di $S^{-1}\mathcal{O}_\mathbb{K}$, allora I è equivalente a I_j per qualche $j \in \{1, \dots, h\}$, cioè $(\alpha)I = (\beta)J$ con $\alpha, \beta \in \mathcal{O}_\mathbb{K}$. Poiché $u \in I_j \cap S$ abbiamo che $1 \in u^{-1}I_j$ e dunque $S^{-1}I_j = S^{-1}\mathcal{O}_\mathbb{K}$, allora

$$(\alpha)_S I_S = S^{-1}(\alpha)S^{-1}I = S^{-1}(\alpha)I = S^{-1}(\beta)I_j = S^{-1}(\beta)S^{-1}I_j = \\ = S^{-1}(\beta)S^{-1}\mathcal{O}_\mathbb{K} = S^{-1}(\beta) = (\beta)_S$$

dunque $\frac{\beta}{\alpha} \in S^{-1}\mathcal{O}_\mathbb{K}$ e $I_S = (\frac{\beta}{\alpha})_S$.

Abbiamo mostrato che I_S è un ideale principale, dunque $S^{-1}\mathcal{O}_\mathbb{K}$ è un dominio a ideali principali.

Vediamo ora che $(S^{-1}\mathcal{O}_\mathbb{K})^\times$ è finitamente generato.

Sia $u^{-s}\alpha \in (S^{-1}\mathcal{O}_\mathbb{K})^\times$ e sia $u^{-t}\beta = (u^{-s}\alpha)^{-1}$, allora $\alpha\beta = u^{s+t}$, dunque $\alpha \mid u^{s+t}$ con $s + t \geq 0$. Dunque per ogni $\alpha \in \mathcal{O}_\mathbb{K}$ tale che, per qualche $s \geq 0$, $u^{-s}\alpha \in (S^{-1}\mathcal{O}_\mathbb{K})^\times$, esiste $\beta \in \mathcal{O}_\mathbb{K}$ tale che $\alpha\beta = u^r$ con $r \geq 0$.

Siano $\alpha, \beta \in \mathcal{O}_\mathbb{K}$ e $r \geq 0$ tali che $\alpha\beta = u^r$, mostriamo che tutti gli α con questa proprietà sono generati per moltiplicazione da un numero finito di elementi di $\mathcal{O}_\mathbb{K}$.

Sia $(u) = P_1^{k_1} \cdots P_N^{k_n}$ la fattorizzazione di (u) in ideali primi, allora $(\alpha)(\beta) = (u^r) = (u)^r = P_1^{rk_1} \cdots P_N^{rk_N}$ e dall'unicità della fattorizzazione si ottiene che $(\alpha) = P_1^{l_1} \cdots P_N^{l_N}$ con $0 \leq l_i \leq rk_i \quad \forall i = 1, \dots, N$. Essendo l'insieme delle classi di ideali non nulli di $\mathcal{O}_\mathbb{K}$ un gruppo finito di ordine h, abbiamo che P_i^h è principale per ogni $i = 1, \dots, N$, siano $P_i^h = (\gamma_i)$ e $l_i = q_i h + r_i$ con $0 \leq r_i < h$ per ogni $i = 1, \dots, N$, allora:

$$(\alpha) = (\gamma_1)^{q_1} \cdots (\gamma_N)^{q_N} P_1^{r_1} \cdots P_N^{r_N}$$

dunque $\alpha = \gamma_1^{q_1} \cdots \gamma^{q_N}\gamma$ con $\gamma = \frac{\alpha}{\gamma_1^{q_1} \cdots \gamma^{q_N}} \in P_1^{r_1} \cdots P_N^{r_N} \subseteq \mathcal{O}_\mathbb{K}$. Allora:

$$(\gamma_1^{q_1} \cdots \gamma_N^{q_N}) \left(\frac{\alpha}{\gamma_1^{q_1} \cdots \gamma_N^{q_N}} \right) = (\alpha) = (\gamma_1^{q_1} \cdots \gamma_N^{q_N}) P_1^{r_1} \cdots P_N^{r_N}$$

Dunque $P_1^{r_1} \cdots P_N^{r_N} = \left(\frac{\alpha}{\gamma_1^{q_1} \cdots \gamma_N^{q_N}} \right)$ è un ideale principale.

Se $P_1^{r_1} \cdots P_N^{r_N} = (\delta_{r_1,\dots,r_N})$, allora $\alpha = \gamma_1^{q_1} \cdots \gamma_N^{q_N} \delta_{r_1,\dots,r_N} \varepsilon$ con $\varepsilon \in \mathcal{O}_\mathbb{K}^\times$.

Abbiamo che $(S^{-1}\mathcal{O}_{\mathbb{K}})^\times$ è generato da $\gamma_1, \dots \gamma_N, \delta_{r_1,\dots,r_N}$, che sono in numero finito perché $0 \leq r_j < h \quad \forall j$, e da $\mathcal{O}_{\mathbb{K}}^\times$, che è finitamente generato, dunque $(S^{-1}\mathcal{O}_{\mathbb{K}})^\times$ è finitamente generato.

$(S^{-1}\mathcal{O}_{\mathbb{K}})$ è l'anello R cercato. □

Teorema 1.20 (Dirichlet)**.** *Per ogni coppia di interi a e b con* $\mathrm{MCD}(a,b) = 1$*, la successione di termine generale $an + b$ contiene infiniti numeri primi.*

Per la dimostrazione si veda [K], VII, §1, Teorema 7.1.

1.5 Norme p-adiche

Notazione: con $\mathbb{Z}_p$ indicheremo il campo $\mathbb{Z}/p\mathbb{Z}$.

Definizione 1.8. Dato un numero primo p, per ogni numero razionale non nullo $r \in \mathbb{Q}$ esiste un unico intero $n \in \mathbb{Z}$ tale che $r = p^n \frac{u}{v}$ con $\mathrm{MCD}(p,u) = 1$ e $\mathrm{MCD}(p,v) = 1$, si definisce la norma p-adica di r, $|r|_p = p^{-n}$. Si definisce anche $|0|_p = 0$.

Proprietà della norma p-adica:

- *disuguaglianza ultrametrica*: $|r+s|_p \leq \max\{|r|_p, |s|_p\}$, si ha l'uguaglianza se $|r|_p \neq |s|_p$.

  Infatti, se $r = p^n \frac{u}{v}$ e $s = p^m \frac{z}{w}$, con u, v, z, w coprimi con p, e $m \geq n$, allora $|s|_p \leq |r|_p$ e $\max\{|r|_p, |s|_p\} = |r|_p$, inoltre

  $$r + s = p^n \left(\frac{u}{v} + p^{m-n}\frac{z}{w}\right) = p^n \frac{uw + p^{m-n}zv}{vw}$$

  e $\mathrm{MCD}(vw, p) = 1$, quindi

  $$|r+s|_p \leq p^{-n} = |r|_p = \max\{|r|_p, |s|_p\}$$

- *rispetta il prodotto*: $|rs|_p = |r|_p|s|_p$.

Definizione 1.9. Si dice che $r \in \mathbb{Q}$ è p-intero se $|r|_p \leq 1$.

Gli elementi p-interi di $\mathbb{Q}$ formano un sottoanello di $\mathbb{Q}$ contenente $\mathbb{Z}$, infatti: se $|r|_p \leq 1$ e $|s|_p \leq 1$ allora $|r+s|_p \leq \max\{|r|_p, |s|_p\} \leq 1$ e $|rs|_p = |r|_p|s|_p \leq 1$.

Definiamo sui razionali p-interi una mappa di riduzione modulo p

$$r_p : \{r \in \mathbb{Q} : |r|_p \leq 1\} \to \mathbb{Z}_p \qquad r_p(r) = \begin{cases} r \mod p & \text{se } |r|_p = 1, \\ 0 & \text{se } |r|_p < 1. \end{cases}$$

cioè, se $r = p^n \frac{u}{v}$ con $n \geq 0$, $\text{MCD}(p,u) = 1$, $\text{MCD}(p,v) = 1$, allora

$$r_p(r) = \begin{cases} \frac{u}{v} \mod p & \text{se } n = 0, \\ 0 & \text{se } n > 0. \end{cases}$$

La mappa di riduzione r_p è ben definita, perché $\mathbb{Z}_p$ è un campo, ed è un omomorfismo di anelli, infatti: se $r = p^n \frac{u}{v}$ e $s = p^m \frac{z}{w}$ con u, v, z, w coprimi con p e $m \geq n \geq 0$ allora:

$$r + s = p^n \frac{uw + p^{m-n} zv}{vw} \qquad rs = p^{n+m} \frac{uz}{vw}$$

se $m = n = 0$

$$r_p(r+s) = \frac{uw + zv}{vw} \mod p = \frac{u}{v} \mod p + \frac{z}{w} \mod p = r_p(r) + r_p(s)$$

se $m > n = 0$

$$r_p(r+s) = \frac{uw + p^{m-n} zv}{vw} \mod p = \frac{uw}{vw} \mod p = \frac{u}{v} \mod p + 0 = \\ = r_p(r) + r_p(s)$$

se $m \geq n > 0$ $\qquad r_p(r+s) = 0 = 0 + 0 = r_p(r) + r_p(s).$

e

se $m = n = 0$ $\qquad r_p(rs) = \frac{uz}{vw} \mod p = \frac{u}{v} \mod p \quad \frac{z}{w} \mod p = r_p(r) r_p(s),$

se $m > 0$ $\qquad r_p(rs) = 0 = r_p(r) r_p(s).$

Definizione 1.10. Se $P = (z, x, y) \in \mathbb{P}_2(\mathbb{Q})$ allora a meno di equivalenza proiettiva si possono scegliere $z, x, y \in \mathbb{Q}$ p-interi e tali che almeno uno abbia norma p-adica 1, in tal caso (z, x, y) si dice la rappresentazione p-ridotta del punto P.

Definiamo ora una mappa di riduzione modulo p sui punti del piano proiettivo:

$$r_p : \mathbb{P}_2(\mathbb{Q}) \to \mathbb{P}_2(\mathbb{Z}_p) \qquad r_p(z, x, y) = (r_p(z), r_p(x), r_p(y))$$

dove z, x, y sono p-interi e almeno una tra $|z|_p, |x|_p, |y|_p$ è 1, tale mappa è ben definita e suriettiva e può essere usata per ridurre modulo p le curve algebriche proiettive piane.

Sia $F \in \mathbb{Q}[z, x, y]$ una curva piana proiettiva, moltiplichiamo i coefficienti di F per un'opportuna potenza di p in modo che siano tutti p-interi e almeno uno con norma p-adica 1, riduciamo con la mappa r_p i nuovi coefficienti e denotiamo con $F_p \in \mathbb{Z}_p[z, x, y]$ il polinomio omogeneo risultante.

Proposizione 1.21. *Se $F \in \mathbb{Q}[z,x,y]$ è una curva piana proiettiva e $r_p : \mathbb{P}_2(\mathbb{Q}) \to \mathbb{P}_2(\mathbb{Z}_p)$ è l'omomorfismo di riduzione modulo p, allora $r_p(F(\mathbb{Q}) \subseteq F_p(\mathbb{Z}_p)$.*

Dimostrazione. Se (z,x,y) è la rappresentazione p-ridotta di un punto di $\mathbb{P}_2(\mathbb{Q})$ allora $(z,x,y) \in F(\mathbb{Q})$ se e solo se $F(z,x,y) = 0$, in tal caso

$$r_p(F(z,x,y)) = F_p(r_p(z), r_p(x), r_p(y)) = F_p(r_p(z,x,y)) = 0$$

e $r_p(z,x,y) \in F_p(\mathbb{Z}_p)$. □

Capitolo 2

Curve Ellittiche

Sia E una cubica non singolare su $\mathbb{K}$, campo algebricamente chiuso, per la proposizione 1.5 E ha almeno un punto di flesso su $\mathbb{K}$ e dunque per la proposizione 1.6 E può essere messa in forma di Weierstrass (ridotta se la caratteristica di $\mathbb{K}$ non è 2 o 3).

Se $\mathbb{K}$ non è algebricamente chiuso e $F(z,x,y) \in \mathbb{K}[z,x,y]$ definisce una cubica non singolare tale che $F(\mathbb{K}) \neq \emptyset$ può accadere che F non abbia punti di flesso in $F(\mathbb{K})$. A questo proposito consideriamo il seguente esempio: sia $\mathscr{C}$ la curva proiettiva definita da

$$F(z,x,y) = z^3 + 2x^3 + 3y^3 \quad \in \mathbb{Q}[z,x,y]$$

vogliamo mostrare che $\mathscr{C}$ è una cubica liscia con un punto razionale e senza flessi razionali. Verifichiamo che si tratta di una cubica liscia (e dunque irriducibile):

$$\begin{cases} \frac{\partial F}{\partial z}(z,x,y) = 3z^2 = 0 \\ \frac{\partial F}{\partial x}(z,x,y) = 6x^2 = 0 \\ \frac{\partial F}{\partial y}(z,x,y) = 9y^2 = 0 \end{cases} \iff \begin{pmatrix} z \\ x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Calcoliamo la curva hessiana di $\mathscr{C}$:

$$\mathscr{H} = \det \begin{pmatrix} 6z & 0 & 0 \\ 0 & 12x & 0 \\ 0 & 0 & 18y \end{pmatrix} = 1296zxy$$

Allora i punti di flesso di $\mathscr{C}$ sono i punti di intersezione di $\mathscr{C}$ con l'hessiana $\mathscr{H}$:

$$\begin{cases} zxy = 0 \\ z^3 + 2x^3 + 3y^3 = 0 \end{cases}$$

e sono:

$$\begin{pmatrix} 0 \\ 1 \\ -\sqrt[3]{\frac{2}{3}} \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -\sqrt[3]{\frac{2}{3}}(\frac{-1+\sqrt{3}i}{2}) \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -\sqrt[3]{\frac{2}{3}}(\frac{-1-\sqrt{3}i}{2}) \end{pmatrix}$$
$$\begin{pmatrix} -\sqrt[3]{3} \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -\sqrt[3]{3}(\frac{-1+\sqrt{3}i}{2}) \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -\sqrt[3]{3}(\frac{-1-\sqrt{3}i}{2}) \\ 0 \\ 1 \end{pmatrix}$$
$$\begin{pmatrix} -\sqrt[3]{2} \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -\sqrt[3]{2}(\frac{-1+\sqrt{3}i}{2}) \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -\sqrt[3]{2}(\frac{-1-\sqrt{3}i}{2}) \\ 1 \\ 0 \end{pmatrix}$$

osserviamo che nessun punto di flesso di $\mathscr{C}$ è razionale.

Osserviamo anche che $P = \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}$ è un punto razionale che soddisfa l'equazione $z^3 + 2x^3 + 3y^3 = 0$, dunque $\mathscr{C}$ è una cubica liscia su $\mathbb{Q}$ con un punto razionale, ma non può essere messa in forma di Weierstrass su $\mathbb{Q}$, perché priva di punti di flesso su $\mathbb{Q}$.

Definizione 2.1. Diciamo curva ellittica una cubica non singolare con un punto razionale definita da un'equazione in forma di Weierstrass.

Le curve ellittiche sono cubiche non singolari con un punto razionale e dunque ammettono la struttura di gruppo indotta dalla somma di Poincaré. Vogliamo studiare le operazioni di gruppo per le curve ellittiche con equazione in forma di Weierstrass, completa e ridotta, e trovare espressioni esplicite in termini delle coordinate dei punti.

Sia E una curva ellittica con equazione in forma di Weierstrass, scegliamo come elemento neutro per la somma di Poincaré il punto all'infinito $O = (0, 0, 1)$, che è un punto di flesso. Osserviamo che le rette passanti per O sono la retta all'infinito e le rette verticali del riferimento affine (x, y) associato alle coordinate proiettive (z, x, y).
Se E ha equazione (1.2) e $P = (x_0, y_0) \in E(\mathbb{K})$ la retta $O \vee P$ ha equazione $x = x_0$ e interseca la cubica in due punti, P e $P \cdot O$, aventi la stessa ascissa x_0; per trovare l'ordinata di $P \cdot O$ considero l'equazione di secondo grado che si ottiene sostituendo x_0 a x nell'equazione della curva:

$$y^2 + (a_1x_0 + a_3)y = x_0^3 + a_2x_0^2 + a_4x_0 + a_6$$

risolvendo si ottiene

$$y_0 = \frac{-(a_1x_0 + a_3) + \delta}{2} \qquad \Rightarrow \qquad \delta = 2y_0 + a_1x_0 + a_3$$

l'ordinata di $P \cdot O$ è data da

$$y = \frac{-(a_1 x_0 + a_3) - \delta}{2} = -y_0 - a_1 x_0 - a_3$$

quindi $P \cdot O = (x_0, -y_0 - a_1 x_0 - a_3)$.

O è un punto di flesso per E, quindi $O \cdot O = O$ e se $P = (x_0, y_0) \in F(\mathbb{K})$ si ha $-P = P \cdot (O \cdot O) = P \cdot O$, dunque

$$-P = (x_0, -y_0 - a_1 x_0 - a_3).$$

In particolare, se $a_1 = a_3 = 0$ (se la caratteristica del campo è diversa da 2 considerando la curva in forma di Weierstrass (1.3)) allora

$$-P = (x_0, -y_0).$$

Se $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(\mathbb{K})$ e $P_1 \neq P_2$, sia $y = mx + b$ la retta passante per P_1 e P_2:

$$m = \frac{y_2 - y_1}{x_2 - x_1} \qquad b = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1} \tag{2.1}$$

sia $P_3 = P_1 + P_2 = O \cdot (P_1 \cdot P_2) = -P_1 \cdot P_2$, se $P_3 = (x_3, y_3)$ allora siccome l'ascissa di $-P_1 \cdot P_2$ è uguale a quella di $P_1 \cdot P_2$ e $P_1, P_2, P_1 \cdot P_2$ sono i punti di intersezione di $y = mx + b$ con la cubica:

$$\begin{cases} y = mx + b \\ E(x, y) = 0 \end{cases}$$

dove $E(x, y) = -(y^2 + a_1 xy + a_3 y) + x^3 + a_2 x^2 + a_4 x + a_6$ si ha che x_1, x_2, x_3 sono le radici di $E(x, mx + b)$ e dunque da

$$\begin{aligned} E(x, mx + b) &= x^3 + (a_2 - m^2 - a_1 m)x^2 + \dots \\ &= (x - x_1)(x - x_2)(x - x_3) = x^3 - (x_1 + x_2 + x_3)x^2 + \dots \end{aligned}$$

si ottiene

$$x_3 = -x_1 - x_2 - a_2 + m^2 + a_1 m \tag{2.2}$$

e

$$y_3 = -(mx_3 + b) - a_1 x_3 - a_3 = -(m + a_1)x_3 - a_3 - b \tag{2.3}$$

Se $P_1 = P_2 = P = (x_0, y_0)$ sia $y = mx + b$ la retta tangente a E in P:

$$m = \frac{3x_0^2 + 2a_2 x_0 + a_4 - a_1 y_0}{2y_0 + a_1 x_0 + a_3} \qquad b = \frac{-x_0^3 + a_4 x_0 + 2a_6 - a_3 y_0}{2y_0 + a_1 x_0 + a_3} \tag{2.4}$$

Le coordinate di $2P = P + P$ sono

$$\begin{aligned} x_{2P} &= -2x_0 - a_2 + m^2 + a_1 m = \frac{x_0^4 - b_4 x_0^2 - 2b_6 x_0 - b_8}{4x_0^3 + b_2 x_0^2 + 2b_4 x_0 + b_6} \\ y_{2P} &= -(m + a_1)x_{2P} - a_3 - b \end{aligned} \tag{2.5}$$

Teorema 2.1. *Sia E una curva ellittica su un campo $\mathbb{K}$ di caratteristica diversa da 2 o 3. Supponiamo E sia definita dall'equazione $y^2 = (x-\alpha)(x-\beta)(x-\gamma) = x^3+rx^2+sx+t = f(x)$ con $\alpha, \beta, \gamma \in \mathbb{K}$. Allora $(x_2, y_2) \in 2E(\mathbb{K})$ se e solo se $x_2 - \alpha, x_2 - \beta, x_2 - \gamma$ sono quadrati in $\mathbb{K}$.*

Dimostrazione. Supponiamo esista $(x_1, y_1) \in E(\mathbb{K})$ tale che $(x_2, y_2) = 2(x_1, y_1)$, sia $y = mx + b$ la retta tangente a E in (x_1, y_1), allora (x_1, y_1) e $(x_2, -y_2)$ soddisfano entrambe l'equazione $(x-\alpha)(x-\beta)(x-\gamma) = y^2 = (mx+b)^2$, siccome $y = mx+b$ è tangente a E in (x_1, y_1) le radici di $(x-\alpha)(x-\beta)(x-\gamma) - (mx+b)^2$ sono x_2, x_1, x_1 e dunque

$$(x-\alpha)(x-\beta)(x-\gamma) - (mx+b)^2 = (x-x_2)(x-x_1)^2. \tag{2.6}$$

Osservo che se $x_1 = \alpha$ allora $(x_1, y_1) = (x_2, y_2) = (\alpha, 0)$ è un punto di flesso e $x_2 - \alpha = 0$ è un quadrato in $\mathbb{K}$; se $x_1 \neq \alpha$ sia $x = \alpha$, allora da 2.6 si ottiene $-(m\alpha+b)^2 = (\alpha - x_2)(\alpha - x_1)^2$ e dunque che $x_2 - \alpha$ è un quadrato in $\mathbb{K}$. Analogamente si dimostra che $x_2 - \beta$ e $x_2 - \gamma$ sono dei quadrati in $\mathbb{K}$.

Viceversa, supponiamo che $x_2 - \alpha, x_2 - \beta, x_2 - \gamma$ siano dei quadrati in $\mathbb{K}$, a meno di cambio di variabili che non cambia il punto di flesso all'infinito possiamo supporre $x_2 = 0$ e dunque $y_2^2 = -\alpha\beta\gamma = t$. Per ipotesi esistono $\alpha_1, \beta_1, \gamma_1 \in \mathbb{K}$ tali che $-\alpha = \alpha_1^2, -\beta = \beta_1^2, -\gamma = \gamma_1^2$ e $y_2 = \alpha_1\beta_1\gamma_1$. Sia $y = mx + y_2$ una retta passante per $(0, y_2)$ e tangente a E in $(x_1, y_1) \neq (0, y_2)$, dunque

$$\begin{aligned} (x-\alpha)(x-\beta)(x-\gamma) - (mx+y_2)^2 &= x(x-x_1)^2 \\ x^3 + rx^2 + sx + t - (m^2x^2 + 2my_2x + y_2^2) &= x(x-x_1)^2 \\ x^2 + (r-m^2)x + s - 2my_2 &= (x-x_1)^2 \end{aligned} \tag{2.7}$$

il primo membro di (2.7) ha discriminante nullo perchè è un quadrato:

$$\begin{aligned} \Delta = (r-m^2)^2 - 4(s-2my_2) &= 0 \\ \Rightarrow \quad (r-m^2)^2 &= 4(s-2my_2) \end{aligned} \tag{2.8}$$

L'equazione (2.8) è di quarto grado in m, se ha una radice $m_0 \in \mathbb{K}$ allora

$$\begin{aligned} x_1 &= \frac{m_0^2 - r}{2} \in \mathbb{K} \\ y_1 &= -m_0x_1 - y_2 \in \mathbb{K} \end{aligned}$$

quindi $(x_1, y_1) \in E(\mathbb{K})$ e $2(x_1, y_1) = (0, y_2)$.

Basta mostrare ora che (2.8) ha una radice $m_0 \in \mathbb{K}$. Considero

$$\begin{aligned} (m^2 - r + u)^2 &= 4(s-2my_2) + u^2 + 2um^2 - 2ru \\ \Rightarrow \quad (m^2 - r + u)^2 &= 2um^2 - 8y_2m + (u^2 - 2ru + 4s) \end{aligned} \tag{2.9}$$

e cerco $u \in \mathbb{K}$ tale che il secondo membro di (2.9) sia un quadrato in m:

$$\Delta = 16y_2^2 - 2u(u^2 - 2ru + 4s) = 8y^2 - u^3 + 2ru^2 - 4su$$
$$\iff u^3 - 2ru^2 + 4su - 8y_2^2 = 0$$

sia $u = -2v$ allora

$$-8v^3 - 8rv^2 - 8su - 8y_2^2 = 0$$
$$\iff v^3 + rv^2 + su + y_2^2 = 0$$

ma $y_2^2 = t$ dunque

$$v^2 + rv^2 + su + t = 0$$

ha tre soluzioni: α, β, γ. Sia $u = -2\alpha$, allora sostituendo in (2.9) si ottiene:

$$(m^2 - r - 2\alpha)^2 = -4\alpha m^2 - 8y_2 m + (4\alpha^2 + 4r\alpha + 4s)$$

ma $r = -(\alpha + \beta + \gamma)$ e $s = \alpha\beta + \alpha\gamma + \beta\gamma$ dunque

$$(m^2 + \alpha + \beta + \gamma - 2\alpha)^2 = -4\alpha m^2 - 8y_2 m + (4\alpha^2 - 4\alpha(\alpha + \beta + \gamma) + 4(\alpha\beta + \alpha\gamma + \beta\gamma)$$
$$(m^2 - \alpha + \beta + \gamma)^2 = -4\alpha m^2 - 8y_2 m + 4\beta\gamma$$

sostituendo $-\alpha = \alpha_1^2, -\beta = \beta_1^2, -\gamma = \gamma_1^2$ e $y_2 = \alpha_1\beta_1\gamma_1$ si ottiene

$$(m^2 - \alpha + \beta + \gamma)^2 = 4(\alpha_1 m - \beta_1\gamma_1)^2$$
$$\Rightarrow \quad m^2 - \alpha + \beta + \gamma = \pm 2(\alpha_1 m - \beta_1\gamma_1)$$
$$\Rightarrow \quad m^2 \mp 2\alpha_1 m + \alpha_1^2 = \beta_1^2 \pm 2\beta_1\gamma_1 + \gamma_1^2$$
$$\Rightarrow (m \mp \alpha_1)^2 = (\beta_1 \pm \gamma_1)^2$$

Dunque

$$m = \pm\alpha_1 + \beta_1 \pm \gamma_1 \in \mathbb{K}$$
$$m = \pm\alpha_1 - \beta_1 \mp \gamma_1 \in \mathbb{K}$$

sono le soluzioni di (2.8).

□

Definizione 2.2. Se E è una curva ellittica di equazione in forma di Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

e

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

è il discriminante di E definito in (1.7), si definisce l'invariante j della curva ellittica E

$$j = \frac{c_4^3}{\Delta}.$$

con c_4 definito da (1.6).

Osservazione. L'invariante j per una curva ellittica E è ben definito perché E è una cubica non singolare e dunque, per la proposizione 1.8, $\Delta \neq 0$. Inoltre se la caratteristica di $\mathbb{K}$ non è 2 o 3, j è invariante per trasformazioni (1.8) che conservano la forma di Weierstrass, infatti abbiamo già visto, alla fine del paragrafo 1.2, che sotto tali condizioni sulla caratteristica di $\mathbb{K}$ c_4 e Δ non dipendono dai parametri r, s, t delle trasformazioni (1.8), mentre per quanto riguarda il parametro u delle stesse trasformazioni c_4 ha peso 4 e Δ ha peso 12, dunque $j = \frac{c_4^3}{\Delta}$ ha peso 0.

Proposizione 2.2. *Se $\mathbb{K}$ ha caratteristica diversa da 2 o 3, allora*

(i) se due curve ellittiche sono legate da un cambio di variabili che mantiene la forma di Weierstrass (1.8), allora hanno lo stesso invariante j;

(ii) se $j_0 \in \mathbb{K}$ esiste una curva ellittica su $\mathbb{K}$ con invariante $j = j_0$;

(iii) se $\mathbb{K}$ è algebricamente chiuso e due curve ellittiche hanno lo stesso invariante j allora sono legate da un cambio di variabili del tipo (1.8).

Per la dimostrazione si veda [K], III, §2, Proposizione 3.7.

Dunque su un campo algebricamente chiuso due cubiche non singolari in forma di Weierstrass hanno lo stesso invariante j se e solo se si possono ottenere una dall'altra mediante un cambio di variabili che conserva la forma di Weierstrass.

Esempio 1. *Consideriamo le curve ellittiche di equazione $y^2 = x^3 + px + q$, se la caratteristica del campo $\mathbb{K}$ è diversa da 2 e 3, allora con le formule (1.4) e (1.6) calcoliamo*

$$a_1 = a_2 = a_3 = 0, \quad a_4 = p, \quad a_6 = q$$
$$b_2 = a_1^2 + 4a_2 = 0, \quad b_4 = 2a_4 + a_1a_3 = 2p, \quad b_6 = a_3^2 + 4a_6 = 4q$$
$$c_4 = b_2^2 - 24b_4 = -48p = -2^3 3p, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6 = -864q = -2^5 3^3 q$$
$$\Delta = \frac{c_4^3 - c_6^2}{1728} = \frac{-2^{12}3^3p^3 - 2^{10}3^6q^2}{2^6 3^3} = -2^4(4p^3 + 27q^2)$$
$$j = \frac{c_4^3}{\Delta} = \frac{-2^{12}3^3p^3}{-2^4(4p^3 + 27q^2)} = 1728\frac{4p^3}{4p^3 + 27q^2}$$

Questo esempio, oltre a fornire un'utile formula per il calcolo dell'invariante j di numerose curve ellittiche, ci permette di verificare la validità dell'uguaglianza $\Delta = 2^4 d_b$ della proposizione 1.7, essendo in questo caso $d_b = -4p^3 - 27q^2$.

Esempi 1. *Dall'esempio precedente otteniamo che tutte le curve di equazione $y^2 = x^3 + Ax$ hanno invariante $j = 1728$ e quindi sulla chiusura algebrica di $\mathbb{K}$ sono tutte equivalenti a meno di trasformazioni che conservano la forma di Weierstrass. Sarà di nostro interesse studiare le seguenti curve ellittiche:*

$y^2 = x^3 - 4x$ *cubica legata al caso quartico dell'Ultimo Teorema di Fermat,*

$y^2 = x^3 - n^2x$ *curve associate ai numeri congruenti,*

$y^2 = x^3 + 8x$ *cubica legata al problema di Fermat per Mersenne.*

Capitolo 3

Teorema di Mordell

Il teorema di Mordell afferma che, data una curva ellittica E su $\mathbb{Q}$, il gruppo dei punti razionali $E(\mathbb{Q})$ è finitamente generato.

La dimostrazione consiste nel mostrare prima che $E(\mathbb{Q})/2E(\mathbb{Q})$ è finito e quindi che $E(\mathbb{Q})$ è finitamente generato.

Per dimostrare che $E(\mathbb{Q})/2E(\mathbb{Q})$ è finito si considerano delle mappe associate ai punti di 2-torsione della curva E, ovvero alle radici del polinomio di terzo grado in x della forma di Weierstrass ridotta di E $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$, in generale tali radici α, β, γ non sono razionali, sono contenute nell'estensione algebrica $\mathbb{K} = \mathbb{Q}(\alpha, \beta, \gamma)$ di $\mathbb{Q}$. Le mappe $\varphi_\alpha, \varphi_\beta, \varphi_\gamma$ sono definite: $E(\mathbb{K})/2E(\mathbb{K}) \to \mathbb{K}^\times/\mathbb{K}^{\times 2}$. Alcuni risultati di teoria dei numeri, che sono riportati nel capitolo 1, garantiscono l'esistenza di un sottoanello $\mathcal{R}$ di $\mathbb{K}$ a fattorizzazione unica con gruppo delle unità U finitamente generato che contiene $\mathbb{Z}[\alpha, \beta, \gamma]$, se d è il discriminante del polinomio $(x-\alpha)(x-\beta)(x-\gamma)$ si dimostra che

$$\varphi_\alpha \times \varphi_\beta : E(\mathbb{K})/2E(\mathbb{K}) \to U/U^2 \oplus \sum_{\substack{p \in \mathcal{R} \\ p \text{ primo} \\ p|d}} (\mathbb{Z}_2 \oplus \mathbb{Z}_2)$$

è una mappa iniettiva ed essendo il codominio un insieme finito si ottiene che $E(\mathbb{K})/2E(\mathbb{K})$ è finito. Allora con alcune considerazioni di teoria di Galois si mostra che anche $E(\mathbb{Q})/2E(\mathbb{Q})$ lo è.

A questo punto, per dimostrare che $E(\mathbb{Q})$ è finitamente generato Mordell fa uso di un argomento *reductio ad absurdum* adattando il metodo di discesa infinita usato da Fermat per dimostrare il caso quartico del suo Ultimo Teorema, che analizzeremo nel capitolo 5. Per poter applicare il metodo di discesa infinita alle curve ellittiche è necessario disporre di una relazione d'ordine per confrontare i punti, una relazione d'ordine che abbia le stesse proprietà della relazione di $\leq$ sui numeri naturali. A tal fine Mordell definisce una funzione altezza canonica h, che si può mostrare essere una norma al quadrato, che misura il comportamento all'infinito della successione delle

potenze dei punti, per cui confrontare due punti significa confrontarne le altezze.

3.1 Altezza

Sia E una curva ellittica su $\mathbb{Q}$, scelgo un riferimento proiettivo in modo che l'equazione di E sia in forma di Weierstrass ridotta (1.5):

$$y^2 = x^3 + Ax + B \tag{3.1}$$

con $A, B \in \mathbb{Z}$.

Se $P = (x, y) \in E(\mathbb{Q})$ allora si scrive in modo unico $x = \frac{p}{q}$ con $p, q \in \mathbb{Z}$ coprimi. Si può dunque definire una prima nozione "ingenua" di altezza

$$h_0(P) = \log \max\{|p|, |q|\} \tag{3.2}$$

Osservo che $h_0(P) \geq 0$ per ogni $P \in E(\mathbb{Q})$ e si pone $h_0(O) = 0$, dove $O = (0, 1, 0)$.
Osservo anche che per ogni costante $c \in \mathbb{R}$ l'insieme $\{P \in E(\mathbb{Q}) : h_0(P) \leq c\}$ è finito.

Proposizione 3.1. *Per ogni $P \in E(\mathbb{Q})$ si ha*

$$h_0(2P) = 4h_0(P) + O(1) \tag{3.3}$$

dove $O(1)$ è limitato e indipendente dalla scelta di $P \in E(\mathbb{Q})$.

Dimostrazione. L'equazione che definisce la curva ellittica E è la (3.1):

$$y^2 = x^3 + Ax + B$$

i cui coefficienti della forma di Weierstrass sono

$$a_1 = a_2 = a_3 = 0, \quad a_4 = A, \quad a_6 = B$$

usando le formule (1.4) possiamo calcolare i corrispondenti coefficienti della forma di Weierstrass ridotta

$$b_2 = 0, \quad b_4 = 2A, \quad b_6 = 4B, \quad b_8 = -A^2$$

Supponiamo che $P = (x, y) \in E(\mathbb{Q})$ non sia un punto di 2-torsione, sia

$$x = \frac{p}{q} \quad \text{con} \quad \text{MCD}(p, q) = 1$$

e sia $2P = (x^*, y^*)$, allora

$$\begin{aligned} x^* &= \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6} = \frac{x^4 - 2Ax_2 - 8Bx + A^2}{4x^3 + 4Ax + 4B} = \\ &= \frac{x^4 - 2Ax_2 - 8Bx + A^2}{4(x^3 + Ax + B)} = \frac{p^4 - 2Ap^2q^2 - 8Bpq^3 - Aq^4}{4q(p^3 + Apq^2 + Bq^3)} \end{aligned}$$

se definiamo

$$\begin{aligned} p^* &= p^4 - 2Ap^2q^2 - 8Bpq^3 - Aq^4 \\ q^* &= 4q(p^3 + Apq^2 + Bq^3) \\ \delta = \mathrm{MCD}(p^*, q^*) \quad \text{e} \quad p^{**} &= \frac{p^*}{\delta} \qquad q^{**} = \frac{q^*}{\delta} \end{aligned}$$

abbiamo

$$x^* = \frac{p^*}{q^*} = \frac{p^{**}}{q^{**}} \quad \text{con} \quad \mathrm{MCD}(p^{**}, q^{**}) = 1$$

e

$$\begin{aligned} &\max\{|p^{**}|, |q^{**}|\} \leq \max\{|p^*|, |q^*|\} \leq \\ &\quad \leq (\max\{|p|, |q|\})^4 \max\{1 + 2|A| + 8|B| + A^2, 4(1 + |A| + |B|)\} = \\ &\quad = C_{A,B}(\max\{|p|, |q|\})^4 \end{aligned}$$

dove $C_{A,B}$ è una costante che non dipende dalla scelta del punto P, ma solo dalla curva E.

Otteniamo allora che:

$$\begin{aligned} h_0(2P) &= \log \max\{|p^{**}|, |q^{**}|\} \leq \log(C_{A,B}(\max\{|p|, |q|\})^4) = \\ &= 4 \log \max\{|p|, |q|\} + \log C_{A,B} = 4h_0(P) + \log C_{A,B} \end{aligned}$$

Il discriminante del polinomio $x^3 + Ax + B$ è $d = -4A^3 - 27B^2 \neq 0$ perché E è una cubica liscia. Calcolando il risultante tra i polinomi che definiscono p^* e q^* si ottengono le seguenti relazioni:

$$\begin{aligned} 4dq^7 &= (3p^3 - 5Apq^2 - 27q^3)q^* - 4(3p^2q + 4Aq^3)p^* \\ 4dq^7 &= -(A^2Bp^3 + (5A^4 + 32AB^2)p^2q + (26A^3B + 192B^3)pq^2 - 3(A^5 + 8A^2B^2)q^3)q^* - \\ &\quad - 4((4A^3 + 27B^2)p^3 - A^2Bp^2q + 3(A^4 + 22AB^2)pq^2 + 3(A^3B + 8B^3)q^3)p^* \end{aligned}$$

Da queste otteniamo le seguenti stime:

$$\begin{aligned} (\max\{|p|, |q|\})^7 &\leq C'_{A,B}(\max\{|p|, |q|\})^3 \max\{|p^*|, |q^*|\} \\ \Rightarrow (\max\{|p|, |q|\})^4 &\leq C'_{A,B} \max\{|p^*|, |q^*|\} \end{aligned}$$

inoltre $\delta \mid 4dq^7, 4dp^7$, ma essendo $\mathrm{MCD}(p, q) = 1$ si ha $\delta \mid 4d$ e dunque $|\delta| \leq 4|d|$ è limitato indipendentemente dalla scelta di $P \in E(\mathbb{Q})$. Quindi

$$\begin{aligned} \max\{|p^*|, |q^*|\} &\leq |\delta| \max\{|p^{**}|, |q^{**}|\} \quad \text{e} \\ (\max\{|p|, |q|\})^4 &\leq |\delta| C'_{A,B} \max\{|p^{**}|, |q^{**}|\} \end{aligned}$$

Allora

$$\begin{aligned} 4h_0(P) &= 4 \log \max\{|p|, |q|\} \leq \log \max\{|p^{**}|, |q^{**}|\} + \log(|\delta| C'_{A,B}) = \\ &= h_0(2P) + \log(|\delta| C'_{A,B}) \end{aligned}$$

Abbiamo dimostrato che

$$4h_0(P) - \log(|\delta|C'_{A,B}) \leq h_0(2P) \leq 4h_0(P) + \log C_{A,B}$$
$$\Rightarrow |h_0(2P) - 4h_0(P)| \leq \max\{\log(|\delta|C'_{A,B}), \log C_{A,B}\}$$

cioè $h_0(2P) = 4h_0(P) + O(1)$ con $O(1)$ limitato indipendentemente dalla scelta di $P \in E(\mathbb{Q})$. □

Proposizione 3.2. *Esiste un'unica funzione $h : E(\mathbb{Q}) \to \mathbb{R})$ tale che*

(i) $h(P) - h_0(P)$ sia limitata;

(ii) $h(2P) = 4h(P)$;

e risulta definita da

$$h(P) = \lim_{n \to +\infty} \frac{h_0(2^n P)}{4^n} \tag{3.4}$$

Dimostrazione. Unicità. Sia $h : E(\mathbb{Q}) \to \mathbb{R}$ una funzione che soddisfa (i) e (ii), allora per (i) esiste una costante $c \in \mathbb{R}$ che dipende solo da E tale che per ogni $P \in E(\mathbb{Q})$

$$|h(P) - h_0(P)| \leq c$$

allora $\forall n \in \mathbb{N}$ si ha

$$|4^n h(P) - h_0(2^n P)| = |h(2^n P) - h_0(2^n P)| \leq c$$

dunque

$$\left| h(P) - \frac{h_0(2^n P)}{4^n} \right| \leq \frac{c}{4^n} \qquad \forall n \in \mathbb{N}$$

passando al limite per $n \to +\infty$ si ottiene

$$h(P) = \lim_{n \to +\infty} \frac{h_0(2^n P)}{4^n}$$

Quindi se esiste una funzione che soddisfa (i) e (ii) allora è definita da (3.4), questo prova l'unicità di h.

Esistenza. Mostro che la successione $\left\{ \frac{h_0(2^n P)}{4^n} \right\}_{n \in \mathbb{N}}$ è di Cauchy in $\mathbb{R}$, quindi il limite esiste e (3.4) è ben definita.

Per la proposizione 3.1 esiste una costante $c' \in \mathbb{R}$, che dipende solo da E, tale che

$$|h_0(2P) - 4h_0(P)| \leq c' \qquad \forall P \in E(\mathbb{Q}).$$

Se $n, m \in \mathbb{N}$, $m < n$, si ha

$$\left|\frac{h_0(2^n P)}{4^n} - \frac{h_0(2^m P)}{4^m}\right| = \left|\sum_{k=m}^{n-1}\left(\frac{h_0(2^{k+1}P)}{4^k} - \frac{h_0(2^k P)}{4^k}\right)\right| \leq$$

$$\leq \sum_{k=m}^{n-1}\left|\frac{h_0(2^{k+1}P)}{4^{k+1}} - \frac{h_0(2^k P}{4^k}\right| = \sum_{k=m} n - 14^{-(k+1)}|h_0(2^{k+1}P) - 4h_0(2^k P)| \leq$$

$$\leq \sum_{k=m}^{n-1}\frac{c'}{4^{k+1}} \leq \frac{c'}{3\cdot 4^m} \quad \overset{m\to+\infty}{\to} \quad 0$$

Dunque la successione è di Cauchy e il limite è ben definito.

Prendendo $m = 0$ si ottiene

$$|h(P) - h_0(P)| \leq \frac{c'}{3} \tag{3.5}$$

e quindi vale (i). Inoltre

$$h(2P) = \lim_{n\to+\infty}\frac{h_0(2^{n+1}P)}{4^n} = 4\lim_{n\to+\infty}\frac{h_0(2^{n+1}P)}{4^{n+1}} = 4h(P)$$

anche (ii) è verificata. □

Definizione 3.1. La funzione $h : E(\mathbb{Q}) \to \mathbb{R}$ così definita si chiama altezza canonica sul gruppo dei punti razionali della curva ellittica E.

Proposizione 3.3. *Proprietà dell'altezza canonica h:*

(i) $h(P) \geq 0 \quad \forall P \in E(\mathbb{Q})$.

(ii) $\{P \in E(\mathbb{Q}) : h(P) \leq c\}$ *è finito, per ogni costante* $c \in \mathbb{R}$.

(iii) $h(P) = 0$ *se e solo se* $P \in E(\mathbb{Q})$ *è un punto di torsione.*

(iv) $h(P+Q) + h(P-Q) = 2h(P) + 2h(Q) \quad \forall P, Q \in E(\mathbb{Q})$.

Dimostrazione. (i) Chiaramente $h(P) \geq 0$, per ogni P in $E(\mathbb{Q})$ perché $h_0(P) \geq 0 \quad \forall P \in E(\mathbb{Q})$.

(ii) Osservo che per (3.5) si ha

$$\{P \in E(\mathbb{Q}) : h(P) \leq c\} \subseteq \left\{P \in E(\mathbb{Q}) : h_0(P) \leq c + \frac{c'}{3}\right\}$$

che è un insieme finito.

(iii) Se P è un punto di torsione allora $h_0(2^n P)$ assume un numero finito di valori, dunque è una successione limitata, e quindi

$$h(P) = \lim_{n\to+\infty}\frac{h_0(2^n P)}{4^n} = 0.$$

Inoltre, se P ha periodo infinito, poiché per (ii) $\{P \in E(\mathbb{Q}) : h(P) \leq 1\}$ è un insieme finito, esiste $n \in \mathbb{N}$ tale che $h(2^n P) > 1$ e dunque per il punto (ii) della proposizione 3.2

$$h(P) > \frac{1}{4^n} > 0.$$

(iv) Proviamo prima la disuguaglianza

$$h(P+Q) + h(P-Q) \leq 2h(P) + 2h(Q) \tag{3.6}$$

Poiché $h = lim_{n\to+\infty} \frac{h_0(2^n P)}{4^n}$, basta mostrare che

$$h_0(P+Q) + h_0(P-Q) \leq 2h_0(P) + 2h_0(Q) + O(1) \tag{3.7}$$

con $O(1)$ indipendente dalla scelta di $P, Q \in E(\mathbb{Q})$.
Se uno tra P e Q è il punto all'infinito la disuguaglianza è banale, se uno tra $P+Q$ e $P-Q$ è il punto all'infinito la (3.7) segue dalla proposizione 3.1.

Supponiamo dunque che nessuno tra P, Q, $P+Q$ e $P-Q$ sia il punto all'infinito, siano

$$\begin{aligned} P &= (x,y) \qquad x = \frac{p}{q} \qquad GCD(p,q) = 1 \\ Q &= (x',y') \qquad x' = \frac{p'}{q'} \qquad GCD(p',q') = 1 \end{aligned} \tag{3.8}$$

siano

$$|x|_\infty = \max\{|p|,|q|\}, \qquad |x'|_\infty = \max\{|p'|,|q'|\}$$

siccome $P \neq \pm Q$, altrimenti si ricade nei punti precedenti, usando la formula di addizione (2.2) si calcola

$$x_\pm = x(P \pm Q) = \left(\frac{y' \mp y}{x' - x}\right)^2 - (x' + x)$$

usando il fatto che le coordinate di P e Q soddisfano l'equazione (3.1) e sostituendo poi le relazioni (3.8) si calcolano

$$\begin{aligned} x_+ + x_- &= 2\frac{y'^2 + y^2 - (x'+x)(x'-x)^2}{(x'-x)^2} = \\ &= 2\frac{x'^3 + x^3 + A(x'+x) + 2B - (x'+x)(x'^2 - 2x'x + x^2)}{(x'-x)^2} = \\ &= 2\frac{xx'(x+x') + A(x'+x) + 2B}{(x'-x)^2} = \\ &= 2\frac{pp'(p'q+pq') + A(p'q+pq') + 2Bq^2q'^2}{(p'q-pq')^2} \end{aligned} \tag{3.9}$$

$$
\begin{aligned}
x_+x_- &= \left(\frac{y'^2-2y'y+y^2}{(x'-x)^2}-(x'+x)\right)\left(\frac{y'^2+2y'y+y^2}{(x'-x)^2}-(x'+x)\right)= \\
&= \left(\frac{y'^2+y^2}{(x'-x)^2}-(x'+x)\right)^2-4\frac{y'y}{(x'-x)^4}= \\
&= \frac{(y'^2-y^2)^2}{(x'-x)^4}-2\frac{y'^2+y^2}{(x'-x)^2}(x'+x)+(x'+x)^2= \\
&= \frac{(x'-x)^2(x'^2+xx'+x^2+A)^2}{(x'-x)^4}-2\left(\frac{(x+x')^2(x'^2-xx'+x^2+A)}{(x'-x)^2}+\right. \\
&\qquad \left.+2B\frac{x'+x}{(x'-x)^2}\right)+(x'+x)^2= \\
&= \frac{(A-x'x)^2-4B(x'+x)}{(x'-x)^2}= \\
&= \frac{(Aqq'-pp')^2-4Bqq'(p'q-pq')}{(p'q-pq')^2}
\end{aligned}
\tag{3.10}
$$

Scriviamo $x_+ + x_- = \frac{r}{t}$ e $x_+x_- = \frac{s}{t}$, allora

$$\max\{|r|,|s|,|t|\} \le C|x|_\infty^2|x'|_\infty^2 \tag{3.11}$$

con $C = \max\{4(1+|A|+|B|),(1+|A|)^2+8|B|,4\}$ costante positiva che non dipende dalla scelta dei punti P e Q.

Inoltre x_+ e x_- sono le radici dell'equazione

$$x^2-\frac{r}{t}x+\frac{s}{t}=0 \quad \text{cioè sono} \quad \frac{r\pm\sqrt{r^2-4st}}{2t}\in\frac{1}{2t}\mathbb{Z}$$

dunque, se

$$
\begin{aligned}
x_+ &= \frac{p_+}{q_+} \quad \text{con} \quad GCD(p_+,q_+)=1 \qquad \text{e} \\
x_- &= \frac{p_-}{q_-} \quad \text{con} \quad GCD(p_-,q_-)=1
\end{aligned}
$$

esistono $\delta_+,\delta_-\in\mathbb{Z}$ tali che

$$\delta_+q_+ = 2t \quad \text{e} \quad \delta_-q_- = 2t,$$

allora

$$\delta_+\delta_-q_+q_- = 4t^2 \tag{3.12}$$

$$
\begin{aligned}
\frac{r}{t} = x_+ + x_- = \frac{p_+}{q_+}+\frac{p_-}{q_-} &= \frac{p_+q_- + p_-q_+}{q_+q_-} = \delta_+\delta_-\frac{p_+q_- + p_-q_+}{4t^2} \\
&\Rightarrow \quad \delta_+\delta_-(p_+q_- + p_-q_+) = 4rt
\end{aligned}
\tag{3.13}
$$

$$
\begin{aligned}
\frac{s}{t} = x_+x_- &= \frac{p_+p_-}{q_+q_-} = \delta_+\delta_-\frac{p_+p_-}{4t^2} \\
&\Rightarrow \quad \delta_+\delta_-p_+p_- = 4st
\end{aligned}
\tag{3.14}
$$

Da (3.14) si deduce che $t \mid \delta_+ p_+ \delta_- p_-$. Siano p un primo e $a, b \in \mathbb{Z}$ tali che $p^{a+b} \parallel t$, $p^a \mid \delta_+ p_+$ e $p^b \mid \delta_- p_-$, allora da (3.13) si ottiene che $p^a \mid \delta_+ q_+$ e $p^b \mid \delta_- q_-$, dunque $p^a \mid GCD(\delta_+ p_+, \delta_+ q_+) = \delta_+$ e $p^b \mid GCD(\delta_- p_-, \delta_- q_-) = \delta_-$ e infine $p^{a+b} \mid \delta_+ \delta_-$. Si può ripetere il ragionamento per ogni divisore primo di t, dunque $t \mid \delta_+ \delta_-$. Considerando questo fatto e la stima (3.17), dalle equazioni (3.12),(3.13) e (3.14) si ricava che

$$|q_+ q_-| \leq 4|t|, \quad |p_+ q_- + p_- q_+| \leq 4|r| \quad \text{e} \quad |p_+ p_-| \leq 4|s|$$

e dunque

$$\begin{aligned} &\max\{|p_+|, |q_+|\} \max\{|p_-|, |q_-|\} \leq 2 \max\{|p_+ q_- + p_- q_+|, |p_+ p_-|, |q_+ q_-|\} \leq \\ &\quad \leq 8 \max\{|r|, |s|, |t|\} \leq 8C |x|_\infty^2 |x'|_\infty^2 \end{aligned}$$

applicando il logaritmo al primo e all'ultimo membro della catena di disuguaglianze si ottiene (3.7), con $O(1) = \log 8C$ indipendente dalla scelta di $P, Q \in E(\mathbb{Q})$. Così abbiamo provato (3.6). Siano ora $P' = P + Q$ e $Q' = P - Q$, allora

$$\begin{gathered} h(P' + Q') + h(P' - Q') = h(2P) + h(2Q) = 4h(P) + 4h(Q) \\ 2h(P') + 2h(Q') = 2h(P + Q) + 2h(P - Q) \end{gathered}$$

e applicando la (3.6) ai punti P' e Q' si ottiene la disuguaglianza inversa

$$2h(P) + 2h(Q) \leq h(P + Q) + h(P - Q)$$

Abbiamo così provato il punto (iv).

□

3.2 Dimostrazione

Sia E una curva ellittica su $\mathbb{Q}$ in forma di Weierstrass (1.3), sia

$$y^2 = (x - \alpha)(x - \beta)(x - \gamma) \tag{3.15}$$

l'equazione di E e sia $\mathbb{K}$ un campo di spezzamento per $f(x) = (x - \alpha)(x - \beta)(x - \gamma)$.

Proposizione 3.4. *Se E è una curva ellittica su $\mathbb{Q}$ di equazione $y^2 = f(x)$ e $\mathbb{K}$ è un campo di spezzamento di $f(x) = (x-\alpha)(x-\beta)(x-\gamma)$ su $\mathbb{Q}$, allora l'omomorfismo canonico*

$$E(\mathbb{Q})/2E(\mathbb{Q}) \to E(\mathbb{K})/2E(\mathbb{K})$$

ha $\leq 2^{2[\mathbb{K}:\mathbb{Q}]}$ elementi nel suo nucleo.

Dimostrazione. $\mathbb{K}$ è campo di spezzamento di un polinomio su $\mathbb{Q}$, che è un campo perfetto, dunque $\mathbb{K}$ è un'estensione di Galois su $\mathbb{Q}$.

Per ogni $Q = (x, y) \in E(\mathbb{K})$ e per ogni $\sigma \in Gal(\mathbb{K}|\mathbb{Q})$ sia $\sigma(Q) = (\sigma(x), \sigma(y))$, allora $\sigma(Q) \in E(\mathbb{K})$ perché l'equazione che definisce E ha i coefficienti in $\mathbb{Q}$.

Sia $E[2] = \{Q \in E(\mathbb{K}) : 2Q = 0\}$ l'insieme dei punti di 2-torsione di E su $\mathbb{K}$. Sia

$$\varphi : E(\mathbb{Q})/2E(\mathbb{Q}) \to E(\mathbb{K})/2E(\mathbb{K})$$

l'omomorfismo canonico di inclusione, allora $\ker\varphi = E(\mathbb{Q}) \cap 2E(\mathbb{K})$.

Se $P \in \ker\varphi$ allora esiste $Q_P \in E(\mathbb{K})$ tale che $P = 2Q_P$, sia

$$\lambda_P : Gal(\mathbb{K}|\mathbb{Q}) \to E[2] \qquad \lambda_P(\sigma) = \sigma(Q_P) - Q_P$$

essendo σ è un automorfismo di $\mathbb{K}$ e $P \in E(\mathbb{Q})$, si ha

$$2\lambda_P(\sigma) = 2(\sigma(Q_P) - Q_P) = \sigma(2Q_P) - 2Q_P = \sigma(P) - P = P - P = 0$$

dunque λ_P è ben definita.

Inoltre

$$\begin{aligned}
\lambda_P = \lambda_{P'} &\iff \sigma(Q_P) - Q_P = \sigma(Q_{P'}) - Q_{P'} \quad \forall\sigma \in Gal(\mathbb{K}|\mathbb{Q}) \\
&\iff \sigma(Q_P - Q_{P'}) = Q_p - Q_{P'} \quad \forall\sigma \in Gal(\mathbb{K}|\mathbb{Q}) \\
&\iff Q_P - Q_{P'} \in E(\mathbb{Q}) \\
&\iff P - P' \in 2E(\mathbb{Q})
\end{aligned}$$

Dunque

$$|\ker\varphi| = |\{\lambda_P \in E[2]^{Gal(\mathbb{K}|\mathbb{Q})} : P \in E(\mathbb{Q}) \cap 2E(\mathbb{K})\}| \leq |E[2]^{Gal(\mathbb{K}|\mathbb{Q})}| = 2^{[\mathbb{K}:\mathbb{Q}]}$$

è finito perchè $\mathbb{K}$ è un'estensione algebrica di grado finito su $\mathbb{Q}$. □

Dunque se $E(\mathbb{K})/2E(\mathbb{K})$ è finito allora anche $E(\mathbb{Q})/2E(\mathbb{Q})$ è finito.

$\mathbb{K}$ è un'estensione di $\mathbb{Q}$ di grado finito, allora, per il teorema 1.19, $\mathbb{K}$ ha un sottoanello R a ideali principali contenente l'anello degli interi algebrici e il cui gruppo delle unità è finitamente generato.

Sia $\varphi_\alpha : E(\mathbb{K}) \to \mathbb{K}^\times/\mathbb{K}^{\times 2}$ definita da

$$\varphi_\alpha(P) = \begin{cases} (x-\alpha)\mathbb{K}^{\times 2} & \text{se } P = (x,y) \notin \{\infty, (\alpha, 0)\} \\ (\alpha-\beta)(\alpha-\gamma)\mathbb{K}^{\times 2} & \text{se } P = (\alpha, 0) \\ \mathbb{K}^{\times 2} & \text{se } P = \infty \end{cases} \tag{3.16}$$

Proposizione 3.5. *φ_α è un omomorfismo di gruppi.*

Dimostrazione. Siano $P_1, P_2 \in E(\mathbb{K})$, se $P_1 + P_2 = P_3$ allora

$$\varphi_\alpha(P_1)\varphi_\alpha(P_2) = \varphi_\alpha(P_3) \quad \iff \quad \varphi_\alpha(P_1)\varphi_\alpha(P_2)\varphi_\alpha(P_3)^{-1} = \mathbb{K}^{\times 2}$$

Per la scelta della forma di Weierstrass di E e per come è definita φ_α abbiamo $\varphi_\alpha(P) = \varphi_\alpha(-P)$ e $\varphi_\alpha(P) = \varphi_\alpha(P)^{-1}$ per ogni $P \in E(\mathbb{K})$ dunque basta mostrare che se $P_1 + P_2 + P_3 = 0$ si ha $\varphi_\alpha(P_1)\varphi_\alpha(P_2)\varphi_\alpha(P_3) = \mathbb{K}^{\times 2}$.

Se uno tra P_1, P_2, P_3 è il punto all'infinito, per esempio consideriamo P_1, allora $P_2 + P_3 = 0$, dunque $\varphi_\alpha(P_2) = \varphi_\alpha(-P_3) = \varphi_\alpha(P_3)$ e

$$\varphi_\alpha(P_1)\varphi_\alpha(P_2)\varphi_\alpha(P_3) = \varphi_\alpha(P_3)^2 = \mathbb{K}^{\times 2}$$

.

Se $P_i = (x_i, y_i) \neq (\alpha, 0)$, $i = 1, 2, 3$, allora P_1, P_2, P_3 sono allineati, sia $y = mx + b$ la retta passante per P_1, P_2, P_3, allora x_1, x_2, x_3 sono le radici dell'equazione:

$$(x - \alpha)(x - \beta)(x - \gamma) = (mx + b)^2$$

quindi

$$(x - \alpha)(x - \beta)(x - \gamma) - (mx + b)^2 = (x - x_1)(x - x_2)(x - x_3)$$

valutando l'uguaglianza per $x = \alpha$ si ottiene

$$-(m\alpha + b)^2 = (\alpha - x_1)(\alpha - x_2)(\alpha - x_3)$$
$$(x_1 - \alpha)(x_2 - \alpha)(x_3 - \alpha) = (m\alpha + b)^2 \in \mathbb{K}^{\times 2}$$

e dunque $\varphi_\alpha(P_1)\varphi_\alpha(P_2)\varphi_\alpha(P_3) = \mathbb{K}^{\times 2}$.

Se uno tra P_1, P_2, P_3 è il punto $(\alpha, 0)$, per esempio consideriamo $P_1 = (\alpha, 0)$, allora $P_2, P_3 \neq (\alpha, 0)$ altrimenti si ricade nel caso in cui uno dei punti è ∞. Ragionando come sopra, se $y = mx+b$ è la retta passante per P_1, P_2, P_3 si ha

$$(x - \alpha)(x - \beta)(x - \gamma) - (mx + b)^2 = (x - \alpha)(x - x_2)(x - x_3)$$
$$\alpha = -\frac{b}{m} \quad \Rightarrow \quad mx + b = m(x - \alpha)$$
$$\Rightarrow (x - \beta)(x - \gamma) + m^2(x - \alpha) = (x - x_2)(x - x_3)$$

valutando l'uguaglianza in $x = \alpha$ si ottiene

$$(\alpha - \beta)(\alpha - \gamma) = (x_2 - \alpha)(x_3 - \alpha)$$
$$\Rightarrow \varphi_\alpha(P_1)\varphi_\alpha(P_2)\varphi_\alpha(P_3) = (\alpha - \beta)^2(\alpha - \gamma)^2\mathbb{K}^{\times 2} = \mathbb{K}^{\times 2}$$

□

Definiamo anche un'applicazione $\varphi_\beta : E(\mathbb{K}) \to \mathbb{K}^\times/\mathbb{K}^{\times 2}$:

$$\varphi_\beta(P) = \begin{cases} (x-\beta) & \text{se } P = (x,y) \neq\in \{\infty, (\beta,0)\} \\ (\beta-\alpha)(\beta-\gamma) & \text{se } P = (\beta,0) \\ \mathbb{K}^{\times 2} & \text{se } P = \infty \end{cases}$$

Con una dimostrazione analoga a quella fatta per φ_α si mostra che φ_β è un omomorfismo di gruppi. Consideriamo ora

$$\varphi_\alpha \times \varphi_\beta : E(\mathbb{K})/2E(\mathbb{K}) \to \mathbb{K}^\times/\mathbb{K}^{\times 2} \times \mathbb{K}^\times/\mathbb{K}^{\times 2}$$

Proposizione 3.6. *$\varphi_\alpha \times \varphi_\beta$ è iniettiva.*

Dimostrazione. Sia $P = (x,y) \in E(\mathbb{K})$ tale che $\varphi_\alpha \times \varphi_\beta(P) = (\mathbb{K}^{\times 2}, \mathbb{K}^{\times 2})$, cioè $\varphi_\alpha(P) = \mathbb{K}^{\times 2}$ e $\varphi_\beta(P) = \mathbb{K}^{\times 2}$, considero tre casi:

se $x \neq\in \{\alpha, \beta\}$ allora $x-\alpha, x-\beta \in \mathbb{K}^{\times 2}$, ma $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ e quindi anche $x-\gamma$ è un quadrato in $\mathbb{K}$, allora per il teorema 2.1 si ha che $P \in 2E(\mathbb{K})$;

se $x = \alpha$ allora $(\alpha-\beta)(\alpha-\gamma), \alpha-\beta \in \mathbb{K}^{\times 2}$ dunque anche $\alpha-\gamma \in \mathbb{K}^{\times 2}$, ma $\alpha-\alpha = 0 \in \mathbb{K}^{\times 2}$, allora per il teorema 2.1 si ha che $P \in 2E(\mathbb{K})$;

se $x = \beta$ allora $(\beta-\alpha)(\beta-\gamma), \beta-\alpha \in \mathbb{K}^{\times 2}$ dunque anche $\beta-\gamma \in \mathbb{K}^{\times 2}$, ma $\beta-\beta = 0 \in \mathbb{K}^{\times 2}$, allora per il teorema 2.1 si ha che $P \in 2E(\mathbb{K})$. □

Sia U il gruppo delle unità di R, allora essendo R un dominio a ideali principali e dunque a fattorizzazione unica, abbiamo:

$$\mathbb{K}^\times/\mathbb{K}^{\times 2} = U/U^2 \oplus \sum_{\substack{p\in R \\ p \text{ primo}}} \mathbb{Z}_2$$

perchè ogni elemento di $\mathbb{K}^\times/\mathbb{K}^{\times 2}$ si scrive, a meno della moltiplicazione per invertibili di R, come $p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}\mathbb{K}^{\times 2}$ con $p_i \in R$ e $a_i \in \{0,1\}$, $k \in \mathbb{N}$. Dunque:

$$(\mathbb{K}^\times/\mathbb{K}^{\times 2}) \times (\mathbb{K}^\times/\mathbb{K}^{\times 2}) = U/U^2 \oplus \sum_{\substack{p\in R \\ p \text{ primo}}} (\mathbb{Z}_2 \oplus \mathbb{Z}_2)$$

Proposizione 3.7. *L'immagine di $E(\mathbb{K})/2E(\mathbb{K})$ tramite $\varphi_\alpha \times \varphi_\beta$ è contenuta in*

$$U/U^2 \oplus \sum_{p|d} (\mathbb{Z}_2 \oplus \mathbb{Z}_2)$$

dove d è il discriminante del polinomio $f(x) = (x-\alpha)(x-\beta)(x-\gamma)$.

Dimostrazione. Sia $P \in E(\mathbb{K})$, mostriamo che se $p \nmid d$ la p-esima coordinata di $\varphi_\alpha \times \varphi_\beta(P)$ è nulla.

La p-esima coordinata di $\varphi_\alpha \times \varphi_\beta(\infty) = (\mathbb{K}^{\times 2}, \mathbb{K}^{\times 2})$ è nulla per ogni primo $p \in R$.

Sia $P = (x, y) \neq \infty$, sia $p \in R$ un primo e siano $a, b, c \in \mathbb{Z}$ tali che

$$p^a \| (x - \alpha) \qquad p^b \| (x - \beta) \qquad p^c \| (x - \gamma)^1$$

Allora $p^{a+b+c} \| (x-\alpha)(x-\beta)(x-\gamma) = y^2 \in \mathbb{K}^2$ e $a + b + c \equiv 0 \mod 2$.

Osservo che α, β, γ sono interi algebrici di $\mathbb{K}$ perché sono gli zeri di un polinomio monico a coefficienti in $\mathbb{Z}$, dunque $\alpha, \beta, \gamma \in R$, mentre $x \in \mathbb{K}$, che è il campo dei quozienti di R.

Supponiamo che uno tra a, b, c sia negativo, per esempio a, ciò equivale a dire che $p^a \in \mathbb{K} \setminus R$, allora $p^a \| (x - \alpha)$ se e solo se $p^{|a|}$ divide esattamente il denominatore di x, in tal caso $p^a \| (x - \beta), (x - \gamma)$ e dunque $a = b = c \equiv 0 \mod 2$. Abbiamo mostrato che se $a < 0$ allora p^a è un quadrato. Analogamente se $b < 0$ o $c < 0$. Quindi se uno tra a, b, c è negativo la p-esima coordinata di $\varphi_\alpha \times \varphi_\beta(P)$ è nulla.

Siano $a, b, c \geq 0$ e suppniamo che $p \nmid d$, dove $d = (\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2$ è i discriminante di $(x - \alpha)(x - \beta)(x - \gamma)$.

Se $a > 0$ allora $p^a \| (x - \alpha)$, inoltre $x - \beta = (x - \alpha) + (\alpha - \beta)$ e $p \nmid d$ quindi $p \nmid (x - \beta)$, analogamente si vede che $p \nmid (x - \gamma)$. Abbiamo dunque $b = c = 0$ e $a \equiv 0 \mod 2$. Analogamente se $b > 0$ o $c > 0$. Dunque se $p \nmid d$ allora $a \equiv b \equiv c \equiv 0 \mod 2$.

Se $x \neq \alpha, \beta$ allora $\varphi_\alpha \times \varphi_\beta(P) = ((x - \alpha)\mathbb{K}^{\times 2}, (x - \beta)\mathbb{K}^{\times 2})$, dunque se $p \nmid d$ la p-esima coordinata di $\varphi_\alpha \times \varphi_\beta(P)$ è nulla.

Se $x = \alpha$, allora $\varphi_\alpha \times \varphi_\beta(P) = ((\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)\mathbb{K}^{\times 2}, (\alpha - \beta)\mathbb{K}^{\times 2})$, dunque se $p \nmid d$ la p-esima coordinata di $\varphi_\alpha \times \varphi_\beta(P)$ è nulla. Analogamente se $x = \beta$.

Tutti i ragionamenti sono stati fatti usando la proprietà di fattorizzazione unica degli elementi di R, e dunque a meno del prodotto per invertibili di R. Abbiamo così mostrato che $\varphi_\alpha \times \varphi_\beta(E(\mathbb{K})/2E(\mathbb{K})) \subseteq U/U^2 \oplus \sum_{p|d}(\mathbb{Z}_2 \oplus \mathbb{Z}_2)$. □

Osserviamo ora che $U/U^2 \oplus \sum_{p|d}(\mathbb{Z}_2 \oplus \mathbb{Z}_2)$ è un gruppo finito, infatti: U è un gruppo abeliano finitamente generato, dunque somma diretta di un numero finito, sia n, di gruppi ciclici e dunque U/U^2 ha 2^n elementi, inoltre $\sum_{p|d}(\mathbb{Z}_2 \oplus \mathbb{Z}_2)$ è finito perché è finito il numero di fattori primi distinti di d.

Abbiamo mostrato che $\varphi_\alpha \times \varphi_\beta : E(\mathbb{K})/2E(\mathbb{K}) \to U/U^2 \oplus \sum_{p|d}(\mathbb{Z}_2 \oplus \mathbb{Z}_2)$ è una mappa iniettiva con codominio finito, dunque $E(\mathbb{K})/2E(\mathbb{K})$ è finito. Ma allora per la proposizione 3.4 anche $E(\mathbb{Q})/2E(\mathbb{Q})$ è finito.

Teorema 3.8 (Mordell)**.** *Se E è una curva ellittica su $\mathbb{Q}$ allora il gruppo abeliano $E(\mathbb{Q})$ è finitamente generato.*

[1] La scrittura $p^k \| a$, p^k divide esattamente a, significa che $p^k \mid a$ e $p^{k+1} \nmid a$

Dimostrazione. Per quanto visto sopra $E(\mathbb{Q}/2E(\mathbb{Q})$ è finito, dunque esiste una costante $c > 0$ tale che l'insieme

$$S = \{P \in E(\mathbb{Q}) : h(P) \leq c\}$$

contenga un rappresentante per ogni classe laterale di $E(\mathbb{Q})/2E(\mathbb{Q})$. Mostriamo che S genera $E(\mathbb{Q})$.

Supponiamo per assurdo che non sia vero, allora $E(\mathbb{Q}) \setminus \langle S \rangle \neq \emptyset$. Per il punto (ii) della proposizione 3.3 l'insieme

$$\{P' \in E(\mathbb{Q}) : h(P') < c'\}$$

è finito per ogni costante $c' \in \mathbb{R}$, dunque esiste $P \in E(\mathbb{Q}) \setminus \langle S \rangle$ tale che $h(P)$ sia minima tra i punti di $E(\mathbb{Q}) \setminus \langle S \rangle$. Per le ipotesi fatte sull'insieme S, esiste $Q \in S$ tale che $P - Q = 2R \in 2E(\mathbb{Q})$, con $R \in E(\mathbb{Q})$.

Nella proposizione 3.3 abbiamo dimostrato che

$$h(P + Q) + h(P - Q) = 2h(P) + 2h(Q)$$

dunque vale una delle seguenti disuguaglianze:

$$h(P + Q) \leq h(P) + h(Q)$$
$$h(P - Q) \leq h(P) + h(Q)$$

Sia $* = +$ oppure $* = -$ in modo che $h(P * Q) \leq h(P) + h(Q)$. Abbiamo che $P - Q = 2R$ e $P + Q = 2(Q + R)$, quindi possiamo scrivere $P * Q = 2P'$, con $P' \in E(\mathbb{Q})$. Allora, usando il fatto che $h(P) > c$ perché $P \notin S$, otteniamo

$$4h(P') = h(2P') = h(P * Q) \leq h(P) + h(Q) \leq h(P) + c < 2h(P) \leq 4h(P)$$

e dunque $h(P') < h(P)$, allora per la minimalità di $h(P)$ dev'essere $P' \in S$, ma se così fosse otterremmo $P = 2P' - (*Q) \in \langle S \rangle$ contro il fatto che abbiamo preso $P \in E(\mathbb{Q}) \setminus \langle S \rangle$. Dunque $E(\mathbb{Q}) = \langle S \rangle$ è generato da un insieme finito, abbiamo dimostrato che $E(\mathbb{Q})$ è finitamente generato. □

Il teorema di Mordell permette di concludere che il gruppo dei punti razionali di una curva ellittica E è un gruppo abeliano finitamente generato e quindi un prodotto finito di gruppi ciclici, possiamo scrivere

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus F$$

dove $\mathbb{Z}^r$ è la parte libera e r si dice il rango di E, mentre F è il sottogruppo di torsione.

3.3 Stime sul rango

Sia E una curva ellittica su $\mathbb{Q}$ di equazione $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ con $\alpha, \beta, \gamma \in \mathbb{Z}$ e sia d il discriminante del polinomio $(x-\alpha)(x-\beta)(x-\gamma)$. Per la proposizione 3.7 abbiamo che

$$\varphi_\alpha \times \varphi_\beta(E(\mathbb{Q})/2E(\mathbb{Q})) \subseteq \sum_{\pm, p|d} \oplus(\mathbb{Z}_2 \oplus \mathbb{Z}_2)$$

e $\varphi_\alpha \times \varphi_\beta$ è iniettiva, dunque

$$\mathrm{card}(E(\mathbb{Q})/2E(\mathbb{Q})) \leq 2^s$$

con $s = 2 + 2\,\mathrm{card}\{p \text{ primo} : p \mid d\}$.

Facendo riferimento a [C], II, §3 per quanto riguarda la teoria delle curve polari, facciamo ora alcune considerazioni sui punti di torsione di $E(\mathbb{C})$.

Definizione 3.2. Se $F \in \mathbb{C}[z,x,y]$ è una curva proiettiva piana di grado d e $Q = (q_z, q_x, q_y) \in \mathbb{P}^2(\mathbb{C})$ diciamo curva polare di F rispetto a Q la curva definita dal polinomio omogeneo di grado $d-1$

$$p_Q(z,x,y) = q_z \frac{\partial F}{\partial z}(z,x,y) + q_x \frac{\partial F}{\partial x}(z,x,y) + q_y \frac{\partial F}{\partial y}(z,x,y)$$

Teorema 3.9 (Teorema fondamentale delle curve polari)**.** *Data una curva piana $\mathscr{C}$ su $\mathbb{C}$ che sia senza componenti multiple o lineari, allora l'intersezione di $\mathscr{C}$ con la sua polare rispetto ad un punto $Q \in \mathbb{P}^2(\mathbb{C})$ consiste dei punti singolari di $\mathbb{C}$ e dei punti di tangenza con $\mathscr{C}$ delle rette per Q tangenti a $\mathscr{C}$.*

Per la dimostrazione si veda [C], II,§3, Teorema 3.2.
E è una curva ellittica, in particolare è una curva liscia di grado 3, dunque soddisfa le ipotesi del teorema fondamentale delle curve polari. Per come è stata definita la somma di Poincaré, in termini di rette secanti e tangenti, i punti di 2-torsione di $E(\mathbb{C})$ sono dati dall'intersezione di E con la polare rispetto al punto $O = (0,0,1)$, l'elemento neutro del gruppo, sono $(0,0,1), (1,\alpha,0), (1,\beta,0), (1,\gamma,0) \in E(\mathbb{Q})$ e formano un sottogruppo di $E(\mathbb{Q})$ isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Se $Q \neq (0,0,1)$ è un punto di 2-torsione, la polare di E rispetto a Q interseca E in Q, con molteplicità 2, e in $(0,0,1)$, con molteplicità 4.

Mostriamo che gli unici punti di 2^n-torsione di $E(\mathbb{C})$ sono i punti di 2-torsione. Infatti se $P \in E(\mathbb{C})$ è un punto di 4-torsione allora $Q = 2P$ è un punto di 2-torsione dunque la polare di E rispetto a Q passa per P e, per quanto visto sopra, $P \in \{Q, (0,0,1)\}$, dunque P è un punto di 2-torsione. Con un ragionamento induttivo si vede subito che se $P \in E(\mathbb{C})$ è un punto di 2^n-torsione con $n \geq 2$, allora P è un punto di 2-torsione.

Abbiamo dunque che $F \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus G$ con G gruppo di ordine dispari. Sia $\mu : F \to 2F$ definita da $\mu(P) = 2P$, $\ker(\mu) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ dunque $2F \cong G$ e $F/2F \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Per il teorema di Mordell $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus F$. Abbiamo

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}^r \oplus F)/(2\mathbb{Z}^r \oplus 2F) \cong \mathbb{Z}^r/2\mathbb{Z}^r \oplus F/2F$$

abbiamo mostrato che $F/2F$ è il sottogruppo dei punti di 2-torsione, $F/2F \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, dunque $\mathrm{card}(F/2F) = 2^2$, inoltre $\mathrm{card}(\mathbb{Z}^r/2\mathbb{Z}^r) = 2^r$, quindi $\mathrm{card}(E(\mathbb{Q})/2E(\mathbb{Q})) = 2^{r+2}$ e abbiamo la prima stima sul rango:

$$\begin{aligned} r + 2 \leq s = 2 + 2\,\mathrm{card}\{p \text{ primo} : p \mid d\} \\ \Rightarrow \quad r \leq 2\,\mathrm{card}\{p \text{ primo} : p \mid d\} \end{aligned} \tag{3.17}$$

Diciamo che un primo p è **buono** se $p \nmid d$, è **alquanto cattivo** se p divide esattamente uno tra $\alpha - \beta, \alpha - \gamma, \beta - \gamma$, è **molto cattivo** se $p \mid \alpha - \beta, \alpha - \gamma, \beta - \gamma$. Si vede facilmente che se p divide due tra $\alpha - \beta, \alpha - \gamma$ e $\beta - \gamma$ allora divide anche il terzo: se, per esempio, $p \mid \alpha - \beta, \alpha - \gamma$ allora $p \mid (\alpha - \gamma) - (\alpha - \beta) = \beta - \gamma$. Chiamiamo n_1 il numero dei primi abbastanza cattivi e n_2 il numero dei primi molto cattivi.

Proposizione 3.10. *Sia E una curva ellittica di equazione*

$$y^2 = (x - \alpha)(x - \beta)(x - \gamma)$$

con $\alpha, \beta, \gamma \in \mathbb{Z}$ e $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus F$, allora $r \leq n_1 + 2n_2 - 1$.

Dimostrazione. Dalle proposizioni 3.6 e 3.7 abbiamo che

$$\varphi_\alpha \times \varphi_\beta : E(\mathbb{Q})/2E(\mathbb{Q}) \to \sum_{\pm, p \mid d} \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_2)$$

è un morfismo iniettivo. Mostriamo che sulle coordinate $\pm$ e p **alquanto cattivi** l'immagine di $E(\mathbb{Q})/2E(\mathbb{Q})$ tramite $\varphi_\alpha \times \varphi_\beta$ sta in un sottogruppo $\mathbb{Z}_2$ di $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Consideriamo la coordinata $\pm$. Supponiamo, a meno di cambiare i nomi, che $\alpha < \beta < \gamma$ e quindi $x - \alpha > x - \beta > x - \gamma$.
Sia $P = (x, y) \in E(\mathbb{Q})$, poiché $(x - \alpha)(x - \beta)(x - \gamma) = y^2 > 0$ le possibili combinazioni di segni per $x - \alpha, x - \beta, x - \gamma$ sono $+++$ oppure $+--$ dunque:

se $x \neq \alpha$ la coordinata $\pm$ dell'immagine di P è $(\varphi_\alpha \times \varphi_\beta(P))_\pm = ((x - \alpha)\mathbb{Q}^{\times 2} \times (x - \beta)\mathbb{Q}^{\times 2})_\pm \in \{(+,+), (+,-)\} \cong \mathbb{Z}_2$;

se $x = \alpha$ allora $\varphi_\alpha(P) = (\alpha-\beta)(\alpha-\gamma)\mathbb{Q}^{\times 2} > 0$ dunque come sopra si ha $(\varphi_\alpha \times \varphi_\beta(P))_\pm \in \{(+,+),(+,-)\} \cong \mathbb{Z}_2$.

Consideriamo ora la p-esima coordinata, con p **alquanto cattivo**. Supponiamo che $p \mid \alpha-\beta$, dunque $p \nmid \alpha-\gamma, \beta-\gamma$.
Sia $P = (x,y) \in E(\mathbb{Q})$ con $x \notin \{\alpha,\beta,\gamma\}$. Siano $a,b,c \in \mathbb{Z}$ tali che $p^a \| x-\alpha, p^b \| x-\beta, p^c \| x-\gamma$, allora $p^{a+b+c} \| (x-\alpha)(x-\beta)(x-\gamma) = y^2$ che è un quadrato, dunque $a+b+c \equiv 0 \mod 2$. Abbiamo già visto, dimostrando la proposizione 3.7, che se qualcuno tra a,b,c è negativo allora $a \equiv b \equiv c \equiv 0 \mod 2$, dunque $(\varphi_\alpha \times \varphi_\beta(P))_p = (a \mod 2, b \mod 2) = (0,0) \in \mathbb{Z}_2$.

Se $a > 0$ allora $p \mid x-\alpha$, ma $p \nmid \alpha-\gamma$ quindi $p \nmid (x-\alpha)+(\alpha-\gamma) = x-\gamma$ e allora $c = 0$ e $a+b \equiv 0 \mod 2$. Abbiamo $(\varphi_\alpha \times \varphi_\beta(P))_p \in \{(0,0),(1,1)\} \cong \mathbb{Z}_2$. Se $b > 0$ si procede come nel caso $a > 0$.

Se $c > 0$ allora $p \mid x-\gamma$, ma $p \nmid \alpha-\gamma, \beta-\gamma$ quindi $p \nmid (x-\gamma)-(\alpha-\gamma) = x-\alpha$ e $p \nmid (x-\gamma)-(\beta-\gamma) = x-\beta$ e allora $a = b = 0$ e $(\varphi_\alpha \times \varphi_\beta(P))_p = (0,0) \in \mathbb{Z}_2$.

Se $x = \alpha$ allora $\varphi_\alpha(P) = (\alpha-\beta)(\alpha-\gamma)\mathbb{Q}^{\times 2}$ e $\varphi_\beta(P) = (\alpha-\beta)\mathbb{Q}^{\times 2}$, poiché $p \nmid \alpha-\gamma = \frac{\varphi_\alpha(P)}{\varphi_\beta(P)}$ otteniamo che $p \mid \varphi_\alpha(P)$ se e solo se $p \mid \varphi_\beta(P)$, dunque $(\varphi_\alpha \times \varphi_\beta(P))_p \in \{(0,0),(1,1)\} \cong \mathbb{Z}_2$. Se $x = \beta$ si conclude come nel caso $x = \alpha$.
Se $x = \gamma$ allora $\varphi_\alpha(P) = (\gamma-\alpha)\mathbb{Q}^{\times 2}$ e $\varphi_\beta(P) = (\gamma-\beta)\mathbb{Q}^{\times 2}$, $p \nmid \gamma-\alpha, \gamma-\beta$ dunque $(\varphi_\alpha \times \varphi_\beta(P))_p = (0,0) \in \mathbb{Z}_2$.

Se p **alquanto cattivo** tale che $p \mid \alpha-\gamma$ oppure $p \mid \beta-\gamma$ si ragiona analogamente.

Dunque $(\varphi_\alpha \times \varphi_\beta(E(\mathbb{Q})/2E(\mathbb{Q})))_p \leq \mathbb{Z}_2$ per ogni primo p **alquanto cattivo**. Otteniamo

$$\varphi_\alpha \times \varphi_\beta(E(\mathbb{Q})/2E(\mathbb{Q})) \leq \sum_{\substack{\pm,p \text{ alquanto} \\ \text{cattivo}}} \oplus \mathbb{Z}_2 \quad \oplus \sum_{\substack{p \text{ molto} \\ \text{cattivo}}} \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_2)$$

e allora $r+2 \leq n_1+1+2n_2$, cioè $r \leq n_1+2n_2-1$. □

Proposizione 3.11. *Se p è un primo dispari e E è la curva ellittica di equazione $y^2 = x^3 - p^2x$, allora il rango r di $E(\mathbb{Q})$ soddisfa:*

$$\begin{cases} r \leq 2 & \text{se } p \equiv 1 \mod 8, \\ r = 0 & \text{se } p \equiv 3 \mod 8, \\ r \leq 1 & \text{se } p \equiv 5,7 \mod 8. \end{cases}$$

Dimostrazione. $y^2 = x^3 - p^2x = x(x-p)(x+p)$, siano $\alpha = -p, \beta = 0, \gamma = p$, abbiamo $d = (\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2 = 4p^6$, dunque 2 è un primo **alquanto cattivo**, p è un primo **molto cattivo** e tutti gli altri primi sono **buoni**.

Il sottogruppo dei punti di 2-torsione di $E(\mathbb{Q})$ è

$$E[2] = \{(-p,0),(0,0),(p,0),\infty\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

Sia $P = (x,y) \in E(\mathbb{Q}) \setminus E[2]$, poiché $x(x-p)(x+p) = y^2 > 0$ e $x+p > x > x-p$ le possibili combinazioni di segni per $x+p, x, x-p$ sono $+++$ oppure $+--$.
Per $q \in \{2,p\}$ definiamo $\varphi^q(P) = (\varphi_\alpha \times \varphi_\beta \times \varphi_\gamma(P))_q$, se $\varphi^q(P) = (a,b,c)$ allora $a+b+c \equiv 0 \mod 2$ perché $x(x-p)(x+p) = y^2$ è un quadrato. Osserviamo anche che $2 \mid x+p$ se e solo se $2 \mid x-p$, dunque $\varphi^2(P) \in \{(0,0,0),(1,0,1)\}$ e $\varphi^p(P) \in \{(0,0,0),(1,1,0),(1,0,1),(0,1,1)\}$.

Se $P = (-p,0)$ allora $\varphi_\alpha \times \varphi_\beta \times \varphi_\gamma(P) = 2p^2\mathbb{Q}^{\times 2} \times (-p)\mathbb{Q}^{\times 2} \times (-2p)\mathbb{Q}^{\times 2}$ dunque $\varphi^2(P) = (1,0,1)$ e $\varphi^p(P) = (0,1,1)$.

Se $P = (0,0)$ allora $\varphi_\alpha \times \varphi_\beta \times \varphi_\gamma(P) = p\mathbb{Q}^{\times 2} \times (-p^2)\mathbb{Q}^{\times 2} \times (-p)\mathbb{Q}^{\times 2}$ dunque $\varphi^2(P) = (0,0,0)$ e $\varphi^p(P) = (1,0,1)$.

Se $P = (p,0)$ allora $\varphi_\alpha \times \varphi_\beta \times \varphi_\gamma(P) = 2p\mathbb{Q}^{\times 2} \times p\mathbb{Q}^{\times 2} \times 2p^2\mathbb{Q}^{\times 2}$ dunque $\varphi^2(P) = (1,0,1)$ e $\varphi^p(P) = (1,1,0)$.

Sia $P = (x,y) \in E(\mathbb{Q}) \setminus E[2]$, se $\varphi^p(P) = (0,0,0)$ allora la p-esima coordinata di $\varphi_\alpha \times \varphi_\beta(P)$ è $(0,0)$, se invece $\varphi^p(P) = (a,b,c) \neq (0,0,0)$ allora esiste $Q \in E[2]$ tale che $\varphi^p(Q) = \varphi^p(P)$, ma $\varphi_\alpha, \varphi_\beta, \varphi_\gamma$ sono omomorfismi, dunque $\varphi^p(P+Q) = (0,0,0)$. Per $P+Q = (x,y)$ abbiamo le seguenti combinazioni:

$$\varphi^{\pm}(P+Q) \in \{(+,+,+),(+,-,-)\}$$
$$\varphi^2(P+Q) \in \{(0,0,0),(1,0,1)\}$$
$$\varphi^p(P+Q) = (0,0,0)$$

dunque, se con $\square$ indichiamo che il numero corrispondente è un quadrato,

$$(x+p, x, x-p) \in \{(\square,\square,\square),(2\square,\square,2\square),(\square,-\square,-\square),(2\square,-\square,-2\square)\}$$

- Se $(x+p,x,x-p) = (\square,-\square,-\square)$ allora $2p = (x+p)-(x-p) = \square + \square$. Se p dividesse il numeratore di uno dei due quadrati, allora p^2 dividerebbe i numeratori di entrambi i quadrati e si avrebbe $p^2 \mid 2p$ che è una contraddizione. Dunque i numeratori dei due quadrati sono coprimi con p, eliminando i denominatori si ottiene $\square + \square \equiv 0 \mod p$ dove questi due quadrati sono interi e coprimi con p, allora -1 è un quadrato modulo p e dunque $p \equiv 1 \mod 4$.

  Infatti $a^2 \equiv -1 \mod p \Rightarrow a^2 = -1 + pk$ *con* $k \in \mathbb{Z}, \Rightarrow a^2 \equiv -1 + pk \mod 4$*, ma* a *è dispari , perchè lo è* p*, dunque* $a \equiv 1,3 \mod 4, \Rightarrow a^2 \equiv 1 \mod 4, \Rightarrow pk \equiv 2 \mod 4$*,* p *è dispari, quindi* $p \equiv 1 \mod 4$ *oppure* $p \equiv 3 \mod 4$*, se fosse* $p \equiv 3 \mod 4, \Rightarrow 3k \equiv 2 \mod 4, \Rightarrow k \equiv 2 \mod 4, \Rightarrow 2p \equiv 2 \mod 4, \Rightarrow p \equiv 1 \mod 4$*, contro il fatto che* $p \equiv 3$

mod 4, *dunque non può accadere che* $p \equiv 3 \mod 4$ *e allora* $p \equiv 1 \mod 4$.

Quindi $p \equiv 1, 5 \mod 8$.

- Se $(x+p, x, x-p) = (2\square, \square, 2\square)$ allora $p = (x+p) - x = 2\square - \square$. Osserviamo che p divide il numeratore di x se e solo se p divide il numeratore di $x+p$ e in tal caso si avrebbe $p^2 \mid p$ che è una contraddizione. Dunque i numeratori di $2\square$ e $\square$ sono coprimi con p, eliminando i denominatori si ottiene $2\square - \square \equiv 0 \mod p$, quindi 2 è un quadrato modulo p e $p \equiv 1, 7 \mod 8$.

  Infatti $a^2 \equiv 2 \mod p \iff a^2 = 2 + pk$ *con* $k \in \mathbb{Z}, \Rightarrow a^2 \equiv 2 + pk \mod 8$, *ma* $a^2 \equiv 1 \mod 8$ *perchè a è dispari, essendo dispari p, dunque* $2 + pk \equiv 1 \mod 8 \Rightarrow p \equiv \pm 1 \mod 8$.

- Se $(x+p, x, x-p) = (2\square, -\square, -2\square)$ allora $p = x - (x-p) = 2\square - \square$ quindi $p \equiv 1, 7 \mod 8$, ma anche $p = (x+p) - x = 2\square + \square$, ragionando come sopra si osserva che i numeratori di $2\square$ e $\square$ sono coprimi con p, allora eliminando i denominatori si ottiene $2\square + \square \equiv 0 \mod p$, dunque -2 è un quadrato modulo p e abbiamo che $p \equiv 1, 3 \mod 8$.

  Infatti $a^2 \equiv -2 \mod p \iff a^2 = -2 + pk$ *con* $k \in \mathbb{Z}, \Rightarrow a^2 \equiv -2 + pk \mod 8$, *ma* $a^2 \equiv 1 \mod 8, \rightarrow -2 + pk \equiv 1 \mod 8 \Rightarrow pk \equiv 3 \mod 8 \Rightarrow p \equiv 1, 3 \mod 8$.

  Quindi in questo caso $p \equiv 1 \mod 8$.

Osserviamo che $\varphi^{\pm}(P+Q) = (+,+,+), \varphi^2(P+Q) = (0,0,0) = \varphi^p(P+Q)$ se e solo se $\varphi_\alpha \times \varphi_\beta(P+Q) = \mathbb{Q}^{\times 2} \times \mathbb{Q}^{\times 2}$ se e solo se $P + 2E(\mathbb{Q}) = Q + 2E(\mathbb{Q})$, perché $\varphi_\alpha \times \varphi_\beta : E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \times \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ è iniettiva. Dunque $\mathrm{card}(E(\mathbb{Q})/2E(\mathbb{Q}))$ si può calcolare in base ai valori assunti da $\varphi_\alpha \times \varphi_\beta(P+Q)$.

Se $p \equiv 1 \mod 8$ allora ci sono quattro possibilità per $\varphi_\alpha \times \varphi_\beta(P+Q)$: $\{(\square, \square), (2\square, \square), (\square, -\square), (2\square, -\square)\}$ dunque $\mathrm{card}(E(\mathbb{Q})/2E(\mathbb{Q})) \leq 2^2 \cdot 4 = 2^4$ e $r \leq 2$.

Se $p \equiv 3 \mod 8$ allora c'è una sola possibilità per $\varphi_\alpha \times \varphi_\beta(P+Q)$: $\{(\square, \square)\}$ dunque $\mathrm{card}(E(\mathbb{Q})/2E(\mathbb{Q})) \leq 2^2$ e $r = 0$.

Se $p \equiv 1 \mod 8$ allora ci sono due possibilità per $\varphi_\alpha \times \varphi_\beta(P+Q)$: $\{(\square, \square), (\square, -\square)\}$ dunque $\mathrm{card}(E(\mathbb{Q})/2E(\mathbb{Q})) \leq 2^2 \cdot 2 = 2^3$ e $r \leq 1$.

Se $p \equiv 7 \mod 8$ allora ci sono due possibilità per $\varphi_\alpha \times \varphi_\beta(P+Q)$: $\{(\square, \square), (2\square, \square)\}$ dunque $\mathrm{card}(E(\mathbb{Q})/2E(\mathbb{Q})) \leq 2^2 \cdot 2 = 2^3$ e $r \leq 1$. $\square$

Capitolo 4

Teoremi di Lutz e Nagell

In questo capitolo ci occuperemo dei punti di torsione delle curve ellittiche: metodi per costruirli e per determinare il sottogruppo di torsione, che indicheremo con $E(\mathbb{Q})_{\text{tors}}$, del gruppo dei punti razionali $E(\mathbb{Q})$.

4.1 Costruzione di punti con fissata torsione

Sia E una curva ellittica di equazione $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ con $\alpha, \beta, \gamma \in \mathbb{Z}$. Non è restrittivo considerare solo equazioni della forma $y^2 = x(x-\alpha)(x-\beta)$, infatti traslando il punto $(\gamma, 0)$ in $(0,0)$ con la trasformazione $x' = x - \gamma, y' = y$ si ottiene $y'^2 = x'(x' + \gamma - \alpha)(x' + \gamma - \beta)$.

Osserviamo che $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \subseteq E(\mathbb{Q})_{\text{tors}}$ perché $\alpha, \beta \in \mathbb{Z}$ dunque i punti di 2-torsione $(0,0), (\alpha, 0), (\beta, 0)$ sono razionali.

Affinché $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \subseteq E(\mathbb{Q})_{\text{tors}}$ uno dei punti di 2-torsione deve appartenere a $2E(\mathbb{Q})$, supponiamo sia $(0,0)$, non è restrittivo, a meno di permutare α, β, γ. Per la proposizione 2.1 $(0,0) \in 2E(\mathbb{Q})$ se e solo se $-\alpha$ e $-\beta$ sono dei quadrati, cioè $y^2 = x(x + r^2)(x + s^2)$ con $r, s \in \mathbb{Z}$. Se $y = mx$ è una retta passante per $(0,0)$ e tangente a E le radici di

$$x(x + r^2)(x + s^2) - y^2 = x(x + r^2)(x + s^2) - m^2x^2 = 0$$

sono $0, x_1, x_1$ dove $2(x_1, y_1) = (0,0)$, cioè $x^2(r^2 + s^2 - m^2)x + r^2s^2$ è un quadrato perfetto, ma questo accade se e solo se

$$\begin{aligned}
\Delta = (r^2 + s^2 - m^2)^2 - 4r^2s^2 = r^4 + s^4 + m^4 - 2r^2s^2 - 2r^2m^2 - 2s^2m^2 = \\
= m^4 - 2(r^2 + s^2)m^2 + (r^2 - s^2)^2 = 0 \\
\Rightarrow m^2 \in \{r^2 + s^2 \pm 2rs\} = \{(r \pm s)^2\} \Rightarrow m \in \{\pm(r+s), \pm(r-s)\} \\
\Rightarrow x_1 = \frac{m^2 - r^2 - s^2}{2} \in \{\pm rs\} \\
\Rightarrow y_1 = mx_1 \in \{\pm rs(r+s), \pm rs(r-s)\}
\end{aligned}$$

ci sono quattro punti di 4-torsione il cui quadrato è il punto $(0,0)$, gli elementi di $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ sono

$$\infty, \quad (0,0), \quad (-r^2,0), \quad (-s^2,0), \quad (rs, \pm rs(r+s)), \quad (-rs, \mp rs(r-s)).$$

Affinché $\mathbb{Z}_8 \oplus \mathbb{Z}_2 \subseteq E(\mathbb{Q})_{\text{tors}}$ possiamo ripetere il ragionamento fatto sopra supponendo che $P = (rs, rs(r+s)) \in 2E(\mathbb{Q})$, cioè $rs, rs+r^2, rs+s^2$ siano dei quadrati. Siano $r = Rr'$ e $s = Ss'$ con R, S quadrati e r', s' privi di fattori quadrati, allora rs è un quadrato se e solo se $r's'$ lo è, se e solo se $r' = s' = a$, e quindi $rs + r^2 = RSa^2 + R^2a^2$ e $rs + s^2 = RSa^2 + S^2a^2$ sono quadrati se e solo se $R + S$ è un quadrato, se e solo se $R = \alpha^2, S = \beta^2, R + S = \alpha^2 + \beta^2 = \gamma^2$, cioè α, β, γ è una terna pitagorica. Dunque $\mathbb{Z}_8 \oplus \mathbb{Z}_2 \subseteq E(\mathbb{Q})_{\text{tors}}$ se E ha equazione $y^2 = x(x - \alpha^4a^2)(x - \beta^4a^2)$ con $\alpha^2 + \beta^2 = \gamma^2$ e a è privo di fattori quadrati.

4.2 Riduzione modulo p

Sia E una curva ellittica su $\mathbb{Q}$. A meno di un opportuno cambio di variabili che conserva la forma di Weierstrass $y = u^3y', x = u^2x'$ con $u \in \mathbb{Q}$, possiamo scegliere l'equazione di E a coefficienti p-interi di cui almeno uno con norma p-adica 1, allora E_p è definita dall'equazione di E considerata con i coefficienti in $\mathbb{Z}_p$ e, se Δ è il discriminante di E, il discriminante di E_p è $\Delta_p = \Delta \mod p$. Dunque E_p è non singolare se e solo se $p \nmid \Delta$.

Proposizione 4.1. *Se E_p è non singolare allora $r_p : E(\mathbb{Q}) \to E_p(\mathbb{Z}_p)$ è un omomorfismo di gruppi.*

Dimostrazione. $r_p(0,0,1) = (0,0,1)$ dunque $r_p(O) = O_p$, inoltre $r_p(P \cdot Q) = r_p(P) \cdot r_p(Q)$, allora $r_p(P+Q) = r_p(O \cdot (P \cdot Q)) = r_p(O) \cdot (r_p(P) \cdot r_p(Q)) = O_p \cdot (r_p(P) \cdot r_p(Q)) = r_p(P) + r_p(Q)$. □

Se $p \nmid \Delta$ allora $\ker(r_p) = \{(z,x,y) \in E(\mathbb{Q}) : r_p(z,x,y) = (0,0,1)\}$, dunque se $(z,x,y) \in \ker(r_p)$ sia ha $y \neq 0$ e, a meno di equivalenza proiettiva, si può supporre $y = 1$. Osserviamo che se $(z,x,1) \in E(\mathbb{Q})$ allora $(z,x,1) \in \ker(r_p)$ se $|z|_p < 1$ e $|x|_p < 1$, dunque

$$\ker(r_p) = \{(z,x,1) \in E(\mathbb{Q}) : |z|_p < 1, |x|_p < 1\}$$

Proposizione 4.2. *Sia $(z,x,1) \in E(\mathbb{Q})$, se $|z|_p < 1$ allora $|x|_p < 1$ e $|z|_p = |x|_p^3$.*

Dimostrazione. E è una curva ellittica di equazione $y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$, se $y = 1$ si ha

$$z = -a_1xz - a_3z^2 + x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

Supponiamo che $|z|_p < 1$ e $|x|_p \geq 1$, allora usando il fatto che a_1, a_2, a_3, a_4, a_6 hanno norma p-adica ≤ 1, si hanno le seguenti disuguaglianze:

$$\begin{aligned} |-a_1xz|_p &\leq |xz|_p < |x|_p \leq |x^3|_p \\ |-a_3z^2|_p &\leq |z^2|_p < 1 \leq |x|_p \leq |x^3|_p \\ |a_2x^2z|_p &\leq |x^2z|_p < |x^2|_p \leq |x^3|_p \\ |a_4xz^2|_p &\leq |xz^2|_p < |x|_p \leq |x^3|_p \\ |a_6z^3|_p &\leq |z^3|_p < 1 \leq |x|_p \leq |x^3|_p \end{aligned}$$

dunque $\max\{|-a_1xz|_p, |-a_3z^2|_p, |x^3|_p, |a_2x^2z|_p, |a_4xz^2|_p, |a_6z^3|_p\} = |x^3|_p$ e per la disuguaglianza ultrametrica si ha

$$|z|_p = \max\{|-a_1xz|_p, |-a_3z^2|_p, |x^3|_p, |a_2x^2z|_p, |a_4xz^2|_p, |a_6z^3|_p\} = |x^3|_p \geq 1$$

contro il fatto che $|z|_p < 1$. Abbiamo dimostrato che se $|z| < 1$ allora $|x|_p < 1$.

Mostriamo ora che $|z|_p = |x^3|_p$. Abbiamo

$$x^3 = z + a_1xz + a_3z^2 - a_2x^2z - a_3xz^2 - a_6z^3$$

se $z = 0$ allora $x = 0$ e quindi $|z|_p = 0 = |x|_p^3$, se $z \neq 0$ allora

$$\begin{aligned} |a_1xz|_p &\leq |xz|_p < |z|_p \\ |a_3z^2|_p &\leq |z^2|_p < |z|_p \\ |-a_2x^2z|_p &\leq |x^2z|_p < |z|_p \\ |-a_4xz^2|_p &\leq |xz^2|_p < |z^2|_p < |z|_p \\ |-a_6z^3|_p &\leq |z^3|_p < |z|_p \end{aligned}$$

Dunque per la disuguaglianza ultrametrica $|x|_p^3 = |x^3|_p = |z|_p$. □

Per ogni numero naturale $n \geq 1$ definiamo

$$E^{(n)}(\mathbb{Q}) = \{(z, x, 1) \in E(\mathbb{Q}) : |z|_p < 1, |x|_p \leq p^{-n}\}$$

per la proposizione precedente si ha

$$E^{(n)}(\mathbb{Q}) = \{(z, x, 1) \in E(\mathbb{Q}) : |z|_p \leq p^{-3n}\}$$

In particolare $E^{(1)}(\mathbb{Q}) = \ker(r_p)$. Il filtro p-adico di $E^{(1)}(\mathbb{Q})$ è

$$E^{(1)}(\mathbb{Q}) \supseteq E^{(2)}(\mathbb{Q}) \supseteq E^{(3)}(\mathbb{Q}) \supseteq \dots$$

e si ha

$$\bigcap_{n=1}^{\infty} E^{(n)}(\mathbb{Q}) = \{(0, 0, 1)\}$$

Proposizione 4.3. *Sia E una curva ellittica di equazione $y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$ a coefficienti p-interi in $\mathbb{Q}$, se $P_1 = (z_1, x_1, 1), P_2 = (z_2, x_2, 1) \in E^{(n)}(\mathbb{Q})$ e la retta passante per P_1 e P_2 interseca E in $P_3 = (z_3, x_3, 1)$ allora $P_3 \in E^{(n)}(\mathbb{Q})$ e*

$$|x_1 + x_2 + x_3|_p \leq \begin{cases} p^{-3n} & \text{se } a_1 = 0, \\ p^{-2n} & \text{in ogni caso} \end{cases}$$

Dimostrazione. Per ogni $s, t \in \mathbb{N}$ valgono le seguenti uguaglianze:

$$\begin{aligned} x_1^s z_1^t - x_2^s z_2^t = (x_1^s - x_2^s)z_1^t + x_2^s(z_1^t - z_2^t) = \\ = (x_1 - x_2)(x_1^{s-1} + x_1^{s-2}x_2 + \cdots + x_2^{s-1})z_1^t + \\ + x_2^s(z_1 - z_2)(z_1^{t-1} + z_1^{t-2}z_2 + \cdots + z_2^{t-1}) \end{aligned}$$

$P = (z, x, 1) \in E(\mathbb{Q})$ se $z + a_1xz + a_3z^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$, supponiamo $P_1 \neq P_2$, poiché $P_1, P_2 \in E(\mathbb{Q})$ sottraendo le due corrispondenti espressioni abbiamo un'uguaglianza

$$\begin{aligned} (z_1 - z_2) + a_1(x_1z_1 - x_2z_2) + a_3(z_1^2 - z_2^2) = \\ = (x_1^3 - x_2^3) + a_2(x_1^2z_1 - x_2^2z_2) + a_4(x_1z_1^2 - x_2z_2^2) + a_6(z_1^3 - z_2^3) \end{aligned}$$

in cui ogni termine è un multiplo intero di $x_1^s z_1^t - x_2^s z_2^t$ per opportuni $s, t \in \mathbb{N}$, l'espressione sopra si può scrivere così

$$\begin{aligned} &(z_1 - z_2) + a_1((x_1 - x_2)z_1 + (z_1 - z_2)x_2) + a_3(z_1 - z_2)(z_1 + z_2) = \\ &= (x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2) + a_2((x_1 - x_2)(x_1 + x_2)z_1 + (z_1 - z_2)x_2^2) + \\ &+ a_4((x_1 - x_2)z_1^2 + (z_1 - z_2)(z_1 + z_2)x_2) + a_6(z_1 - z_2)(z_1^2 + z_1z_2 + z_2^2) \end{aligned}$$

raccogliendo $(z_1 - z_2)$ a destra e $(x_1 - x_2)$ a sinistra abbiamo

$$\begin{aligned} (z_1 - z_2)(1 + a_1x_2 + a_3(z_1 + z_2) - a_2x_2^2 - a_4(z_1 + z_2)x_2 - a_6(z_1^2 + z_1z_2 + z_2^2)) = \\ = (x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2 - a_1z_1 + a_2(x_1 + x_2)z_1 + a_4z_1^2) \end{aligned}$$

che riscriviamo più comodamente

$$(z_1 - z_2)(1 + u) = (x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2 + v)$$

Poiché $P_1, P_2 \in E^{(n)}(\mathbb{Q})$ ogni termine di u ha norma p-adica $\leq p^{-n}$ quindi $|u|_p \leq p^{-n} < 1$ e $|1 + u| = 1$, ogni termine di v ha norma p-adica $\leq p^{-3n}$ dunque $|v|_p \leq p^{-3n}$.
Se $x_1 = x_2$ allora $1 + u \neq 0$ perché $|1 + u|_p \neq 0$ e si ha necessariamente $z_1 = z_2$.

Se $P_1 \neq P_2$ allora $x_1 \neq x_2$ e la retta passante per P_1 e P_2 ha equazione $z = mx + b$ con

$$m = \frac{z_1 - z_2}{x_1 - x_2} = \frac{x_1^2 + x_1x_2 + x_2^2 + v}{1 + u}$$

e

$$|m|_p = \left|\frac{x_1^2 + x_1x_2 + x_2^2 + v}{1 + u}\right|_p = |x_1^2 + x_1x_2 + x_2^2 + v|_p \leq$$
$$\leq \max\{|x_1^2|_p, |x_1x_2|_p, |x_2^2|_p, |v|_p\} \leq p^{-2n}$$

Se $P_1 = P_2$ allora la retta tangente a E in P_1 ha equazione $z = mx + b$ con

$$m = \frac{-a_1z_1 + 3x_1^2 + 2a_2x_1z_1 + a_4z_1^2}{1 + a_1x_1 + 2a_3z_1 - a_2x_1^2 - 2a_4x_1z_1 - 3a_6z_1^2} =$$
$$= \frac{-a_1z_1 + 3x_1^2 + 2a_2x_1z_1 + a_4z_1^2}{1 + u'}$$

dove $|u'|_p < 1$, dunque $|1 + u'|_p = 1$ e

$$|m|_p = |-a_1z_1 + 3x_1^2 + 2a_2x_1z_1 + a_4z_1^2|_p \leq$$
$$\leq \max\{|-a_1z_1|_p, |3x_1^2|_p, |2a_2x_1z_1|_p, |a_4z_1^2|_p\} \leq$$
$$\leq \max\{p^{-3n}, p^{-2n}, p^{-4n}, p^{-6n}\} = p^{-2n}$$

Dunque in entrambi i casi $|b|_p = |z_1 - mx_1|_p \leq p^{-3n}$. P_1, P_2, P_3 sono i punti di intersezione di E con la retta $z = mx + b$, dunque x_1, x_2, x_3 sono le soluzioni dell'equazione

$$(mx+b)+a_1x(mx+b)+a_3(mx+b)^2 = x^3+a_2x^2(mx+b)+a_4x(mx+b)^2+a_6(mx+b)^3$$

e dell'equazione

$$0 = (x-x_1)(x-x_2)(x-x_3) = x^3-(x_1+x_2+x_3)x^2+(x_1x_2+x_1x_3+x_2x_3)x-x_1x_2x_3$$

confrontando i coefficienti delle due equazioni si ottiene

$$x_1 + x_2 + x_3 = -\frac{-a_1m - a_3m^2 + a_2b + 2a_4mb + 3a_6m^2b}{1 + a_2m + a_4m^2 + a_6m^3}$$

il denominatore ha norma p-adica 1 perché $|m|_p \leq p^{-2n} < 1$, dunque

$$|x_1 + x_2 + x_3|_p = |-a_1m - a_3m^2 + a_2b + 2a_4mb + 3a_6m^2b|_p \leq$$
$$\leq \max\{|a_1|_p p^{-2n}, p^{-3n}\} \leq \begin{cases} p^{-3n} & \text{se } a_1 = 0, \\ p^{-2n} & \text{in ogni caso.} \end{cases}$$

Inoltre $|z_3|_p = |mx_3 + b|_p \leq p^{-3n} < 1$ e se fosse $|x_3|_p > p^{-n}$ allora $|x_1|_p, |x_2|_p \leq p^{-n} < |x_3|_p$ e per la disuguaglianza ultrametrica avremmo $|x_1 + x_2 + x_3|_p = \max\{|x_1|_p, |x_2|_p, |x_3|_p\} = |x_3|_p > p^{-n} \geq p^{-2n}$ contro il fatto che $|x_1 + x_2 + x_3|_p \leq p^{-2n}$. Dunque $P_3 \in E^{(n)}(\mathbb{Q})$.

□

Proposizione 4.4. *Per ogni $n \geq 1$ $E^{(n)}(\mathbb{Q})$ è un sottogruppo di $E(\mathbb{Q})$. Sia $\mathcal{R}$ l'anello dei p-interi di $\mathbb{Q}$, allora è ben definita la mappa*

$$E^{(n)}(\mathbb{Q}) \to p^n\mathcal{R}$$
$$P = (z, x, 1) \mapsto x(P) = x$$

e la composizione di tale mappa con la proiezione $p^n\mathcal{R} \to p^n\mathcal{R}/p^{2n}\mathcal{R}$ è un omomorfismo di gruppi: $E^{(n)}(\mathbb{Q}) \to p^n\mathcal{R}/p^{2n}\mathcal{R}$ con il nucleo contenuto in $E^{(2n)}(\mathbb{Q})$. Dunque si ottiene un omomorfismo iniettivo

$$E^{(n)}(\mathbb{Q})/E^{(2n)}(\mathbb{Q}) \to p^n\mathcal{R}/p^{2n}\mathcal{R}$$

Dimostrazione. Se $P_1, P_2 \in E^{(n)}(\mathbb{Q})$ per la proposizione 4.3 anche $P_3 = P_1 \cdot P_2 \in E^{(n)}(\mathbb{Q})$, ma $O \in E^{(n)}(\mathbb{Q}) \quad \forall n \geq 1$, applicando ancora la proposizione 4.3 abbiamo che $P_1 + P_2 = O \cdot P_3 \in E^{(n)}(\mathbb{Q})$ e $-P_1 = O \cdot P_1 \in E^{(n)}(\mathbb{Q})$, dunque $E^{(n)}(\mathbb{Q})$ è un sottogruppo di $E(\mathbb{Q})$.

La mappa $E^{(n)}(\mathbb{Q}) \to p^n\mathcal{R}$, $P \mapsto x(P)$ è ben definita, infatti se $P \in E^{(n)}(\mathbb{Q})$ e $x = x(P)$ allora $|x|_p \leq p^{-n}$ e $|p^{-n}x|_p = |p^{-n}|_p|x|_p = p^n|x|_p \leq 1$ quindi $p^{-n}x \in \mathcal{R}$ e $x \in p^n\mathcal{R}$.

Se $P_1, P_2, P_3 \in E^{(n)}(\mathbb{Q})$ e $P_3 = P_1 \cdot P_2$, per la proposizione 4.3 abbiamo $x(P_1) + x(P_2) + x(P_3) \in p^{2n}\mathcal{R}$. Sia $P_3 = (z_3, x_3, 1)$ allora

$$O \cdot P_3 = -P_3 = \left(1, \frac{x_3}{z_3}, -\frac{1}{z_3} - a_1\frac{x_3}{z_3} - a_3\right) = (z_3, x_3, -1 - a_1x_3 - a_3z_3) =$$
$$= \left(-\frac{z_3}{1 + a_1x_3 + a_3z_3}, -\frac{x_3}{1 + a_1x_3 + a_3z_3}, 1\right)$$
$$\Rightarrow \quad x(P_1 + P_2) = x(O \cdot P_3) = -\frac{x_3}{1 + a_1x_3 + a_3z_3}$$

dunque

$$x(P_1 + P_2) + x(P_3) = -\frac{x_3}{1 + a_1x_3 + a_3z_3} + x_3 = x_3\frac{a_1x_3 + a_3z_3}{1 + a_1x_3 + a_3z_3}$$

essendo $|a_1x_3 + a_3z_3|_p \leq p^{-n}$ e $|1 + a_1x_3 + a_3z_3|_p = 1$

$$|x(P_1 + P_2) + x(P_3)|_p = |x_3|_p|a_1x_3 + a_3z_3|_p \leq p^{-2n}$$
$$\Rightarrow \quad x(P_1 + P_2) + x(P_3) \in p^{2n}\mathcal{R}$$

e per la disuguaglianza ultrametrica

$$x(P_1+P_2)-x(P_1)-x(P_2) = (x(P_1+P_2)+x(P_3))-(x(P_1)+x(P_2)+x(P_3)) \in p^{2n}\mathcal{R}$$

Abbiamo mostrato che la mappa $E^{(n)}(\mathbb{Q}) \to p^n\mathcal{R}/p^{2n}\mathcal{R}$, $P \mapsto x(P) \mod p^{2n}\mathcal{R}$ è un omomorfismo di gruppi. Se P sta nel nucleo di tale omomorfismo allora $x(P) \in p^{2n}\mathcal{R}$ quindi $|x(P)|_p \leq p^{-2n}$ e $P \in E^{(2n)}(\mathbb{Q})$. Il nucleo dell'omomorfismo è contenuto in $E^{(2n)}(\mathbb{Q})$ e l'omomorfismo indotto $E^{(n)}(\mathbb{Q})/E^{(2n)}(\mathbb{Q}) \to p^n\mathcal{R}/p^{2n}\mathcal{R}$ è iniettivo.

□

Osserviamo che se $a_1 = 0$ con una dimostrazione analoga si ottiene un omomorfismo iniettivo $E^{(n)}(\mathbb{Q})/E^{(3n)}(\mathbb{Q}) \to p^n\mathcal{R}/p^{3n}\mathcal{R}$.

Denotiamo con $E(\mathbb{Q})_{\text{tors}}$ il sottogruppo di torsione di $E(\mathbb{Q}$.

Proposizione 4.5. *Per ogni primo dispari p si ha $E(\mathbb{Q})_{tors} \cap E^{(1)}(\mathbb{Q}) = 0$, vale anche per $p = 2$ se $a_1 = 0$.*

Dimostrazione. Consideriamo prima il caso in cui $a_1 = 0$. Sia p un primo e supponiamo $E(\mathbb{Q})_{\text{tors}} \cap E^{(1)}(\mathbb{Q}) \neq 0$, sia $P \in E(\mathbb{Q})_{\text{tors}} \cap E^{(1)}(\mathbb{Q})$, $P \neq O$, un punto di ordine un primo q.
$\bigcap_{n=1}^{\infty} E^{(n)}(\mathbb{Q}) = \{O\}$ dunque esiste un numero naturale $n \geq 1$ tale che $P \in E^{(n)}(\mathbb{Q})$ e $P \notin E^{(n+1)}(\mathbb{Q})$.
$E^{(n)}(\mathbb{Q})/E^{(3n)}(\mathbb{Q}) \to p^n\mathcal{R}/p^{3n}\mathcal{R}$, $P \mapsto x(P) \mod p^{3n}\mathcal{R}$ è un omomorfismo iniettivo, $qP = O$ dunque $qx(P) = x(qP) \in p^{3n}\mathcal{R}$, se $q \neq p$ allora $x(P) \in p^{3n}\mathcal{R} \subseteq p^{2n}\mathcal{R}$, se $q = p$ allora $x(P) \in p^{2n}\mathcal{R}$. In ogni caso per l'iniettività di $E^{(n)}(\mathbb{Q})/E^{(2n)}(\mathbb{Q}) \to p^n\mathcal{R}/p^{2n}\mathcal{R}$ si ha $P \in E^{(2n)}(\mathbb{Q}) \subseteq E^{(n+1)}(\mathbb{Q})$ contro il fatto che $P \notin E^{(n+1)}(\mathbb{Q})$.

Se $a_1 \neq 0$ e p è un primo dispari, supponiamo esista $P = (z, x, 1) \in E(\mathbb{Q})_{\text{tors}} \cap E^{(1)}(\mathbb{Q})$, $P \neq O$, allora P è un punto di torsione con $|z|_p, |x|_p < 1$ e $z \neq 0$. Facciamo degli opportuni cambi di variabili in modo da ottenere una forma di Weierstrass in cui il termine in xyz non compaia: $P = (1, x', y')$ con

$$x' = \frac{x}{z}, \quad y' = \frac{1}{z} \quad \text{e} \quad y'^2 + a_1x'y' + a_3y' = x'^3 + a_2x'^2 + a_4x + a_6$$

se $x'' = 4x'$, $y'' = 8y' + 4a_1x'$, allora $(1, x'', y'')$ è un punto di torsione di $y''^2+8a_3y'' = x''^3+4a_2x''^2+(16a_4+8a_1a_3)x''+64a_6$ e se $\bar{z} = 1/y''$, $\bar{x} = x''/y''$, $(\bar{z}, \bar{x}, 1)$ è un punto di torsione della curva $\bar{E}$ di equazione $\bar{z} + 8a_3\bar{z}^2 = \bar{x}^3 + 4a_2\bar{x}^2\bar{z} + (16a_4 + 8a_1a_3)\bar{x}\bar{z}^2 + 64a_6\bar{z}^3$.
Osserviamo che per questa curva $(\bar{z}, \bar{x}, 1) \neq (0, 0, 1)$ è un punto di torsione, $\bar{z} = \frac{z}{8+4a_1x}$, siccome p è dispari e $|x|_p < 1$ per la disuguaglianza ultrametrica $|8+4a_1x|_p = 1$ e quindi $|\bar{z}|_p = |z|_p < 1$, per la proposizione 4.2 anche $|\bar{x}|_p < 1$ dunque $(\bar{z}, \bar{x}, 1) \in \bar{E}(\mathbb{Q})_{\text{tors}} \cap \bar{E}^{(1)}(\mathbb{Q})$ contro quanto dimostrato prima per le curve con $a_1 = 0$. □

4.3 Teoremi di Lutz-Nagell

Teorema 4.6 (Lutz-Nagell)**.** *Sia E la curva ellittica di equazione*

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

a coefficienti in $\mathbb{Z}$. Allora

i) se $a_1 = 0$ e $P = (x, y) \in E(\mathbb{Q})_{tors}$, allora $x, y \in \mathbb{Z}$;

ii) se $P = (x, y) \in E(\mathbb{Q})_{tors}$, allora $4x, 8y \in \mathbb{Z}$;

iii) se p è un primo dispari e $p \nmid \Delta$, allora $r_p : E(\mathbb{Q})_{tors} \to E_p(\mathbb{Z}_p)$ è iniettiva, vale anche per $p = 2$ se $a_1 = 0$;

iv) se $a_1 = a_2 = a_3 = 0$, cioè $y^2 = x^3 + Ax + B$, se $P = (x, y) \in E(\mathbb{Q})_{tors}$ allora $y = 0$ oppure $y^2 \mid d = -4A^3 - 27B^2$.

Dimostrazione. i) Se $a_1 = 0$, sia $P = (1, x, y) \in E(\mathbb{Q})_{\text{tors}}$ con $y \neq 0$, allora $P = (z', x', 1)$ con $z' = 1/y$, $x' = x/y$. Sia p un primo, allora per la proposizione 4.5 $P \notin E^{(1)}(\mathbb{Q})$ e per la proposizione 4.2 $|z'|_p \geq 1$. Allora $|y|_p = \left|\frac{1}{z'}\right|_p \leq 1$ per ogni primo p e si conclude che $y \in \mathbb{Z}$. Abbiamo mostrato che se $(1, x, y) \in E(\mathbb{Q})_{\text{tors}})$ allora $y \in \mathbb{Z}$, in tal caso x è una radice razionale del polinomio monico a coefficienti interi $x^3 + a_2x^2 + a_4x + a_6 = y^2 + a_3y$, dunque anche $x \in \mathbb{Z}$.

ii) Sia $P = (x, y) \in E(\mathbb{Q})_{\text{tors}}$, sia $(x', y') = (4x, 8y)$, allora $y'^2 + 2a_1x'y' + 8a_3y' = x'^3 + 4a_2x'^2 + 16a_4x' + 64a_6$, completiamo il quadrato a primo membro: sia $(x'', y'') = (x', y' + a_1x')$, allora $y''^2 + 8a_3y'' = x''^3 + (4a_2 + a_1^2)x''^2 + (16a_4 + 8a_1a_3)x'' + 64a_6$. Per il punto i) concludiamo che $x'', y'' \in \mathbb{Z}$, ma allora $x', y' \in \mathbb{Z}$, cioè $4x, 8y \in \mathbb{Z}$.

iii) Se $p \nmid \Delta$ allora $\ker(r_p) = E^{(1)}(\mathbb{Q})$, per la proposizione 4.5 $E(\mathbb{Q})_{\text{tors}} \cap E^{(1)}(\mathbb{Q}) = 0$, dunque $r_p|_{E(\mathbb{Q})_{\text{tors}}}$ è iniettiva.

iv) Sia $y^2 = x^3 + Ax + B$ l'equazione di E, se $P = (x, y) \in E(\mathbb{Q})_{\text{tors}}$ allora

$$x(2P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)} = \frac{\nu(x)}{4y^2} \quad \Rightarrow \quad \nu(x) = 4y^2x(2P)$$

per il punto i) abbiamo $x, y, x(2P) \in \mathbb{Z}$ dunque $\nu(x) \in \mathbb{Z}$ e $y^2 \mid \nu(x)$,

$$d = -4A^3 - 27B^2 = -(3x^2 + 4A)\nu(x) + (3x^3 - 5Ax - 27B)y^2$$

quindi $y^2 \mid d$.

□

Dal teorema di Lutz-Nagell si può ricavare un algoritmo per determinare il sottogruppo di torsione, $E(\mathbb{Q})_{\text{tors}}$, di una curva ellittica. Si mette la curva in forma di Weierstrass ridotta: $y^2 = x^3 + Ax + B$, si considerano tutti gli interi $y \in \mathbb{Z}$ tali che $y^2 \mid d = -4A^3 - 27B^2$, per ciascuno di essi esiste un numero finito di interi $x \in \mathbb{Z}$ tali che $(x, y) \in E(\mathbb{Q})$, cio`e soddisfano l'equazione $y^2 = x^3 + Ax + B$. In questo modo resta determinato un numero finito di punti che sono gli unici candidati ad essere punti di torsione per la

curva ellittica E, quindi abbiamo un limite superiore finito per $\operatorname{card} E(\mathbb{Q})_{\text{tors}}$. Per ciascuno dei punti (x, y) selezionati si può controllare se è un punto di torsione calcolando al più $\operatorname{card} E(\mathbb{Q})_{\text{tors}}$ potenze di (x, y) secondo la legge di gruppo di E.

L'algoritmo funziona in generale, ma spesso risulta un procedimento eccessivamente lungo se lo scopo è solo determinare la struttura del sottogruppo di torsione, senza necessariamente trovarne tutti gli elementi. Nell'esempio seguente vediamo che a tal fine è più semplice usare il punto iii) del teorema 4.6 piuttosto che il punto iv) dello stesso teorema.

Esempio 2. *Sia E la curva di equazione $y^2 - xy + 2y = x^3 + 2x^2$,*

$$\begin{aligned}
&a_1 = -1, \quad a_2 = a_3 = 2, \quad a_4 = a_6 = 0\\
&b_2 = a_1^2 + 4a_2 = 9, \quad b_4 = 2a_4 + a_1a_3 = -2, \quad b_6 = a_3^2 + 4a_6 = 4,\\
&b_8 = a_1^6a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 = 8\\
&\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 = -2^7 13
\end{aligned}$$

con opportuni cambi di variabili mettiamo l'equazione di E in forma di Weierstrass ridotta, in modo da poter applicare i teoremi di Lutz-Nagell.

$$\begin{aligned}
&a_1 = -1, \quad a_2 = a_3 = 2, \quad a_4 = a_6 = 0\\
&b_2 = 9, \quad b_4 = -2, \quad b_6 = 4, \quad b_8 = 8
\end{aligned}$$

$$y^2 - xy + 2y = x^3 + 2x^2 \qquad \Longleftrightarrow \qquad \left(y + \frac{x}{2} + 1\right)^2 = x^3 + \frac{9x^2}{4} - x + 1$$

siano $y' = y + \frac{x}{2} + 1$ e $x' = x$ allora

$$\begin{aligned}
y'^2 = x'^3 + \frac{9x'^2}{4} - x' + 1 \qquad &\Longleftrightarrow \qquad 4y'^2 = 4x'^3 + 9x'^2 - 4x' + 4\\
&\Longleftrightarrow \qquad 2^6y'^2 = 2^6x'^3 + 2^43^2x'^2 - 2^6x' + 2^6
\end{aligned}$$

siano $y'' = 2^3y'$ e $x'' = 2^2x'$ allora $y''^2 = x''^3 + 9x'' - 16x' + 64$, se $\bar{y} = y''$ e $\bar{x} = x'' + 3$ otteniamo $\bar{y}^2 = \bar{x}^3 - 43\bar{x} + 166$.

I cambi di variabili usati sono:

$$\begin{cases} \bar{x} = 4x + 3 \\ \bar{y} = 8y + 4x + 8 \end{cases} \qquad \begin{cases} x = \frac{\bar{x}-3}{4} \\ y = \frac{\bar{y}-\bar{x}-5}{8} \end{cases}$$

Dunque

$$\begin{aligned}
\bar{y}^2 = \bar{x}^3 - 43\bar{x} + 166 \qquad &A = -43, \quad B = 166\\
d = -4A^3 - 27B^2 &= -2^{15}13
\end{aligned}$$

Usiamo ora l'algoritmo descritto sopra, cioè applichiamo il punto iv) del teorema 4.6

$$\begin{array}{llll} \bar{y}=0 & \to \nexists \bar{x}\in\mathbb{Z} & \bar{y}=\pm 1 \to \nexists \bar{x}\in\mathbb{Z} & \bar{y}=\pm 2 \to \quad \nexists \bar{x}\in\mathbb{Z} \\ \bar{y}=\pm 4 & \to \nexists \bar{x}\in\mathbb{Z} & \bar{y}=\pm 8 \to \bar{x}=3 & \bar{y}=\pm 16 \to \quad \bar{x}=-5 \\ \bar{y}=\pm 32 & \to \bar{x}=11 & \bar{y}=\pm 64 \to \nexists \bar{x}\in\mathbb{Z} & \bar{y}=\pm 108 \to \quad \nexists \bar{x}\in\mathbb{Z} \end{array}$$

Dunque i possibili punti di torsione per $\bar{y}^2=\bar{x}^3-43\bar{x}+166$ *sono* $(\bar{x},\bar{y})\in\{(3,\pm 8),(-5,\pm 16),(11,\pm 32),\infty\}$*, i possibili punti di torsione per* $y^2-xy+2y=x^3+2x^2$ *sono* $(x,y)\in\{(0,0),(0,-2),(-2,0),(-2-4),(2,\pm 4),\infty\}$ *Controlliamo quali di questi punti sono punti di torsione usando le formule (2.5)*

$$x(2P)=\frac{x^4-b_4x^2-2b_6x-b_8}{4x^3+b_2x^2+2b_4x+b_6}=\frac{x^4+2x^2-8x-8}{4x^3+9x^2-4x+4}$$

$$\begin{array}{llll} x=0 & x(2P)=-2 & y(2P)^2+4y(2P)=0 & y\in\{0,-4\} \\ x=2 & x(2P)=0 & y(2P)^2+2y(2P)=0 & y\in\{0,-2\} \\ x=-2 & x(2P)=2 & y(2P)^2-16=0 & y\in\{\pm 4\} \end{array}$$

$$2\{(0,0),(0,-2),(-2,0),(-2-4),(2,\pm 4),\infty\}\subseteq \subseteq\{(0,0),(0,-2),(-2,0),(-2-4),(2,\pm 4),\infty\}$$

dunque sono tutti punti di torsione e

$$E(\mathbb{Q})_{tors}=\{(0,0),(0,-2),(-2,0),(-2-4),(2,\pm 4),\infty\}\cong\mathbb{Z}_7$$

Oppure possiamo applicare il punto iii) del teorema 4.6: $p=3\nmid\Delta$*,* $E_3(\mathbb{Z}_3)=\{\infty,(0,0),(0,-2),(1,0),(1,-1),(2,\pm 1)\}\cong\mathbb{Z}_7$*, la mappa* $r_p: E(\mathbb{Q})_{tors}\to E_3(\mathbb{Z}_3)\cong\mathbb{Z}_7$ *è iniettiva, dunque* $E(\mathbb{Q})_{tors}\cong 0$ *oppure* $E(\mathbb{Q})_{tors}\cong\mathbb{Z}_7$*, ma si verifica facilmente che* $(0,0)\in E(\mathbb{Q})_{tors}$ *quindi* $E(\mathbb{Q})_{tors}\cong\mathbb{Z}_7$

Esempio 3. *Sia E la curva di equazione* $y^2+xy=x^3+4x^2+x$

$$\begin{aligned} &a_1=1,\quad a_2=4,\quad a_4=1,\quad a_3=a_6=0 \\ &b_2=a_1^2+4a_2=17,\quad b_4=2a_4+a_1a_3=2,\quad b_6=a_3^2+4a_6=0, \\ &b_8=a_1^6a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2=-1 \\ &\Delta=-b_2^2b_8-8b_4^3-27b_6^2+9b_2b_4b_6=225=3^25^2 \end{aligned}$$

$p=7\nmid\Delta$*,* $E_7(\mathbb{Z}_7)=\{\infty,(0,0),(1,2),(1,4),(3,2),(5,1),(6,2),(6,6)\}$ *allora per il punto iii) del teorema 4.6* $\mathrm{card}(E(\mathbb{Q})_{tors})\le\mathrm{card}(E_7(\mathbb{Z}_7))=8$*. Con oppotruni cambi di variabili portiamo l'equazione di E in forma di Weierstrass ridotta:*

$$\begin{array}{lll} y'=y+\dfrac{x}{2},\quad x'=x & \Rightarrow y'^2=x'^3+\dfrac{17x'}{4}+x' \\ & \Rightarrow \quad 2^6y'^2=2^6x'^3+2^417x'^2+2^6x' \\ \bar{y}=2^3y',\quad \bar{x}=2^2x' & \Rightarrow \quad \bar{y}^2=\bar{x}^3+17\bar{x}^2+16\bar{x} \\ & \Rightarrow \quad \bar{y}^2=\bar{x}(\bar{x}+1)(\bar{x}+16) \end{array}$$

Abbiamo ottenuto un'equazione della forma $y^2 = x(x + r^2)(x + s^2)$ *dunque, per quanto visto nel paragrafo sulla costruzione di punti con determinata torsione,* $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \subseteq E(\mathbb{Q})_{tors}$*, ma* $\text{card}(E(\mathbb{Q})_{toes}) \leq 8$*, concludiamo quindi che* $E(\mathbb{Q})_{tors} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2$*.*

Proposizione 4.7. *Sia* E_p *la curva* $y^2 = x^3 + Ax$ *su* $\mathbb{Z}_p$*, con* p *un primo tale che* $p \nmid \Delta$*,* $p \geq 7$ *e* $p \equiv 3 \mod 4$*, allora* $E_p(\mathbb{Z}_p)$ *ha esattamente* $p + 1$ *punti.*

Dimostrazione. -1 non è u n quadrato modulo p perché $p \equiv 3 \mod 4$. Consideriamo i punti $P \in E_p(\mathbb{Z}_p)$ con $x \neq 0$:

se $y = 0$ allora $0 = y^2 = x(x^2 + A)$, dunque $P \in \{(\sqrt{-A}, 0), (-\sqrt{-A}, 0)\}$,

se $y \neq 0$ allora $y^2 = x^3 + Ax \neq 0$ e anche $-(x^3 + Ax) = (-x)^3 + A(-x) \neq 0$ esattamente uno tra $x^3 + Ax$ e $-(x^3 + Ax)$ è un quadrato modulo p dunque $P \in \{(x, y), (x, -y)\}$.

Dunque ad ogni coppia $x, -x$ con $x \in \mathbb{Z}_p$, $x \neq 0$, corrispondono due punti distinti in $E_p(\mathbb{Z}_p)$. $E_p(\mathbb{Z}_p)$ contiene $p - 1$ punti con $x \neq 0$, il punto $(0, 0)$ corrispondente a $x = 0$ e il punto all'infinito, in totale $p + 1$ punti. □

Teorema 4.8. *Se* E *ha equazione* $y^2 = x^3 + Ax$ *con* $A \in \mathbb{Z}$ *privo di fattori con potenze quarte, allora*

$$E(\mathbb{Q})_{tors} = \begin{cases} \mathbb{Z}_2 \oplus \mathbb{Z}_2 & \text{se } -A \text{ è un quadrato,} \\ \mathbb{Z}_4 & \text{se } A = 4, \\ \mathbb{Z}_2 & \text{altrimenti.} \end{cases}$$

Dimostrazione. Per il punto iii) del teorema 4.6 per ogni primo $p \nmid \Delta$ $\text{card}(E(\mathbb{Q})_{\text{tors}}) \mid \text{card}(E_p(\mathbb{Z}_p))$, dunque usando il risultato della proposizione 4.7 abbiamo che $\text{card}(E(\mathbb{Q})_{\text{tors}}) \mid p + 1$ per ogni primo $p \equiv 3 \mod 4$ sufficientemente grande. Per il teorema di Dirichlet 1.20 esistono infiniti primi della forma $an + b$ con $\text{MCD}(a, b) = 1$.

Sia p un primo, $p \equiv 3 \mod 4$ e $p \equiv 3 \mod 8$, allora $p + 1 \equiv 4 \mod 8 \Rightarrow 8 \nmid p + 1 \Rightarrow 8 \nmid \text{card}(E(\mathbb{Q})_{\text{tors}}$.

Sia p un primo, $p \equiv 3 \mod 4$ e $p \equiv 7 \mod 12$, allora $p+1 \equiv 8 \mod 12 \Rightarrow 3 \nmid p + 1 \Rightarrow 3 \nmid \text{card}(E(\mathbb{Q})_{\text{tors}}$.

Se $q > 3$ è un primo, sia p un primo, $p \equiv 3 \mod 4$ e $p \equiv 3 \mod 4q$, allora $p + 1 \equiv 4 \mod q \Rightarrow q \nmid p + 1 \Rightarrow q \nmid \text{card}(E(\mathbb{Q})_{\text{tors}})$.

Dunque $\text{card}(E(\mathbb{Q})_{\text{tors}}) \mid 4$ e $\{(0, 0), \infty\} \cong \mathbb{Z}_2 \subseteq E(\mathbb{Q})_{\text{tors}}$.

$E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ se e solo se $y^2 = x(x^2 + A)$ si spezza su $\mathbb{Z}$, se e solo se $-A$ è un quadrato.

Se $-A$ non è un quadrato, sia $P = (x, y) \in E(\mathbb{Q})_{\text{tors}}$, $P \neq (0, 0)$ vediamo sotto quali condizioni $2P = (0, 0)$, cioè $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}_4$.

$$x(2P) = \frac{x^4 - 2Ax^2 + A^2}{4y^2} = \frac{(x^2 - A)^2}{4y^2} = 0$$

se e solo se $x^2 = A$, A non ha fattori con potenze quarte, dunque x non ha fattori quadrati, $y^2 = x^3 + Ax = 2x^3$ se e solo se $x = \pm 2$, perchè x non ammette fattori dispari essendo privo di fattori quadrati e $x = \pm 1 \Rightarrow y^2 = \pm 2$ che non ha radici intere. Dunque $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}_4$ se e solo se $A = 4$. □

Proposizione 4.9. *Sia E_p la curva di equazione $y^2 = x^3 + B$ su $\mathbb{Z}_p$, con p un primo tale che $p \nmid \Delta$, $p \geq 5$ e $p \equiv 2 \mod 3$, allora $E_p(\mathbb{Z}_p)$ ha esattamente $p + 1$ punti.*

Dimostrazione. $\mathbb{Z}_p^\times$ è un gruppo moltiplicativo di ordine $p-1$, $p \equiv 2 \mod 3$ dunque $3 \nmid p - 1 \equiv 1 \mod 3$ e $\mathbb{Z}_p^\times$ non ha elementi di ordine 3, $a \mapsto a^3$ è un automorfismo di $\mathbb{Z}_p^\times$ e ogni elemento di $\mathbb{Z}_p$ ha una e una sola radice cubica. Quindi $E_p(\mathbb{Z}_p)$ contiene p punti della forma $(1, x, y)$ e il punto all'infinito, in totale $p + 1$ punti. □

Teorema 4.10. *Se E ha equazione $y^2 = x^3 + B$ con $B \in \mathbb{Z}$ privo di fattori con potenze seste, allora*

$$E(\mathbb{Q})_{tors} = \begin{cases} \mathbb{Z}_6 & \text{se } B = 1, \\ \mathbb{Z}_3 & \text{se } B = -432 \text{ o } B \text{ è un quadrato diverso da 1,} \\ \mathbb{Z}_2 & \text{se } B \text{ è un cubo diverso da 1,} \\ 0 & \text{altrimenti.} \end{cases}$$

Dimostrazione. Per il punto iii) del teorema 4.6 per ogni primo $p \nmid \Delta$ $\text{card}(E(\mathbb{Q})_{\text{tors}}) \mid \text{card}(E_p(\mathbb{Z}_p))$, dunque usando il risultato della proposizione 4.9 abbiamo che $\text{card}(E(\mathbb{Q})_{\text{tors}}) \mid p + 1$ per ogni primo $p \equiv 3 \mod 4$ sufficientemente grande. Per il teorema di Dirichlet 1.20 esistono infiniti primi della forma $an + b$ con $\text{MCD}(a, b) = 1$.

Sia p un primo, $p \equiv 2 \mod 3$ e $p \equiv 5 \mod 12$, allora $p + 1 \equiv 2 \mod 4 \Rightarrow 4 \nmid p + 1 \Rightarrow 4 \nmid \text{card}(E(\mathbb{Q})_{\text{tors}})$.

Sia p un primo, $p \equiv 2 \mod 3$ e $p \equiv 2 \mod 9$, allora $p + 1 \equiv 3 \mod 9 \Rightarrow 9 \nmid p + 1 \Rightarrow 9 \nmid \text{card}(E(\mathbb{Q})_{\text{tors}})$.

Se $q > 3$ è un primo, sia p un primo, $p \equiv 2 \mod 3$ e $p \equiv 2 \mod 3q$, allora $p + 1 \equiv 2 \mod q \Rightarrow q \nmid p + 1 \Rightarrow q \nmid \text{card}(E(\mathbb{Q})_{\text{tors}})$.

Dunque $\text{card}(E(\mathbb{Q})_{\text{tors}} \mid 6$.

Osserviamo che E ha punti di 2-torsione diversi dal punto all'infinito se e solo se $x^3 + B = 0$ ha radici intere, se e solo se B è un cubo e in tal caso si

ha una sola soluzione razionale, dunque E ha due punti di torsione se B è un cubo. Sia $P = (x, y) \in E(\mathbb{Q})_{\text{tors}}$, $P \neq (0, 0)$ vediamo sotto quali condizioni P è un punto di 3-torsione, cioè $2P = -P$.

$$x(2P) = \frac{x^4 - 8Bx}{4(x^3 + B)} = x \qquad \Longleftrightarrow \qquad x(3x^3 + 12B) = 0$$

$x = 0 \Rightarrow y^2 = B$ che ha 2 soluzioni intere se B è un quadrato, $x^3 = -4B \Rightarrow y^2 = -3B \Rightarrow B = -2^4 3^3$ perché B è privo di radici seste.

$E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}_6$ se E ha punti di 2-torsione e punti di 3-torsione, cioè se B è sia un cubo che un quadrato, se e solo se $B = 1$.

$E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}_3$ se E ha punti di 3-torsione, ma non di 2-torsione, cioè se $B = -432$ oppure $B \neq 1$ è un quadrato.

$E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}_2$ se E ha punti di 2-torsione, ma non di 3-torsione, cioè se $B \neq 1$ è un cubo.

□

Capitolo 5

Metodi di discesa di Fermat e curve ellittiche

In questo capitolo ci occuperemo di due problemi risolti da Fermat con dei metodi di discesa e delle loro relazioni con la legge di gruppo di alcune curve ellittiche ad essi associate tramite trasformazioni birazionali.

Entrambi i quesiti consistono nel cercare soluzioni intere non banali di un'equazione omogenea di quarto grado e in entrambi i casi Fermat presuppone di avere una soluzione non banale e mostra che sotto certe condizioni allora ne esiste un'altra in qualche senso "più piccola", sulla curva ellittica birazionalmente equivalente alla quartica questo procedimento corrisponde alla costruzione di un punto $\frac{1}{2}P$ supponendo di conoscere P. In questo senso si parla di metodo di discesa, tale metodo però è usato nei due esempi che vedremo per ottenere risultati molto diversi.

Nel primo caso si dimostra che data una soluzione non banale allora ne esiste necessariamente un'altra di non banale e strettamente "più piccola", ma non possono esistere infinite soluzioni "più piccole"di una fissata, dunque si conclude con un ragionamento per assurdo che non esistono soluzioni non banali, perché se ne esistesse una si innescherebbe un processo di discesa infinita. Questo particolare uso del metodo di discesa si chiama anche metodo della discesa infinita ed è quello usato nella dimostrazione del teorema di Mordell.

Nel secondo caso invece si usa il metodo di discesa per trovare soluzioni non banali, perché permette di ricostruire a partire dalla soluzione "più piccola"la soluzione che si era supposto esistere inizialmente. In particolare assumendo come soluzione "più piccola"una soluzione banale si possono costruire soluzioni non banali della quartica in esame.

In entrambi i casi vedremo che esiste un parallelismo tra il comportamento delle soluzioni della quartica di Fermat e quello dei punti razionali della curva ellittica ad essa associata e che il metodo di discesa può essere applicato con la stessa efficacia all'una come all'altra curva.

5.1 Caso quartico dell'ultimo teorema di Fermat

Teorema 5.1 (Ultimo Teorema di Fermat)**.** *$x^n + y^n = z^n$ non ha soluzioni intere non banali se $n > 2$.*

L'Ultimo Teorema di Fermat è stato dimostrato da A. Wiles nel 1994, qui ci occuperemo soltanto del caso particolare con esponente $n = 4$ che fu dimostrato da Fermat ricorrendo al metodo di discesa. Fermat dimostrò che l'equazione $x^4 + y^4 = z^2$ non ha soluzioni intere non banali e quindi neppure $x^4 + y^4 = z^4$.

Proposizione 5.2 (Fermat)**.** *$x^4 + y^4 = z^2$ non ha soluzioni intere non banali.*

Dimostrazione. Supponiamo di avere una soluzione intera non banale (u, v, w), non è restrittivo supporre u, v coprimi. Siccome (u^2, v^2, w) è una terna pitagorica per il teorema 1.4 possiamo supporre u dispari e v pari ed esistono interi m e n tali che

$$u^2 = m^2 - n^2 \qquad v^2 = 2mn \qquad \mathrm{MCD}(m, n) = 1$$

applicando nuovamente il teorema 1.4 all'equazione $m^2 = u^2 + n^2$ si trovano p e q interi tali che

$$u = p^2 - q^2 \qquad n = 2pq \qquad m = p^2 + q^2 \qquad \mathrm{MCD}(p, q) = 1$$

dunque

$$\left(\frac{v}{2}\right)^2 = \frac{mn}{2} = pq(p^2 + q^2) \tag{5.1}$$

osservo che siccome $\mathrm{MCD}(p, q) = 1$ si ha che $p, q, p^2 + q^2$ sono coprimi, ma da 5.1 si ottiene che sono tutti e tre dei quadrati, quindi esistono r, s interi tali che

$$p = r^2 \qquad q = s^2$$

e $p^2 + q^2 = r^4 + s^4$ sia un quadrato, cioè r, s determinano un'altra soluzione intera dell'equazione di $x^4 + y^4 = z^2$. La nuova soluzione è non banale perché altrimenti, siccome $v = 2rs\sqrt{r^4 + s^4}$, si avrebbe $v = 0$. Dunque $rs \neq 0$ e $r, s < v$ e quindi $\max(|r|, |s|) < \max(|u|, |v|)$. Da ogni soluzione intera non banale $(u, v, u^4 + v^4)$ si può costruire una soluzione non banale $(r, s, r^4 + s^4)$ con $\max(|r|, |s|) < \max(|u|, |v|)$, ma esiste solo un numero finito di numeri interi distinti in valore assoluto minori di $\max(|u|, |v|)$, contro il fatto che si possano costruire infinite soluzioni non banali a partire da (u, v, w) tutte distinte e con la proprietà che $\max(|r|, |s|) < \max(|u|, |v|)$. Dall'aver assunto l'esistenza di una soluzione intera non banale di $x^4 + y^4 = z^2$ abbiamo raggiunto una contraddizione, dunque l'equazione $x^4 + y^4 = z^2$ non ammette soluzioni intere non banali. □

Consideriamo l'equazione $u^4 + v^4 = w^2$ siano

$$\begin{cases} \xi = \frac{u}{v} \\ \eta = \frac{w}{v^2} \end{cases} \qquad \Rightarrow \qquad \eta^2 = \xi^4 + 1$$

con le seguenti trasformazioni birazionali:

$$\begin{cases} x = \frac{2}{\eta - \xi^2} \\ y = \frac{4\xi}{\eta - \xi^2} \end{cases} \qquad \Longleftrightarrow \qquad \begin{cases} \xi = \frac{y}{2x} \\ \eta = \frac{y^2 + 8x}{4x^2} \end{cases} \tag{5.2}$$

otteniamo l'equazione di una curva ellittica:

$$\left(\frac{y^2 + 8x}{4x^2}\right)^2 = \left(\frac{y}{2x}\right)^4 + 1 \quad \Longleftrightarrow \quad \frac{y^4 + 16xy^2 + 64x^2}{16x^4} = \frac{y^4 + 16x^4}{16x^4}$$
$$\Longleftrightarrow \quad \frac{y^2}{x^3} = \frac{x^3 - 4x}{x^3} \quad \Longleftrightarrow \quad x \neq 0, \quad y^2 = x^3 - 4x$$

Vogliamo analizzare le relazioni tra il metodo di discesa usato da Fermat e il comportamento dei punti sulla cubica E: $y^2 = x^3 - 4x$.

Nella proposizione 5.2 abbiamo dimostrato che da una soluzione non banale (u, v, w) dell'equazione $u^4 + v^4 = w^2$ si ottiene un'altra soluzione non banale $(r, s, \sqrt{r^4 + s^4})$ legata alla prima dalle relazioni:

$$\begin{aligned} &(u^2, v^2, w) = (m^2 - n^2, 2mn, m^2 + n^2) \\ &(m, n) = (p^2 + q^2, 2pq) \\ &(p, q) = (r^2, s^2) \quad \Rightarrow \quad (m, n) = (r^4 + s^4, 2r^2 s^2) \\ &(u, v) = (p^2 - q^2, v) = (r^4 - s^4, 2rs\sqrt{r^4 + s^4}) \end{aligned}$$

sia $R = \frac{r}{s}$ e sia $P = (c, d)$ il punto sulla cubica $d^2 = c^3 - 4c$ corrispondente alla soluzione $(r, s, \sqrt{r^4 + s^4})$ tramite le trasformazioni (5.2) e (x, y) il punto

corrispondente a (u, v, w), allora:

$$R^2 = \left(\frac{r}{s}\right)^2 = \left(\frac{d}{2c}\right)^2 = \frac{c^3 - 4c}{4c^2} = \frac{c^2 - 4}{4c}$$

$$\eta - \xi^2 = \frac{w - u^2}{v^2} = \frac{m^2 + n^2 - (m^2 - n^2)}{2mn} = \frac{n}{m} = \frac{2r^2 s^2}{r^4 + s^4} = \frac{2R^2}{R^4 + 1}$$

$$x = \frac{2}{\eta - \xi^2} = \frac{R^4 + 1}{R^2} = \frac{\left(\frac{c^2-4}{4c}\right)^2 + 1}{\frac{c^2-4}{4c}} = \frac{(c^2 + 4)^2}{4c(c^2 - 4)}$$

$$\xi = \frac{u}{v} = \frac{r^4 - s^4}{2rs\sqrt{r^4 + s^4}} = \frac{R^4 - 1}{2R\sqrt{R^4 + 1}} = \frac{\left(\frac{c^2-4}{4c}\right)^2 - 1}{2\sqrt{\frac{c^2-4}{4c}}\sqrt{\left(\frac{c^2-4}{4c}\right)^2 + 1}} =$$

$$= \frac{\frac{c^4-24c^2+16}{16c^2}}{2\sqrt{\frac{c^2-4}{4c}}\frac{c^2+4}{4|c|}} = \frac{c^4 - 24c^2 + 16}{2\sqrt{4c(c^4 - 4)}(c^2 + 4)} = \frac{c^4 - 24c^2 + 16}{2\sqrt{4c\frac{d^2}{c}}(c^2 + 4)} =$$

$$= \frac{c^4 - 24c^2 + 16}{4|d|(c^2 + 4)}$$

$$y = 2\xi x = \frac{c^4 - 24c^2 + 16}{4|d|(c^2 + 4)} \frac{(c^2 + 4)^2}{4c(c^2 - 4)} = \frac{(c^4 - 24c^2 + 16)(c^2 + 4)}{8|d|c(c^2 - 4)}$$

osserviamo che poiché $r, s > 0$ allora $R > 0$ e dalle formule (5.2) otteniamo che

$$d = \frac{4\frac{r}{s}}{\frac{\sqrt{r^4+s^4}}{s^2} - \left(\frac{r}{s}\right)^2} = \frac{4R}{\sqrt{R^4 + 1} - R^2} > 0 \quad \Rightarrow \quad |d| = d$$

consideriamo la cubica $d^2 = c^3 - 4c$:

$$a_1 = a_2 = a_3 = a_6 = 0, \quad a_4 = -4$$
$$b_2 = a_1^2 + 4a_2 = 0, \quad b_4 = 2a_4 + a_1 a_3 = -8$$
$$b_6 = a_3^2 + 4a_6 = 0, \quad b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 = -16$$

usando le formule (2.4) e (2.5) calcoliamo le coordinate del punto $2P$:

$$x_{2P} = \frac{c^4 - b_4 c^2 - 2b_6 c - b_8}{4c^3 + b_2 c^2 + 2b_4 c + b_6} = \frac{c^4 + 8c^2 + 16}{4c^3 - 16c} = \frac{(c^2 + 4)^2}{4c(c^2 - 4)} = x$$

$$
\begin{aligned}
m &= \frac{3c^2 + 2a_2c + a_4 - a_1d}{2d + a_1c + a_3} = \frac{3c^2 - 4}{2d} \\
b &= \frac{-c^3 + a_4c + 2a_6 - a_3d}{2d + a_1c + a_3} = \frac{-c^3 - 4c}{2d} \\
y_{2P} &= -(m + a_1)x_{2P} - a_3 - b = -mx_{2P} - b = \\
&= -\frac{3c^2 - 4}{2d}\frac{(c^2 + 4)^2}{4c(c^2 - 4)} + \frac{c^3 + 4c}{2d} = \\
&= \frac{c^2 + 4}{2d}\frac{-3c^4 - 12c^2 + 4c^2 + 16 + 4c^4 - 16c^2}{4c(c^2 - 4)} = \\
&= \frac{c^2 + 4}{2d}\frac{c^4 - 24c^2 + 16}{4c(c^2 - 4)} = y
\end{aligned}
$$

Abbiamo mostrato che se (x, y) è il punto su $y^2 = x^3 - 4x$ corrispondente a (u, v) e $P = (c, d)$ è il punto corrispondente a (r, s) allora $2P = (x, y)$, cioè sulla curva ellittica il metodo di discesa di Fermat a partire da un punto (x, y) costruisce un punto $(c, d) = \frac{1}{2}(x, y)$.

Vediamo ora che l'argomento della discesa infinita usato da Fermat può essere applicato alla cubica, parallelamente a quanto fatto per le soluzioni della quartica, per stabilire che i soli punti razionali sono i punti di 2-torsione.

Consideriamo il gruppo dei punti razionali della curva ellittica E: dalla proposizione 4.8 $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$, dunque

$$E(\mathbb{Q})_{\text{tors}} = \{\infty, (-2, 0), (0, 0), (2, 0)\}$$

gli unici punti di torsione di E sono i punti di 2-torsione, che tramite le trasformazioni (5.2) corrispondono alle soluzioni banali $(0, \pm 1)$ della quartica $\xi^4 + 1 = \eta^2$.

Se $(x, y) \in E(\mathbb{Q})$ fosse un punto non di torsione, dalle proprietà 3.2 e 3.3 dell'altezza canonica h ricaviamo che $h(x, y) \neq 0$ e

$$h(c, d) = \frac{1}{4}h(x, y) < h(x, y)$$

allora per ogni punto non di torsione (x, y) di E ne esiste un altro $(c, d) \neq (x, y)$ con altezza strettamente minore, ovvero ci sono infiniti punti con altezza minore di $h(x, y)$, contro il fatto che i punti di $E(\mathbb{Q})$ con altezza minore di una costante $h(x, y)$ sono in numero finito. Dunque $E(\mathbb{Q})$ non contiene punti che non siano di torsione: $E(\mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

5.2 Problema di Fermat a Mersenne

Pierre de Fermat (1601-1665) è famoso per i suoi problemi di semplice formulazione, ma non sempre di altrettanto facile risoluzione (si pensi al

suo Ultimo Teorema), che spesso sottoponeva ai matematici del suo tempo. Ci occuperemo di uno di tali problemi, che egli aveva proposto a Saint-Martin e Frenicle senza suscitare il loro entusiasmo, come si evince dalla corrispondenza tra Fermat e Padre Mersenne.

In una lettera del 31 maggio 1643 diretta probabilmente a Saint-Martin, si trova il seguente quesito:

> *Je vous propose*:
>
> > *Trouver un triangle rectangle duquel le plus grand côté soit un quarré et la somme des deux ou trois autres soit quarrée.*

Fermat chiedeva di trovare un triangolo rettangolo in cui l'ipotenusa e la somma dei cateti siano dei quadrati, usando un metodo di discesa egli trovò una soluzione e la inviò a Padre Mersenne in una lettera dell'agosto 1463, di cui è qui riportato un passo:

> *Et, afin que je ne vous tienne pas plus longuement en suspens, j'ai résolu toutes les questiones que j'ai proposées à ces Messieurs (Frenicle et Saint-Martin), dont je ne vous coterai maintenant qu'un exemple, pour leur ôter seulement la mauvaise impression qu'ils avoient conçue contre moi, comme leur ayant proposé un amusement et un travail inutile. Je choisirai pour mon exemple une des plus belles propositions que je lenr ai faites*:
>
> *Trouver un triangle duquel le plus grand côté soit quarré, et la somme des deux autres soit aussi quarrée.*
>
> *Voici le triangle*:
>
> 4687298610289, 4565486027761, 1061652293520

La soluzione di questo problema si trova anche nelle Osservazioni sull'Opera di Diofanto:

> *Observation sur Diophante XLIV*
>
> *Huic de duplicatis æqualitatibus tractatui multa possemus adjungere quæ nec veteres nec novi detexerunt. Sufficit nunc, ut methodi nostræ dignitatem et usum asseramus, ut quæstionem sequentem, quæ sane difficillima est, resolvamus.*
>
> > *Invenire triangulum numero, cujus hypotenusa sit quadratus, et pariter summa laterum circa rectum.*

Triangulum quæsitum repræsentant tres numeri sequentes:

$$4687298610289, \quad 4565486027761, \quad 1061652293520.$$

Vediamo il metodo usato da Fermat per trovare questa soluzione.
Il problema consiste nel determinare una terna pitagorica di interi positivi x, y, z tali che $x + y$ e z siano dei quadrati. Ovvero nel risolvere sugli interi positivi il seguente sistema :

$$\begin{cases} x^2 + y^2 = z^2 \\ x + y = a^2 \\ z = b^2 \end{cases} \tag{5.3}$$

Siano $e = x - y$, allora il sistema (5.3) è equivalente alle seguenti equazioni

$$x = \frac{a^2 + e}{2}, \quad y = \frac{a^2 - e}{2}, \quad z = b^2 \tag{5.4}$$

$$2b^4 - a^4 = e^2 \tag{5.5}$$

Vogliamo trovare soluzioni intere non banali dell'equazione $2b^4 - a^4 = e^2$. Conosciamo una soluzione banale: $(1, 1, 1)$. Mostriamo che esiste un metodo per costruire soluzioni a partire da quelle che conosciamo già. Supponiamo di conoscere una soluzione non banale (a, b, e) di (5.5), ovvero una soluzione non banale del sistema (5.3), e procediamo a ritroso.

Applicando la proposizione 1.4 alla prima equazione del sistema (5.3) esistono $m, n \in \mathbb{Z}$ tali che

$$x = m^2 - n^2, \qquad y = 2mn, \qquad z = m^2 + n^2 \tag{5.6}$$

applicando nuovamente la proposizione 1.4 all'uguaglianza $z = b^2 = m^2 + n^2$, che si ottiene combinando la terza equazione di (5.3) con la terza equazione di (5.6), esistono $r, s \in \mathbb{Z}$ tali che

$$m = r^2 - s^2, \qquad n = 2rs, \qquad b = r^2 + s^2 \tag{5.7}$$

dalla seconda equazione di (5.3) e dalle (5.6) abbiamo

$$a^2 = x + y = (m + n)^2 - 2n^2$$

se

$$\alpha = \frac{m + n}{a}, \qquad \beta = \frac{n}{a} \tag{5.8}$$

otteniamo una conica $1 = \alpha^2 - 2\beta^2$ con un punto razionale $(\alpha, \beta) = (1, 0)$, la parametrizziamo con il fascio di rette $\alpha = h\beta + 1$:

$$1 = (h\beta + 1)^2 - 2\beta^2 = (h^2 - 2)\beta^2 + 2h\beta + 1$$

$$\Rightarrow \quad \beta = \frac{2h}{2 - h^2}, \quad \alpha = \frac{2h^2}{2 - h^2} + 1 = \frac{h^2 + 2}{2 - h^2}$$

sia $h = \frac{t}{u}$ con $t, u \in \mathbb{Z}$ allora

$$\alpha = \frac{t^2 + 2u^2}{2u^2 - t^2}, \qquad \beta = \frac{2ut}{2u^2 - t^2}$$

e dalle (5.8) otteniamo

$$a = \pm(2u^2 - t^2)\lambda, \qquad n = 2ut\lambda, \qquad m = (2u^2 + t^2 - 2ut)\lambda$$

cerchiamo soluzioni con $\lambda = 1$, cioè

$$a = -(2u^2 - t^2), \qquad n = 2ut, \qquad m = (2u^2 + t^2 - 2ut) \tag{5.9}$$

osserviamo che combinando la seconda equazione di (5.7) con la seconda equazione di (5.9) abbiamo $2rs = n = 2ut$, siano $d, c \in \mathbb{Z}$ tali che

$$\frac{r}{t} = \frac{u}{s} = \frac{d}{c} \qquad \text{con} \qquad \text{MCD}(d, c) = 1$$

quindi

$$t = kc, \qquad r = kd, \qquad u = ld, \qquad s = lc \tag{5.10}$$

con $k = \text{MCD}(t, r), l = \text{MCD}(u, s) \in \mathbb{Z}$. Combinando la prima equazione di (5.7) con la terza di (5.9) e sostituendo (5.10) abbiamo

$$\begin{aligned} m &= r^2 - s^2 = k^2d^2 - l^2c^2 \\ &= 2u^2 + t^2 - 2ut = 2l^2d^2 + k^2c^2 - 2ldkc \\ \Rightarrow \quad & d^2 - \left(\frac{l}{k}\right)^2 c^2 = 2\left(\frac{l}{k}\right)^2 d^2 + c^2 - 2\frac{l}{k}dc \\ \Rightarrow \quad & (2d^2 + c^2)\left(\frac{l}{k}\right)^2 - 2dc\frac{l}{k} + c^2 - d^2 = 0 \end{aligned} \tag{5.11}$$

L'equazione di secondo grado (5.11) ammette soluzioni razionali $\frac{l}{k}$ se e solo se il discriminante dell'equazione è un quadrato:

$$\begin{aligned} \Delta &= d^2c^2 - (2d^2 + c^2)(c^2 - d^2) = d^2c^2 - 2d^2c^2 - c^4 + 2d^4 + d^2c^2 = \\ &= 2d^4 - c^4 = f^2 \end{aligned} \tag{5.12}$$

se e solo se (d, c, f) è una soluzione di (5.5), in tal caso $\frac{l}{k} = \frac{dc \pm |f|}{2d^2 + c^2}$, essendo $2d^4 - c^4 = f^2$ se e solo se $2d^4 - c^4 = (-f)^2$ non è restrittivo considerare

$$\frac{l}{k} = \frac{dc - f}{2d^2 + c^2} \tag{5.13}$$

Ora abbiamo un metodo per costruire una soluzione (a, b, e) a partire da una soluzione data (c, d, f).

Se (c, d, f) è la soluzione banale $(1, 1, 1)$ allora otteniamo una soluzione banale:

$$s = 0 \quad \Rightarrow \quad n = 0 \quad \Rightarrow \quad y = 0$$

Se $(c, d, f) = (1, 1, -1)$ da (5.13) otteniamo $\frac{l}{k} = \frac{2}{3}$, siano $l = 2, k = 3$, allora dalle formule (5.10) otteniamo

$$l = 2, \quad k = 3, \quad t = 3, \quad r = 3, \quad u = 2, \quad s = 2$$

dalle (5.9) $a = t^2 - 2u^2 = 1$, dalle (5.7) abbiamo

$$m = r^2 - s^2 = 5, \quad n = 2rs = 12, \quad b = r^2 + s^2 = 13$$

dalle (5.6)

$$x = m^2 - n^2 = -119, \quad y = 2mn = 120, \quad z = m^2 + n^2 = b^2 = 169 \quad (5.14)$$

da cui si ricava che $e = x - y = -239$. La (5.14) è una soluzione intera non banale, ma non è accettabile perché $x = -119 < 0$ non può essere la lunghezza di un lato di un triangolo, se ripetiamo il procedimento con $(c, d, e) = (1, 13, -239)$ otteniamo $\frac{l}{k} = -\frac{2}{3}$, siano $l = -2, k = 3$, allora

$$r = kd = 39, \quad s = lc = -2, \quad m = r^2 - s^2 = 1517, \quad n = 2rs = -156,$$
$$x = m^2 - n^2 = 2276953, \quad y = 2mn = -473304, \quad z = m^2 + n^2 = 2325625$$

non è una soluzione accettabile perché $y < 0$.

Se invece $(c, d, e) = (1, 13, 239)$, da (5.13) otteniamo $\frac{l}{k} = \frac{84}{113}$, siano $l = 84, k = 113$, allora

$$t = kc = 113, \quad r = kd = 1469, \quad u = ld = 2, \quad s = lc = 84$$
$$m = r^2 - s^2 = 2150905, \quad n = 2rs = 246792, \quad b = r^2 + s^2 = 2165017$$
$$x = m^2 - n^2 = 4565486027761, \quad y = 2mn = 1061652293520,$$
$$z = m^2 + n^2 = 4687298610289$$
$$a = t^2 - 2u^2 = 2372159, \quad e = x - y = 3504233734231$$

abbiamo finalmente trovato la soluzione di Fermat.

L'equazione di quarto grado $2b^4 - a^4 = e^2$ usata da Fermat è birazionalmente equivalente alla curva ellittica E di equazione $y^2 = x^3 + 8x$ tramite le seguenti trasformazioni: se

$$\begin{cases} u = \frac{b}{a} \\ v = \frac{e}{a^2} \end{cases} \qquad \Rightarrow \qquad 2u^4 - 1 = v^2$$

allora

$$\begin{cases} x = \frac{2(v+2u^2-1)}{(u-1)^2} \\ y = \frac{4((2u-1)v+2u^3+1)}{(u-1)^3} \end{cases} \qquad \begin{cases} u = \frac{y-2x-8}{y-4x+8} \\ v = \frac{y^2-24x^2+48y-16x-64}{(y-4x+8)^2} \end{cases} \qquad (5.15)$$

Si può mostrare, con un buon programma di calcolo simbolico, che il metodo usato da Fermat per costruire una soluzione (a, b, e) dell'equazione quartica a partire da una soluzione (c, d, f) corrisponde sulla curva ellittica, tramite le trasformazioni (5.15), alla duplicazione dei punti secondo la somma di Poincaré. Rimandiamo all'Appendice per i dettagli.

Studiamo ora la struttura del gruppo $E(\mathbb{Q})$.
L'equazione di E è

$$y^2 = x^3 + 8x = x(x + 2\sqrt{2}i)(x - 2\sqrt{2}i) = (x - \alpha)(x - \beta)(x - \gamma)$$

con $\alpha = 2\sqrt{2}i, \beta = -2\sqrt{2}i, \gamma = 0 \in \mathbb{Z}[\sqrt{2}i]$.

Dalla proposizione 4.8 abbiamo che $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}_2$ e dunque $E(\mathbb{Q})_{\text{tors}} = \{\infty, (0, 0)\}$.

Proposizione 5.3. *$\mathbb{Z}[\sqrt{2}i]$ è un anello euclideo con il gruppo delle unità $\{\pm 1\}$.*

Dimostrazione. Ogni elemento di $\mathbb{Z}[\sqrt{2}i]$ è della forma $a+\sqrt{2}ib$ con $a, b \in \mathbb{Z}$. Sia $N : \mathbb{Q}[\sqrt{2}i] \to \mathbb{R}$ definita da $N(a + \sqrt{2}ib) = (a + \sqrt{2}ib)(a - \sqrt{2}ib) = a^2 + 2b^2$, si verifica facilmente che la mappa N è una norma al quadrato su $\mathbb{Q}[\sqrt{2}i]$, inoltre rispetta la moltiplicazione, infatti:

$$\begin{aligned} N((a + \sqrt{2}ib)(c + \sqrt{2}id)) &= N(ac - 2bd + \sqrt{2}i(bc + ad)) = \\ &= (ac - 2bd)^2 + 2(bc + ad)^2 = a^2c^2 + 4b^2d^2 + 2b^2c^2 + 2a^2d^2 = \\ &= (a^2 + 2b^2)(c^2 + 2d^2) = N(a + \sqrt{2}ib)N(c + \sqrt{2}id) \end{aligned}$$

Mostriamo che $\mathbb{Z}[\sqrt{2}i]$ è un anello euclideo con valutazione $N : \mathbb{Z}[\sqrt{2}i] \to \mathbb{N}$. Siano $z_1 = a + \sqrt{2}ib, z_2 = c + \sqrt{2}id \in \mathbb{Z}[\sqrt{2}i] \subseteq \mathbb{Q}[\sqrt{2}i]$, $z_2 \neq 0$, allora

$$z_2^{-1} = \frac{c - \sqrt{2}id}{c^2 + 2d^2}$$

$$z_1 z_2^{-1} = (a + \sqrt{2}ib)\frac{c - \sqrt{2}id}{c^2 + 2d^2} = \frac{ac + 2bd}{c^2 + 2d^2} + \sqrt{2}i\frac{bc - ad}{c^2 + 2d^2}$$

Poichè ogni numero razionale si può scrivere come somma di una parte intera più una parte frazionaria in valore assoluto minore o uguale a $1/2$, esistono $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ tali che

$$z_1 z_2^{-1} = q_1 + \frac{r_1}{c^2 + 2d^2} + \sqrt{2}i\left(q_2 + \frac{r_2}{c^2 + 2d^2}\right)$$

con $\left|\frac{r_1}{c^2+2d^2}\right|, \left|\frac{r_2}{c^2+2d^2}\right| \leq \frac{1}{2}$. Allora

$$z_1 = (q_1 + \sqrt{2}iq_2)z_2 + \frac{r_1 + \sqrt{2}ir_2}{c^2 + 2d^2}z_2$$

con

$$N\left(\frac{r_1+\sqrt{2}ir_2}{c^2+2d^2}z_2\right) = N\left(\frac{r_1+\sqrt{2}ir_2}{c^2+2d^2}\right)N(z_2) =$$
$$= \left(\left(\frac{r_1}{c^2+2d^2}\right)^2 + 2\left(\frac{r_2}{c^2+2d^2}\right)^2\right)N(z_2) \leq$$
$$\leq \left(\frac{1}{4}+2\frac{1}{4}\right)N(z_2) = \frac{3}{4}N(z_2) < N(z_2)$$

Dunque $\mathbb{Z}[\sqrt{2}i]$ è un anello euclideo, le unità di $\mathbb{Z}[\sqrt{2}i]$ sono gli elementi di norma 1, per una dimostrazione di questo fatto si veda [A], 4, §9, Proposizione 4.9.9., cioè $a+\sqrt{2}ib$ è invertibile se e solo se $N(a+\sqrt{2}ib) = a^2+2b^2 = 1$ se e solo se $a \in \{\pm 1\}, b = 0$, dunque il gruppo delle unità di $\mathbb{Z}[\sqrt{2}i]$ è $\{\pm 1\}$. □

Facendo riferimento alla proposizione 3.7 osserviamo che la prima stima sul rango (3.17) si può generalizzare anche al caso in cui α, β, γ non siano tutti numeri interi, basta considerare al posto di $\mathbb{Z}$ l'anello $\mathcal{R}$ che si usa per dimostrare il teorema di Mordell.

Nel caso particolare della curva E che stiamo studiando $\alpha, \beta, \gamma \in \mathbb{Z}[\sqrt{2}i]$ e $\mathbb{Z}[\sqrt{2}i]$ è un anello euclideo con lo stesso gruppo delle unità di $\mathbb{Z}$, dunque possiamo prendere $\mathcal{R} = \mathbb{Z}[\sqrt{2}i]$. Se p indica i primi in $\mathbb{Z}[\sqrt{2}i]$,

$$\varphi_\alpha \times \varphi_\beta : E(\mathbb{Q})/2E(\mathbb{Q}) \to \sum_{\pm, p|d} \oplus(\mathbb{Z}_2 \oplus \mathbb{Z}_2)$$

è iniettiva e la prima stima sul rango diventa

$$r \leq 2\,\mathrm{card}\{p \in \mathbb{Z}[\sqrt{2}i] \text{ primo} : p \mid d\}$$

Osserviamo che, essendo il gruppo delle unità di $\mathbb{Z}[\sqrt{2}i]$ lo stesso di $\mathbb{Z}$, con un ragionamento analogo alla dimostrazione della proposizione 3.10 si può ottenere per la curva E la seconda stima sul rango:

$$r \leq n_1 + 2n_2 - 1$$

dove n_1 e n_2 sono definiti nella sezione sulle stime sul rango, a pagina 41. Vediamo in dettaglio la parte che riguarda le coordinate $\pm$:

$$\alpha = 2\sqrt{2}i, \quad \beta = 2\sqrt{2}i, \quad \gamma = 0$$
$$(x-\gamma)(x-\beta)(x-\alpha) = x(x+2\sqrt{2}i)(x-2\sqrt{2}i) = x(x^2+8) = y^2 \geq 0$$

Se $P = (x, y) \in E(\mathbb{Q})$ con $x \neq 0$ allora $x > 0$ perché $x^2 + 8 > 0$ e $x(x^2 + 8) > 0$, inoltre, poiché $(-1)^2 = 1$, si hanno due possibilità per la coppia $x + 2\sqrt{2}i, x - 2\sqrt{2}i$. Dunque se $x \neq 0$ si hanno due casi:

$$(x, x+2\sqrt{2}i, x-2\sqrt{2}i), \qquad (x, -x-2\sqrt{2}i, -x+2\sqrt{2}i)$$

Dunque $(\varphi_\alpha \times \varphi_\beta(P))_\pm \in \{(+,+),(-,-)\} \cong \mathbb{Z}_2$ per ogni scelta di $P \in E(\mathbb{Q})$.

Cerchiamo i primi di $\mathbb{Z}[\sqrt{2}i]$ che dividono il discriminante di $x^3 + 8x$

$$d = (0 - 2\sqrt{2}i)^2(0 - (-2\sqrt{2}i))^2(2\sqrt{2}i - (-2\sqrt{2}i))^2 = 2^{11}.$$

Mostriamo che $\sqrt{2}i$ è un primo in $\mathbb{Z}[\sqrt{2}i]$, infatti se $a, b, c, d \in \mathbb{Z}$ e

$$\sqrt{2}i \mid (a + \sqrt{2}ib)(c + \sqrt{2}id) = ac - 2bd + \sqrt{2}i(bc + ad)$$

allora $\sqrt{2}i \mid ac - 2bd$, ma essendo $a, b, c, d \in \mathbb{Z}$ è equivalente richiedere che $2 \mid ac - 2bd$ ovvero che $2 \mid ac$ in $\mathbb{Z}$, ma 2 è un primo in $\mathbb{Z}$ quindi $2 \mid a$ oppure $2 \mid c$, abbiamo così ottenuto che $\sqrt{2}i \mid a + \sqrt{2}ib$ oppure $c + \sqrt{2}id$ e verificato che $\sqrt{2}i$ è un primo in $\mathbb{Z}[\sqrt{2}i]$.
$d = 2^{11} = -(\sqrt{2}i)^{22}$ per l'unicità della fattorizzazione in primi in $\mathbb{Z}[\sqrt{2}i]$, che è un dominio euclideo, $\sqrt{2}i$ è l'unico primo che divide d ed è un primo **molto cattivo** perché $\sqrt{2}i \mid 0, 2\sqrt{2}i, -2\sqrt{2}i$, tutti gli altri primi sono **buoni**. Allora $n_1 = 0, n_2 = 1$ e $r \leq n_1 + 2n_2 - 1 = 1$. Osserviamo che $P = (1, 3)$ è un punto razionale non di torsione sulla curva E, dunque il rango di E è $r = 1$. Quindi $E(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}_2$, ha un sottogruppo di torsione isomorfo a $\mathbb{Z}_2$ e un sottogruppo ciclico infinito.

Capitolo 6

Numeri congruenti

6.1 Il problema dei numeri congruenti

Il problema dei numeri congruenti nasce dalla seguente osservazione: dato un triangolo rettangolo di cateti a, b e ipotenusa x i numeri $x^2 \pm 2ab$ sono dei quadrati, infatti

$$a^2 + b^2 = x^2 \qquad \Longleftrightarrow \qquad (a \pm b)^2 = x^2 \pm 2ab$$

In un manoscritto arabo anonimo risalente al X secolo d.C. si trova il seguente quesito:

> dato un numero intero n trovare un quadrato x^2 tale che $x^2 \pm n$ siano entrambi dei quadrati.

Una formulazione equivalente richiede che n sia l'area di un triangolo rettangolo con i lati razionali. Un tale numero si dice congruente.

Il problema dei numeri congruenti è legato al problema delle terne pitagoriche che è stato risolto nell'antica Grecia parametrizzando il cerchio unitario con un fascio di rette passanti per un punto del cerchio.

Consideriamo il cerchio unitario $x^2 + y^2 = 1$ e il fascio di rette $x = ty - 1$ per il punto $(-1, 0)$ allora tutti i punti del cerchio a coordinate razionali sono

$$(x, y) = \left(\frac{t^2 - 1}{t^2 + 1}, \frac{2t}{t^2 + 1}\right) \qquad t \in \mathbb{Q}$$

se $t = \frac{a}{b}$, al variare di $a, b \in \mathbb{Z}$ tutti i punti del cerchio a coordinate razionali sono

$$(x, y) = \left(\frac{a^2 - b^2}{a^2 + b^2}, \frac{2ab}{a^2 + b^2}\right)$$

Così tutte le terne pitagoriche sono $a^2 - b^2, 2ab, a^2 + b^2$ al variare di $a, b \in \mathbb{Z}$. In particolare $n = 2(2ab)(a^2 - b^2)$ è un numero congruente per ogni scelta di $a, b \in \mathbb{Z}$.

Osserviamo che un intero n è congruente se e solo se k^2n è un numero congruente con $k \in \mathbb{Z}$, cioè la proprietà di essere un numero congruente si conserva dopo moltiplicazioni o dvisioni per quadrati, infatti n è l'area di un triangolo rettangolo di lati razionali a, b, c allora k^2n è l'area di un triangolo rettangolo di lati ka, kb, kc e viceversa.

Se $a, b, c \in \mathbb{Q}$ sono i lati di un triangolo rettangolo esiste un intero k tale che $ka, kb, kc \in \mathbb{Z}$, dunque n è un numero congruente se e solo se esiste $k \in \mathbb{Z}$ tale che k^2n è l'area di un triangolo rettangolo con i lati interi, cioè $k^2n = 2(2ab)(a^2 - b^2)$ con $a, b \in \mathbb{Z}$.

Abbiamo dunque un metodo per generare tutti i numeri congruenti. Ma non abbiamo risolto il problema del manoscritto arabo, non abbiamo un criterio per stabilire se un numero intero è congruente. A Fermat si deve la dimostrazione che $n = 1$ non è congruente: se 1 fosse un numero congruente allora $(u^2-1)(u^2+1) = w^4$ avrebbe una soluzione razionale non banale, ma $u^4 = w^4 + 1$ non ha soluzioni razionali non banali perché è l'equazione con esponente 4 dell'ultimo teorema di Fermat. Da questo risultato combinato con le osservazioni fatte sopra otteniamo che i quadrati non sono numeri congruenti.

6.2 Numeri congruenti e curve ellittiche

Proposizione 6.1. *Se n è un numero naturale privo di fattori quadrati, allora sono equivalenti:*

i) n è congruente;

ii) esistono tre quadrati razionali in progressione aritmetica di ragione n;

iii) la curva ellittica $y^2 = x^3 - n^2x$ ha almeno un punto razionale $(x, y) \notin \{(-n, 0), (0, 0), (n, 0), \infty\}$.

Dimostrazione. i) $\Rightarrow$ ii) n è un numero congruente, cioè $n = \frac{ab}{2}$ dove a, b, c è una terna pitagorica razionale. Sia $x = \frac{c^2}{4}$ allora

$$\frac{(a-b)^2}{4} = \frac{a^2+b^2-2ab}{4} = \frac{c^2}{4} - \frac{ab}{2} = x - n$$
$$\frac{(a+b)^2}{4} = \frac{a^2+b^2+2ab}{4} = \frac{c^2}{4} + \frac{ab}{2} = x + n$$

dunque $x - n, x, x + n$ sono quadrati razionali.

ii) $\Rightarrow$ i) Se $x-n, x, x+n$ sono quadrati razionali (in progressione aritmetica di ragione n), siano

$$a = \sqrt{x+n} + \sqrt{x-n}, \quad b = \sqrt{x+n} - \sqrt{x-n}, \quad c = 2\sqrt{x}$$

allora a, b, c sono numeri razionali, $a^2+b^2 = x+n+x-n+x+n+x-n = 4x = c^2$ e $\frac{ab}{2} = \frac{x+n-(x-n)}{2} = n$.

ii) $\Rightarrow$ iii) $x(x+n)(x-n) = x^3 - n^2x$ è un quadrato razionale perché $x-n, x, x+n$ lo sono, inoltre $(x-n, x, x+n) \neq (-n, 0, n)$ perché n non ha fattori quadrati, dunque il punto $(x, \sqrt{x^3 - n^2x})$ soddisfa la condizione iii).

iii) $\Rightarrow$ ii) Se $P = (x_P, y_P)$ è un punto razionale di $y^2 = x(x+n)(x-n)$ diverso da $(-n, 0), (0, 0), (n, 0), \infty$ allora P non ha ordine 2, quindi $Q = 2P = (x_{2P}, y_{2P}) \neq \infty$ e $Q \in 2E(\mathbb{Q})$ allora per il teorema 2.1 $x_{2P} - n, x_{2P}, x_{2P} + n$ sono dei quadrati razionali.

□

Abbiamo dunque un criterio per stabilire se un numero n è congruente: un numero naturale privo di fattori quadrati è congruente se e solo se il gruppo dei punti razionali della curva ellittica corrispondente non è $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

I teoremi di Lutz e Nagell ci permettono di determinare per ogni curva ellittica il sottogruppo di torsione, in particolare dal teorema 4.8 otteniamo che se n è un numero naturale privo di fattori quadrati ed E è la curva ellittica di equazione $y^2 = x^3 - n^2x$, allora $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Dunque n è un numero congruente se e solo se la curva ellittica corrispondente ha rango $r \geq 1$.

Il problema di trovare un criterio per stabilire se un numero è congruente si è trasformato nel problema di determinare il rango di una curva ellittica, che non è ancora stato risolto in generale.

In alcuni casi per mostrare che un numero non è congruente è sufficiente considerare le stime sul rango viste alla fine del capitolo sul teorema di Mordell.

Esempio 4. *$n = 1$ non è un numero congruente.*

*Sia E la curva ellittica di equazione $y^2 = x(x+1)(x-1)$, per questa curva $d = (1-0)^2(-1-0)^2(-1-1)^2 = 4$, dunque $p = 2$ è un primo **alquanto cattivo** e tutti gli altri primi sono **buoni**, dalla proposizione 3.10 $n_1 = 1, n_2 = 0$ e $r \leq n_1 + 2n_2 - 1 = 0$ e per la proposizione 4.8 già richiamata sopra $E(\mathbb{Q}) = E(\mathbb{Q})_{tors} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Quindi $n = 1$ non è un numero congruente.*

Ma nella maggior parte dei casi le stime sul rango non sono sufficienti per mostrare la non congruenza di un numero.

Esempio 5. *Consideriamo il caso $n = 2$.*

*Sia E la curva ellittica di equazione $y^2 = x(x+2)(x-2)$, allora $d = (2-0)^2(-2-0)^2(-2-2)^2 = 2^8$, dunque $p = 2$ è un primo **molto cattivo** e tutti gli altri primi sono **buoni**, $n_1 = 0, n_2 = 1$ e per la proposizione 3.10 $r \leq n_1 + 2n_2 - 1 = 1$. Le stime sul rango non bastano per determinare se $n = 2$ è un numero congruente.*

Osserviamo che $y^2 = x^3 - 4x$ è la curva ellittica associata al caso quartico dell'ultimo teorema di Fermat, perciò non ammette punti razionali non

banali, dunque $n = 2$ non è un numero cogruente.

Senza ricorrere all'ultimo teorema di Fermat si può dimostrare che $n = 2$ non è un numero congruente analizzando l'azione di $\varphi_\alpha, \varphi_\beta, \varphi_\gamma$ sulle soluzioni non banali di $y^2 = x(x+2)(x-2)$. Siano $\alpha = -2, \beta = 0, \gamma = 2$, sia $P = (x, y) \notin \{(-2, 0), (0, 0), (2, 0), \infty\}$, allora

$$\varphi_\alpha(P) = (x+2)\mathbb{Q}^{\times 2}, \quad \varphi_\beta(P) = x\mathbb{Q}^{\times 2}, \quad \varphi_\gamma(P) = (x-2)\mathbb{Q}^{\times 2}$$

Dalla proposizione 3.7 $\varphi_\alpha \times \varphi_\beta(E(\mathbb{Q})/2E(\mathbb{Q})) \subseteq \sum_{\pm,2} \oplus(\mathbb{Z}_2 \oplus \mathbb{Z}_2)$ e dalla proposizione 3.6 la mappa $\varphi_\alpha \times \varphi_\beta$ è iniettiva, dunque per conoscere la struttura di gruppo di $E(\mathbb{Q})/2E(\mathbb{Q})$ basta studiarne l'immagine.

Poiché $x(x-2)(x+2) = y^2 \geq 0$ e $x+2 > x > x-2$ le possibili combinazioni di segni per $x+p, x, x-p$ sono $+,+,+$ oppure $+,-,-$. Siano $a, b, c \in \mathbb{Z}$ tali che $2^a \| x-2, 2^b \| x, 2^c \| x+2$, poichè $x(x+p)(x-p)$ è un quadrato abbiamo $a+b+c \equiv 0 \mod 2$, inoltre $2 \mid x+p \iff 2 \mid x-p$ quindi $a \equiv c \mod 2$, dunque le possibili combinazioni sono $(a, b, c) \equiv \{(0, 0, 0), (1, 0, 1)\} \mod 2$.

$$\varphi_\alpha \times \varphi_\beta \times \varphi_\gamma(-2, 0) = 2^3\mathbb{Q}^{\times 2} \times -2\mathbb{Q}^{\times 2} \times -2^2\mathbb{Q}^{\times 2} = 2\mathbb{Q}^{\times 2} \times -2\mathbb{Q}^{\times 2} \times -\mathbb{Q}^{\times 2}$$
$$\varphi_\alpha \times \varphi_\beta \times \varphi_\gamma(0, 0) = 2\mathbb{Q}^{\times 2} \times -2^2\mathbb{Q}^{\times 2} \times -2\mathbb{Q}^{\times 2} = 2\mathbb{Q}^{\times 2} \times -\mathbb{Q}^{\times 2} \times -2\mathbb{Q}^{\times 2}$$
$$\varphi_\alpha \times \varphi_\beta \times \varphi_\gamma(2, 0) = 2^2\mathbb{Q}^{\times 2} \times 2\mathbb{Q}^{\times 2} \times 2^3\mathbb{Q}^{\times 2} = 2\mathbb{Q}^{\times 2} \times \mathbb{Q}^{\times 2} \times 2\mathbb{Q}^{\times 2}$$

Dunque esiste $Q \in \{(-2, 0), (0, 0), (2, 0), \infty\}$ tale che le coordinate corrispondenti a 2 delle immagini di Q e P tramite $\varphi_\alpha \times \varphi_\beta \times \varphi_\gamma$ siano uguali. Poichè dalla proposizione 3.5 $\varphi_\alpha, \varphi_\beta, \varphi_\gamma$ sono omomorfismi, la coordinata corrispondente a 2 di $\varphi_\alpha \times \varphi_\beta \times \varphi_\gamma(P+Q)$ è $(0, 0, 0)$. Se $x = x(P+Q)$ e con $\square$ indichiamo che il numero corrispondente è un quadrato, ci sono due possibilità:

$$(x+2, x, x-2) \in \{(\square, \square, \square), (\square, -\square, -\square)\}$$

Supponiamo per assurdo che $(x+2, x, x-2) = (\square, -\square, -\square)$, allora $2 = (x+2) - x = \square + \square$. Osserviamo che se il denominatore di x è pari allora i numeratori dei due quadrati sono dispari ed essendo x un quadrato eliminando i denominatori otteniamo $\square + \square \equiv 0 \mod 8$, dove questi due quadrati sono interi e dispari, ma ciò è impossibile. Infatti se $a^2 + b^2 = 8m = (2^2 + 2^2)m$ allora m è una somma di quadrati, $m = c^2 + d^2$, dunque

$$a^2 + b^2 = |2 + 2i|^2 |c + id|^2 = |(2 + 2i)(c + id)|^2 = (2c - 2d)^2 + (2d + 2c)^2$$

quindi a, b sono entrambi pari.
Se invece il denominatore di x è dispari consideriamo $2 = x - (x-2) = -\square + \square$, eliminando i denominatori otteniamo $2m^2 = -\square + \square \mod 8$ con m dispari, dunque $m^2 \equiv 1 \mod 8$ e $2 \equiv -\square + \square \mod 8$, ma ciò è impossibile.

Infatti se avessimo $-a^2+b^2 = 2+8k$ *con* $a,b,k \in \mathbb{Z}$, *allora* $2 \mid b^2-a^2 = (b+a)(b-a)$ *e* $4 \nmid b^2-a^2$ *contro il fatto che* $2 \mid b+a$ *se e solo se* $2 \mid b-a$.

Abbiamo mostrato che se $x = x(P+Q)$ *allora* $(x+2, x, x-2) = (\square, \square, \square)$, *cioè* $P+Q \in \ker(\varphi_\alpha \times \varphi_\beta) = 2E(\mathbb{Q})$. *Allora* $P+2E(\mathbb{Q}) = -Q+2E(\mathbb{Q}) = Q+2E(\mathbb{Q})$ *perché* $Q = -Q$ *e quindi* $E(\mathbb{Q})/2E(\mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ *e* $\operatorname{card}(E(\mathbb{Q})/2E(\mathbb{Q})) = 2^{r+2} = 2^2$, *abbiamo così dimostrato che* $r = 0$ *e che* $n = 2$ *non è un numero congruente.*

La proposizione 3.11, con ragionamenti analoghi, permette di concludere che ogni primo dispari $p \equiv 3 \mod 8$ non è un numero congruente.

Vediamo ora come caratterizzare i numeri primi $p \equiv 5 \mod 8$ che sono congruenti.

Proposizione 6.2. *Se* $p \equiv 5 \mod 8$ *è un numero primo,* p *è un numero congruente se e solo se l'equazione* $4s^4+r^4 = pn^2$ *ammette soluzioni razionali non banali.*

Dimostrazione. Sia $p \equiv 5 \mod 8$ un numero primo congruente, per la proposizione 3.11 la curva ellittica corrispondente $y^2 = x^3 - p^2x$ ha rango $r = 1$, dunque esiste un punto $P = (x, y) \in E(\mathbb{Q})$ tale che $(x+p, x, x-p) = (\square, -\square, -\square)$. Siano $x+p = a^2, x = -b^2, x-p = -c^2$ con $a, b, c \in \mathbb{Q}$), poiché $(x+p)+(x-p) = 2x$ abbiamo $a^2-c^2 = -2b^2$, ovvero $a^2 = c^2-2b^2$. Siano

$$u = \frac{c}{a}, \quad v = \frac{b}{a} \quad \text{allora} \quad 1 = u^2-2v^2$$

possiamo parametrizzare la conica con il fascio di rette $u = tv+1$ passanti per il punto $(1,0)$:

$$\begin{aligned} 1 &= (tv+1)^2-2v^2 = (t^2-2)v^2+2tv+1 \\ \Rightarrow \quad v &= \frac{2t}{2-t^2} \quad \Rightarrow \quad u = \frac{2t^2}{2-t^2}+1 = \frac{2+t^2}{2-t^2} \end{aligned}$$

tutti i punti razionali affini della conica sono

$$(u,v) = \left(\frac{2t}{2-t^2}, \frac{2+t^2}{2-t^2}\right), \qquad t \in \mathbb{Q}.$$

Sia $t = \frac{r}{s}$ con $r, s \in \mathbb{Z}$ e $\operatorname{MCD}(r,s) = 1$, allora

$$\begin{aligned} \left(\frac{b}{a}, \frac{c}{a}\right) = (v,u) &= \left(\frac{2rs}{2s^2-r^2}, \frac{2s^2+r^2}{2s^2-r^2}\right) \\ \Rightarrow \quad a = (2s^2-r^2)\lambda, &\quad b = 2rs\lambda, \quad c = (2s^2+r^2)\lambda \end{aligned}$$

con $\lambda \in \mathbb{Q}$, se $\lambda = \frac{m}{n}$ con $m, n \in \mathbb{Z}$ e $\operatorname{MCD}(m,n) = 1$, allora $m \mid na, nb$, ma $\operatorname{MCD}(m,n) = 1$, dunque $m \mid a, b$

$$m^2 \mid a^2+b^2 = (x+p)-x = p \quad \Rightarrow \quad m \in \{\pm 1\}$$

Supponiamo che $m = 1$, allora $\lambda = \frac{1}{n}$ con $n \in \mathbb{Z}$ dunque

$$p = a^2 + b^2 = (4s^4 + r^4)\lambda^2 = \frac{4s^4 + r^4}{n^2} \quad \Rightarrow \quad pn^2 = 4s^4 + r^4$$

Abbiamo mostrato che se p è congruente allora $4s^4 + r^4 = pn^2$ ha soluzioni razionali non banali.

Viceversa, se $(r, s, n) \neq (0, 0, 0)$ è una soluzione di $4s^4 + r^4 = pn^2$, siano

$$a = \frac{2s^2 - r^2}{n}, \quad b = \frac{2rs}{n}, \quad c = \frac{2s^2 + r^2}{n}$$

allora

$$c^2 - 2b^2 = \frac{(2s^2 + r^2)^2}{n^2} - 2\frac{4r^2s^2}{n^2} = \frac{(2s^2 - r^2)^2}{n^2} = a^2$$

e

$$a^2 + b^2 = \frac{(2s^2 - r^2)^2}{n^2} + \frac{4r^2s^2}{n^2} = \frac{4s^4 + r^4}{n^2} = p$$

Sia $x = -b^2 \in \mathbb{Q}$, allora

$$x + p = -b^2 + (a^2 + b^2) = a^2$$
$$x - p = -b^2 - (a^2 + b^2) = -a^2 - 2b^2 = -c^2$$

inoltre $y^2 = x(x + p)(x - p) = a^2b^2c^2$, sia $y = abc \in \mathbb{Q}$, allora $P = (x, y) \in E(\mathbb{Q})$ e non è un punto di 2-torsione, dunque p è un numero congruente. □

Esempio 6. *Mostriamo che $p = 5$ è un numero congruente usando il criterio offerto dalla proposizione appena dimostrata.*

Una soluzione non banale di $4s^4 + r^4 = 5n^2$ è $(r, s, n) = (1, 1, 1)$, allora $b = \frac{2rs}{n} = 2$, $x = -b^2 = -4$ e $y^2 = x^3 - 25x = 36$, dunque $(-4, 6)$ è un punto razionale, non di torsione, su $y^2 = x^3 - 25x$ e 5 è un numero congruente.

Esempio 7. *Mostriamo che $p = 53$ è un numero congruente.*

$53 \equiv 5 \mod 8$, *per la proposizione 6.2 $p = 53$ è un numero congruente se e solo se l'equazione $4s^4 + r^4 = 53n^2$ ha soluzioni razionali non banali. La riscriviamo così $4(s^2)^2 + (r^2)^2 = 53n^2$ e consideriamo l'equazione affine $j^2 + 4k^2 = 53$, è una conica con un punto razionale $(j, k) = (7, 1)$ possiamo parametrizzarla con il fascio di rette $k = t(j - 7) + 1$ passante per il punto $(7, 1)$:*

$$53 = j^2 + 4(t(j - 7) + 1)^2 = j^2 + 4t^2(j - 7)^2 + 4 + 8t(j - 7)$$
$$\iff \quad j^2 - 49 + 4t^2(j - 7)^2 + 8t(j - 7) = 0$$
$$\iff \quad (j - 7)(j + 7 + 4t^2(j - 7) + 8t) = 0$$
$$\Rightarrow \quad j = \frac{28t^2 - 8t - 7}{4t^2 + 1}, \quad k = t\frac{-8t - 14}{4t^2 + 1} + 1 = \frac{-4t^2 - 14t + 1}{4t^2 + 1}$$

sia $t = 2\frac{d}{e}$ *con* $d, e \in \mathbb{Z}$ *e* $\mathrm{MCD}(d, e) = 1$ *allora*

$$(j, k) = \left(\frac{28t^2 - 8t - 7}{4t^2 + 1}, \frac{-4t^2 - 14t + 1}{4t^2 + 1}\right) = \left(\frac{7d^2 - 4de - 7e^2}{d^2 + e^2}, \frac{-d^2 - 7de + e^2}{d^2 + e^2}\right)$$

e

$$r^2 = (7d^2 - 4de - 7e^2)\mu, \quad s^2 = (-d^2 - 7de + e^2)\mu, \quad n = (d^2 + e^2)\mu$$

con $\mu \in \mathbb{Q}$, *affinché* $\mathrm{MCD}(r, s) = 1$ *dev'essere* $\mu = \frac{1}{h}$ *con* $h \in \mathbb{Z}$, *dunque*

$$h \mid hr^2 + 7hs^2 = 7d^2 - 4de - 7e^2 + 7(-d^2 - 7de + e^2) = -53de$$

e $h \mid hn = d^2 + e^2$, *poiché* $\mathrm{MCD}(d, e) = 1$ *ne risulta che* $h = 1$ *oppure* $h = 53$. *Supponiamo che sia* $h = 1$, *allora* $\mu = 1$ *e* $s^2 = -d^2 - 7de + e^2$, *consideriamo l'equazione affine* $-d'^2 - 7d'e' + e'^2 = 1$, *è una conica con un punto razionale,* $(d', e') = (0, 1)$, *la parametrizziamo con il fascio di rette* $e' = td' + 1$*:*

$$1 = -d'^2 - 7d'(td' + 1) + (td' + 1)^2 = -d'^2 - 7td'^2 - 7d' + t^2d'^2 + 2td' + 1$$

$$\Rightarrow \quad d' = \frac{2t - 7}{-t^2 + 7t + 1}, \quad e' = \frac{t^2 + 1}{-t^2 + 7t + 1}$$

sia $t = \frac{u}{v}$ *con* $u, v \in \mathbb{Z}$ *e* $\mathrm{MCD}(u, v) = 1$, *allora*

$$d = (2uv - v^2)\nu, \quad e = (u^2 + v^2)\nu, \quad s = (-u^2 + tuv + v^2)\nu$$

con $\nu \in \mathbb{Q}$, *poiché* $\mathrm{MCD}(d, e) = 1$ *dev'essere* $\nu = \frac{1}{l}$ *con* $l \in \mathbb{Z}$, *inoltre*

$$l \mid 2ld + 7le + 7ls = 2(2uv - v^2) + 7(u^2 + v^2) + 7(-u^2 + tuv + v^2) = 53uv$$

e $l \mid le = u^2 + v^2$, *ma* $\mathrm{MCD}(u, v) = 1$ *quindi* $l = 1$ *oppure* $l = 53$, *cerchiamo soluzioni intere* (u, v) *con* $l = 1$, *cioè* $\nu = 1$.

Per trovare una coppia di numeri interi (u, v) *tali che*

$$d = 2uv - v^2, \quad e = u^2 + v^2, \quad s = -u^2 + tuv + v^2$$

e $r^2 = 7d^2 - 4de - 7e^2$ *con* $s \in \mathbb{Z}$ *possiamo, per esempio, implementare il seguente algoritmo nel il programma di calcolo Mathematica7:*

```
Module[{t, u, v, d, e, R, k, f},
 t = Flatten[Table[{i, j}, {i, 1, 150}, {j, 1, 150}], 1];
 d = 2 u v - 7 v^2;
 e = u^2 + v^2;
 R = (Abs[7 d^2 - 4 d e - 7 e^2])^(1/2);
 u = 1; v = 1; k = 2;
 While[! IntegerQ[R] && u < 151 && v < 151, {}; {k++, u = t[[k, 1]],
   v = t[[k, 2]]}];
 {u, v, R}]
```

facendo variare u e v tra 1 e 150 l'algoritmo dà come risultato la prima coppia (u, v) tale che $7d^2 - 4de - 7e^2 = r^2 \in \mathbb{Z}^2$, l'output dell'algoritmo è $(u, v) = (10, 3)$ che corrisponde a $(r, s, n) = (286, 119, 11890)$. Abbiamo così trovato una soluzione razionale non banale di $4s^4 + r^4 = 53n^2$, la proposizione 6.2 permette di concludere che 53 è un numero congruente.

Esempio 8. *Mostriamo che $p = 101 \equiv 5 \mod 8$ è un numero congruente.*

$101 \equiv 5 \mod 8$*, per poter usare la proposizione 6.2 cerchiamo soluzioni non banali dell'equazione $r^4 + 4s^4 = 101n^2$, con $\mathrm{MCD}(r, s) = 1$. Consideriamo l'equazione affine $j^2 + 4k^2 = 101$, è una conica con un punto razionale $(j, k) = (1, 5)$, possiamo parametrizzarla con il fascio di rette $j = t(k-5)+1$:*

$$\begin{aligned} & (t(k-5)+1)^2 + 4k^2 = 101 \\ \iff \quad & t^2(k-5)^2 + 2t(k-5) + 1 + 4k^2 = 101 \\ \iff \quad & (k-5)(t^2(k-5) + 2t + 4(k+5)) = 0 \\ \Rightarrow k = \frac{5t^2 - 2t - 20}{t^2+4} \qquad & j = \frac{-t^2 - 40t + 4}{t^2+4} \end{aligned}$$

sia $t = \frac{d}{e}$ con $d, e \in \mathbb{Z}$ e $\mathrm{MCD}(d, e) = 1$ allora

$$r^2 = (-d^2 - 40de + 4e^2)\lambda, \quad s^2 = (5d^2 - 2de - 20e^2)\lambda, \quad n = (d^2 + 4e^2)\lambda$$

poiché $\mathrm{MCD}(r, s) = 1$ dev'essere $\lambda = \frac{1}{h}$ con $h \in \mathbb{Z}$,

$$\begin{aligned} & h \mid 5hr^2 + hs^2 = 5(-d^2 - 40de + 4e^2) + 5d^2 - 2de - 20e^2 = -202de, \\ & h \mid hn = 4e^2 + d^2, \quad \mathrm{MCD}(d, e) = 1 \qquad \Rightarrow \qquad h \in \{1, 2, 101, 202\} \end{aligned}$$

Se $h = 1$ allora $s^2 = 5d^2 - 2de - 20e^2$, consideriamo l'equazione affine $s'^2 = 5d'^2 - 2d' - 20$ che è una conica con un punto razionale $(d', s') = (-2, 2)$, la parametrizziamo con il fascio di rette $s' = t(d' + 2) + 2$:

$$\begin{aligned} & (t(d'+2)+2)^2 = 5d'^2 - 2d' - 20 \\ \iff \quad & t^2(d'+2)^2 + 4t(d'+2) + 4 + 2d' - 5d'^2 + 20 = 0 \\ \iff \quad & (d'+2)(t^2(d'+2) + 4t + 2 - 5(d'-2) = 0 \\ \Rightarrow \quad & d' = 2\frac{t^2 + 2t + 6}{5 - t^2} \qquad s' = 2\frac{t^2 + 11t + 5}{5 - t^2} \end{aligned}$$

sia $t = \frac{u}{v}$ con $u, v \in \mathbb{Z}$ e $\mathrm{MCD}(u, v) = 1$ allora

$$d = 2(u^2 + 2uv + 6v^2)\mu, \quad e = (5v^2 - u^2)\mu, \quad s = 2(u^2 + 11uv + 5v^2)\mu$$

poiché $\mathrm{MCD}(d, e) = 1$ dev'essere $\mu = \frac{1}{l}$ con $l \in \mathbb{Z}$,

$$\begin{aligned} & l \mid 11ld + 18le - 2ls = \\ & \qquad = 22(u^2 + 2uv + 6v^2) + 18(5v^2 - u^2) - 4(u^2 + 11uv + 5v^2) = 202v^2, \\ & l \mid le = 5v^2 - u^2, \quad \mathrm{MCD}(u, v) = 1 \qquad \Rightarrow \qquad l \in \{1, 2, 101, 202\} \end{aligned}$$

Sia $l = 1$*, cerchiamo soluzioni intere* (u, v) *tali che* $-d^2 - 40de + 4e^2 = r^2 \in \mathbb{Z}^2$*. Implementando il seguente algoritmo con il programma di calcolo Mathematica7:*

```
Module[{t, u, v, d, e, R, k, f},
 t = Flatten[Table[{i, j}, {i, 1, 150}, {j, 1, 150}], 1];
 d = 2 (u^2 + 2 u v + 6 v^2);
 e = 5 v^2 - u^2;
 R = (Abs[-d^2 - 40 d e + 4 e^2])^(1/2);
 u = 1; v = 1; k = 2;
 While[! IntegerQ[R] && u < 151 && v < 151, {}; {k++, u = t[[k, 1]],
   v = t[[k, 2]]}];
 {u, v, R}]
```

otteniamo che la coppia $(u, v) = (7, 3)$ *ha le proprietà richieste e corrisponde alla soluzione razionale non banale* $(r, s, n) = (194, 650, 84164)$ *di* $r^4 + 4s^4 = 101n^2$*. Per la proposizione 6.2 possiamo concludere che 101 è un numero congruente.*

Appendice A

Sul problema di Fermat a Mersenne

Di seguito sono riportati i calcoli eseguiti con il programma *Mathematica7* per mostrare la corrispondenza tra il metodo di discesa usato da Fermat nell'analisi della quartica $2b^4 - a^4 = e^2$ e la duplicazione dei punti sulla curva ellittica $y^2 = x^3 + 8x$ ad essa associata.

Problema di Fermat a Mersenne

Il problema di Fermat a Mersenne consiste nel trovare una terna pitagorica di interi positivi x, y, z tali che x+y e z siano dei quadrati.
Cioè $x^2 + y^2 = z^2,\ x + y = a^2,\ z = b^2$, ponendo $e = x - y$, si ottiene che risolvere il problema di Fermat a Mersenne sugli interi equivale a trovare radici intere dell'equazione $2\,b^4 - a^4 = e^2$.

Metodo di discesa di Fermat.

0. Definisco e in funzione di x, y
1. Parametrizzo il cerchio $x^2 + y^2 = z^2$ con i parametri omogenei m, n
2. Osservo che $m^2 + n^2 = z = b^2$, dunque parametrizzo questo cerchio con i parametri omogenei r, s
3. Osservo che $a^2 = x + y = m^2 - n^2 + 2\,m\,n = (m + n)^2 - 2\,n^2$, parametrizzo la conica che si ottiene ponendo $\alpha = \frac{m+n}{a},\ \beta = \frac{n}{a}$ e cioè $\alpha^2 - 2\,\beta^2 = 1$ con il fascio di rette $\alpha = t\,\beta + 1$, scrivo α e β in funzione di t, omogeneizzo con il parametro u, da queste espressioni ricavo m, n, a in funzione dei parametri (interi coprimi) t, u
4. Osservo che $2\,r\,s = n = 2\,t\,u$, dunque $\frac{r}{t} = \frac{u}{s} = \frac{d}{c}$ con d, c interi coprimi, allora pongo $t = k\,c,\ u = l\,d,\ r = k\,d,\ s = l\,c$, poichè $r^2 - s^2 = m = (u - t)^2 + u^2$, sostituisco r, s, t, u in funzione di c, d, k, l e ottengo $\left(2\,d^2 + c^2\right)\left(\frac{l}{k}\right)^2 - 2\,d\,c\,\frac{l}{k} + c^2 - d^2 = 0$ che ha soluzioni razionali $\frac{l}{k}$ se e solo se il discriminante dell'equazione è un quadrato, cioè $2\,d^4 - c^4 = f^2$, in tal caso si ha $\frac{l}{k} = \frac{d\,c - f}{2\,d^2 + c^2}$, non è restrittivo considerare f invece che +,- il suo modulo perchè sia f che -f danno punti di $2\,d^4 - c^4 = f^2$, inoltre non è restrittivo considerare $l = d\,c - f$ e $k = 2\,d^2 + c^2$, da queste formule si ricavano t, u, r, s in funzione di c, d, f.

In[1]:=
```
e0[x_, y_] := x - y;
x1[m_, n_] := m^2 - n^2;
y1[m_, n_] := 2 m n;
z1[m_, n_] := m^2 + n^2;
m2[r_, s_] := r^2 - s^2;
n2[r_, s_] := 2 r s;
b2[r_, s_] := r^2 + s^2;
m3[t_, u_] := (u - t)^2 + u^2;
n3[t_, u_] := 2 u t;
a3[t_, u_] := -(2 u^2 - t^2);
t4[c_, d_, f_] := (2 d^2 + c^2) c;
u4[c_, d_, f_] := (d c - f) d;
r4[c_, d_, f_] := (2 d^2 + c^2) d;
s4[c_, d_, f_] := (d c - f) c;
```

Equazioni

Dove $\beta = \frac{b}{a}$ e $\epsilon = \frac{e}{a^2}$

In[15]:=
```
Quart[a_, b_, e_] := 2 b^4 - a^4 - e^2;
quart[β_, ϵ_] := 2 β^4 - 1 - ϵ^2;
Cub[x_, y_] := y^2 - x^3 - 8 x;
```

Cambi di variabili,

In[18]:=
```
βo[x_, y_] := (y - 2 x - 8)/(y - 4 x + 8);
ϵo[x_, y_] := (y^2 - 24 x^2 + 48 y - 16 x - 64)/(y - 4 x + 8)^2;
```

In[20]:=
$$xo[\beta\_, \epsilon\_] := \frac{2\left(\epsilon + 2\beta^2 - 1\right)}{(\beta - 1)^2};$$
$$yo[\beta\_, \epsilon\_] := \frac{4\left((2\beta - 1)\epsilon + 2\beta^3 - 1\right)}{(\beta - 1)^3};$$

Controlli

1. I cambi di variabili definiti sopra sono uno l'inverso dell'altro.

In[22]:=
```
βo[xo[βo, ϵo], yo[βo, ϵo]] // Simplify
```

Out[22]=
$$\beta o$$

In[23]:=
```
ϵo[xo[βo, ϵo], yo[βo, ϵo]] // Expand // Simplify
```

Out[23]=
$$\frac{1 - 2\beta o^4 + 5\epsilon o - 8\beta o\,\epsilon o + 2\beta o^2\,\epsilon o}{5 - 8\beta o + 2\beta o^2 - \epsilon o}$$

(osservo che $1 - 2\beta o^4 = -\epsilon o^2$, dunque basta raccogliere ϵo al numeratore e semplificare)

In[24]:=
```
xo[βo[xo, yo], ϵo[xo, yo]] // Simplify
```

Out[24]=
$$\frac{56\,xo - 16\,xo^2 + yo^2}{(-8 + xo)^2}$$

(osservo che $yo^2 = xo^3 + 8\,xo$, dunque basta raccogliere xo al numeratore e semplificare)

In[25]:=
```
yo[βo[xo, yo], ϵo[xo, yo]] // Simplify
```

Out[25]=
$$\frac{24\,xo^3 - 24\,xo^2\,yo + 8\,xo\,(24 + 23\,yo) + yo\left(-512 - 24\,yo + yo^2\right)}{(-8 + xo)^3}$$

(osservo che $xo^3 + 8\,xo = yo^2$, con opportune sostituzioni e raccoglimenti si ottiene il risultato voluto)

2. I cambi di variabili definiti sopra trasformano punti della quart in punti della Cub e viceversa.

In[26]:=
```
quart[βo[x, y], ϵo[x, y]] == 0 // FullSimplify
```

Out[26]=
$$\frac{(-56 + 25\,x - 6\,y)\left(8\,x + x^3 - y^2\right)}{-8 + 4\,x - y} == 0$$

(se il punto di coordinate x, y sta sulla cubica si ha $y^2 = x^3 + 8\,x$ e dunque il suo trasformato sta sulla quartica)

In[27]:=
```
Cub[xo[β, ϵ], yo[β, ϵ]] == 0 // FullSimplify
```

Out[27]=
$$\frac{(5 + 2\,(-4+\beta)\,\beta - \epsilon)\,\left(-1 + 2\,\beta^4 - \epsilon^2\right)}{-1+\beta} == 0$$

(se il punto β, ϵ sta sulla quartica si ha $2\,\beta^4 - 1 = \epsilon^2$ e dunque il suo trasformato sta sulla cubica)

Duplicazione dei punti della cubica

Indico con x2, y2 le coordinate del punto P2 che è il doppio del punto P di coordinate x, y secondo la somma di Poincarè.

In[28]:=
```
x2[x_, y_] := (x^2 - 8)^2 / (4 x (x^2 + 8));
y2[x_, y_] := (x^2 - 8) (x^4 + 48 x^2 + 64) / (8 x y (x^2 + 8));
```

Controllo

Le formule di duplicazione definite sopra trasformano punti della cubica in punti della cubica.

In[30]:=
```
Cub[x2[x, y], y2[x, y]] == 0 // Simplify
```

Out[30]=
$$\frac{\left(-512 - 320\,x^2 + 40\,x^4 + x^6\right)\,\left(8\,x + x^3 - y^2\right)}{\left(8\,x + x^3\right)\,y} == 0$$

(se il punto x, y sta sulla cubica si ha $y^2 = x^3 + 8\,x$ e dunque il suo doppio sta ancora sulla cubica)

Corrispondenza tra la duplicazione dei punti sulla cubica e il metodo di duplicazione di Fermat sulla quartica.

Dati c, d, f interi che soddisfano all'equazione $2\,d^4 - c^4 = f^2$, siano x, y le coordinate del punto P corrispondente sulla cubica (tramite i cambi di coordinate birazionali) e sia P2 il doppio del punto P secondo la legge di gruppo di Poincarè (uso le formule di duplicazione della cubica), siano a, b, e le coordinate del punto della quartica $2\,b^4 - a^4 = e^2$ che si ottengono risalendo il metodo discesa di Fermat e sia Q il punto della cubica corrispondente alla terna a, b, e (tramite i cambi di coordinate birazionali).

In[31]:=
```
x = xo[d/c, f/c^2];
y = yo[d/c, f/c^2];
a = a3[t4[c, d, f], u4[c, d, f]];
b = b2[r4[c, d, f], s4[c, d, f]];
e = e0[x1[m3[t4[c, d, f], u4[c, d, f]], n3[t4[c, d, f], u4[c, d, f]]],
   y1[m3[t4[c, d, f], u4[c, d, f]], n3[t4[c, d, f], u4[c, d, f]]]];
P = {x, y} // Simplify;
P2 = {x2[x, y], y2[x, y]} // Expand // FullSimplify;
Q = {xo[b/a, e/a^2], yo[b/a, e/a^2]} // FullSimplify;
```

Mostro che P2 e Q sono lo stesso punto della cubica (ovvero che hanno le stesse coordinate). Le uguaglianze si ottengono osservando che $2\,d^4 - c^4 = f^2$.

Prima coordinata.

In[39]:=
```
P2[[1]] - Q[[1]] == 0 // Expand // FullSimplify
```

Out[39]=
$$\Big(\big(c^4 - 2\,d^4 + f^2\big)\,\big(c^{16} - 16\,c^{15}\,d + 4\,c^{14}\,\big(d^2 + f\big) + 4\,c^{13}\,\big(28\,d^3 + 17\,d\,f\big) - c^{12}\,\big(194\,d^4 + 280\,d^2\,f + f^2\big) + 16\,c^{11}\,\big(8\,d^5 + 25\,d^3\,f - 5\,d\,f^2\big) - 64\,c^9\,\big(8\,d^7 - 3\,d^5\,f + 22\,d^3\,f^2\big) + 8\,c^{10}\,\big(9\,d^6 - 28\,d^4\,f + 62\,d^2\,f^2 - 2\,f^3\big) + c^8\,\big(1140\,d^8 - 928\,d^6\,f + 1896\,d^4\,f^2 - 80\,d^2\,f^3 + 23\,f^4\big) - 16\,c^7\,\big(132\,d^9 - 92\,d^7\,f + 78\,d^5\,f^2 - 48\,d^3\,f^3 - d\,f^4\big) + 4\,c^6\,\big(876\,d^{10} - 220\,d^8\,f + 214\,d^6\,f^2 - 400\,d^4\,f^3 - 34\,d^2\,f^4 - 3\,f^5\big) - 16\,c^3\,d^3\,\big(400\,d^{10} + 396\,d^8\,f + 248\,d^6\,f^2 + 8\,d^4\,f^3 + 8\,d^2\,f^4 + f^5\big) - 16\,c\,d^5\,\big(176\,d^{10} + 172\,d^8\,f + 144\,d^6\,f^2 + 56\,d^4\,f^3 + 12\,d^2\,f^4 + f^5\big) - 4\,c^5\,\big(1296\,d^{11} + 204\,d^9\,f + 288\,d^7\,f^2 - 424\,d^5\,f^3 - 44\,d^3\,f^4 - 3\,d\,f^5\big) + c^4\,\big(6568\,d^{12} + 4128\,d^{10}\,f + 2140\,d^8\,f^2 - 1088\,d^6\,f^3 - 74\,d^4\,f^4 - 16\,d^2\,f^5 + f^6\big) + 4\,c^2\,d^2\,\big(1240\,d^{12} + 1296\,d^{10}\,f + 1060\,d^8\,f^2 + 272\,d^6\,f^3 + 46\,d^4\,f^4 + 4\,d^2\,f^5 + f^6\big) + 4\,d^4\,\big(184\,d^{12} + 192\,d^{10}\,f + 140\,d^8\,f^2 + 64\,d^6\,f^3 + 26\,d^4\,f^4 + 8\,d^2\,f^5 + f^6\big)\big)\Big) \Big/ \Big((c - d)\,\big(c^2 + 2\,d^2\big)\,\big(c^2 - 2\,d^2 - f\big)\,\big(c^4 - 2\,d^4 + 2\,c\,d\,f - f^2\big)\,\big(3\,c^4 - 8\,c^3\,d - 8\,c\,d^3 + 6\,d^4 + c^2\,\big(8\,d^2 - 2\,f\big) + 4\,d^2\,f + f^2\big)\Big) == 0$$

Seconda coordinata.

```
In[40]:= P2[[2]] - Q[[2]] == 0 // Expand // FullSimplify
```

Out[40]=

$$\Big((c^4 - 2\,d^4 + f^2)\,\Big(79\,c^{26} - 328\,c^{25}\,d + 554\,c^{24}\,d^2 - 440\,c^{23}\,d^3 - 658\,c^{22}\,d^4 + 2928\,c^{21}\,d^5 - 4588\,c^{20}\,d^6 + 3680\,c^{19}\,d^7 + 4592\,c^{18}\,d^8 - 24\,448\,c^{17}\,d^9 + 47\,392\,c^{16}\,d^{10} - 65\,728\,c^{15}\,d^{11} + 70\,448\,c^{14}\,d^{12} - 34\,432\,c^{13}\,d^{13} - 52\,192\,c^{12}\,d^{14} + 210\,176\,c^{11}\,d^{15} - 495\,120\,c^{10}\,d^{16} + 886\,656\,c^9\,d^{17} - 1\,319\,264\,c^8\,d^{18} + 1\,696\,384\,c^7\,d^{19} - 1\,825\,184\,c^6\,d^{20} + 1\,639\,168\,c^5\,d^{21} - 1\,234\,368\,c^4\,d^{22} + 736\,768\,c^3\,d^{23} - 331\,392\,c^2\,d^{24} + 109\,568\,c\,d^{25} - 20\,224\,d^{26} - 2\,(c-d)\,\Big(35\,c^{23} - 122\,c^{22}\,d + 42\,c^{21}\,d^2 + 1596\,c^{20}\,d^3 - 6580\,c^{19}\,d^4 + 14\,152\,c^{18}\,d^5 - 21\,832\,c^{17}\,d^6 + 24\,416\,c^{16}\,d^7 - 14\,712\,c^{15}\,d^8 - 7248\,c^{14}\,d^9 + 27\,984\,c^{13}\,d^{10} - 38\,848\,c^{12}\,d^{11} + 51\,712\,c^{11}\,d^{12} - 98\,368\,c^{10}\,d^{13} + 239\,936\,c^9\,d^{14} - 479\,296\,c^8\,d^{15} + 747\,824\,c^7\,d^{16} - 939\,552\,c^6\,d^{17} + 925\,472\,c^5\,d^{18} - 735\,424\,c^4\,d^{19} + 464\,960\,c^3\,d^{20} - 210\,304\,c^2\,d^{21} + 74\,112\,c\,d^{22} - 19\,712\,d^{23}\Big)\,f - \Big(133\,c^{22} - 492\,c^{21}\,d + 922\,c^{20}\,d^2 - 3584\,c^{19}\,d^3 + 18\,148\,c^{18}\,d^4 - 63\,224\,c^{17}\,d^5 + 144\,272\,c^{16}\,d^6 - 238\,720\,c^{15}\,d^7 + 303\,704\,c^{14}\,d^8 - 261\,520\,c^{13}\,d^9 + 103\,136\,c^{12}\,d^{10} + 5888\,c^{11}\,d^{11} + 187\,968\,c^{10}\,d^{12} - 881\,696\,c^9\,d^{13} + 1\,978\,528\,c^8\,d^{14} - 3\,041\,792\,c^7\,d^{15} + 3\,517\,136\,c^6\,d^{16} - 3\,139\,072\,c^5\,d^{17} + 2\,204\,384\,c^4\,d^{18} - 1\,201\,152\,c^3\,d^{19} + 483\,264\,c^2\,d^{20} - 145\,920\,c\,d^{21} + 29\,824\,d^{22}\Big)\,f^2 + 4\,(c-d)\,\Big(39\,c^{19} - 130\,c^{18}\,d + 220\,c^{17}\,d^2 + 460\,c^{16}\,d^3 - 2574\,c^{15}\,d^4 + 4396\,c^{14}\,d^5 - 3212\,c^{13}\,d^6 - 6520\,c^{12}\,d^7 + 24\,828\,c^{11}\,d^8 - 34\,472\,c^{10}\,d^9 + 4944\,c^9\,d^{10} + 78\,768\,c^8\,d^{11} - 189\,288\,c^7\,d^{12} + 277\,392\,c^6\,d^{13} - 283\,056\,c^5\,d^{14} + 204\,384\,c^4\,d^{15} - 104\,480\,c^3\,d^{16} + 30\,784\,c^2\,d^{17} - 3648\,c\,d^{18} + 1408\,d^{19}\Big)\,f^3 + 2\,\Big(-13\,c^{18} + 178\,c^{17}\,d - 1056\,c^{16}\,d^2 + 3552\,c^{15}\,d^3 - 6438\,c^{14}\,d^4 + 776\,c^{13}\,d^5 + 32\,004\,c^{12}\,d^6 - 103\,888\,c^{11}\,d^7 + 174\,716\,c^{10}\,d^8 - 164\,728\,c^9\,d^9 + 42\,144\,c^8\,d^{10} + 158\,816\,c^7\,d^{11} - 314\,216\,c^6\,d^{12} + 295\,936\,c^5\,d^{13} - 152\,880\,c^4\,d^{14} + 13\,184\,c^3\,d^{15} + 44\,000\,c^2\,d^{16} - 24\,192\,c\,d^{17} + 2240\,d^{18}\Big)\,f^4 - 16\,(c-d)^2\,\Big(4\,c^{14} - 16\,c^{13}\,d + 65\,c^{12}\,d^2 + 14\,c^{11}\,d^3 - 478\,c^{10}\,d^4 + 1964\,c^9\,d^5 - 2754\,c^8\,d^6 + 1328\,c^7\,d^7 + 684\,c^6\,d^8 - 4224\,c^5\,d^9 + 4120\,c^4\,d^{10} - 1120\,c^3\,d^{11} - 1584\,c^2\,d^{12} + 2624\,c\,d^{13} - 384\,d^{14}\Big)\,f^5 + 2\,\Big(35\,c^{14} - 278\,c^{13}\,d + 1232\,c^{12}\,d^2 - 5064\,c^{11}\,d^3 + 14\,896\,c^{10}\,d^4 - 24\,228\,c^9\,d^5 + 21\,796\,c^8\,d^6 - 6368\,c^7\,d^7 - 13\,764\,c^6\,d^8 + 20\,480\,c^5\,d^9 - 5016\,c^4\,d^{10} - 19\,840\,c^3\,d^{11} + 28\,432\,c^2\,d^{12} - 14\,400\,c\,d^{13} + 1952\,d^{14}\Big)\,f^6 - 4\,(c-d)\,\Big(7\,c^{11} - 34\,c^{10}\,d - 164\,c^9\,d^2 + 236\,c^8\,d^3 + 318\,c^7\,d^4 - 1292\,c^6\,d^5 + 2212\,c^5\,d^6 - 1640\,c^4\,d^7 + 760\,c^3\,d^8 + 1168\,c^2\,d^9 - 1552\,c\,d^{10} + 224\,d^{11}\Big)\,f^7 + \Big(11\,c^{10} - 156\,c^9\,d + 150\,c^8\,d^2 - 88\,c^7\,d^3 - 210\,c^6\,d^4 + 80\,c^5\,d^5 + 628\,c^4\,d^6 - 800\,c^3\,d^7 + 1528\,c^2\,d^8 - 896\,c\,d^9 - 112\,d^{10}\Big)\,f^8 + 6\,(c-d)\,(c+2\,d)\,\Big(c^2 + 2\,d^2\Big)^3\,f^9 - \Big(c^2 + 2\,d^2\Big)^3\,f^{10}\Big)\Big) \Big/ \Big((c-d)\,\Big(c^2 + 2\,d^2\Big)\,\Big(c^2 - 2\,d^2 - f\Big)\,\Big(c^4 - 2\,d^4 + 2\,c\,d\,f - f^2\Big)\,\Big(3\,c^4 - 8\,c^3\,d - 8\,c\,d^3 + 6\,d^4 + c^2\,\Big(8\,d^2 - 2\,f\Big) + 4\,d^2\,f + f^2\Big)\,\Big(c^3 + c\,f - 2\,d\,\Big(d^2 + f\Big)\Big)\Big) == 0$$

Esempi

La funzione F prende in input valori per c, d, f e restituisce: P, P2, a, b, e, Q, controlla che P2 e Q sono lo stesso punto, controlla che il punto Q sta sulla cubica.

In[41]:=
```
F[c_, d_, f_] := Module[{a, b, e, x, y, P, P2, Q},
  x = xo[d/c, f/c^2];
  y = yo[d/c, f/c^2];
  a = a3[t4[c, d, f], u4[c, d, f]];
  b = b2[r4[c, d, f], s4[c, d, f]];
  e = e0[x1[m3[t4[c, d, f], u4[c, d, f]], n3[t4[c, d, f], u4[c, d, f]]],
    y1[m3[t4[c, d, f], u4[c, d, f]], n3[t4[c, d, f], u4[c, d, f]]]];
  P = {x, y};
  P2 = {(x^2 - 8)^2/(4 x (x^2 + 8)), (x^2 - 8) (x^4 + 48 x^2 + 64)/(8 x y (x^2 + 8))};
  Q = {xo[b/a, e/a^2], yo[b/a, e/a^2]};
  {c, d, f, P, P2, a, b, e, Q, {P2[[1]] == Q[[1]], P2[[2]] == Q[[2]]}, Cub[Q[[1]], Q[[2]]]}]
```

Partendo da c=1, d=-1, f=1, cioè da P={1, 3}

In[42]:=
```
F[1, -1, 1]
```

Out[42]=
$$\left\{1, -1, 1, \{1, 3\}, \left\{\frac{49}{36}, -\frac{791}{216}\right\}, 1, 13, -239, \left\{\frac{49}{36}, -\frac{791}{216}\right\}, \{\text{True}, \text{True}\}, 0\right\}$$

In[43]:=
```
F[1, 13, -239]
```

Out[43]=
$$\left\{1, 13, -239, \left\{\frac{49}{36}, -\frac{791}{216}\right\}, \left\{\frac{63\,473\,089}{90\,098\,064}, \frac{2\,092\,306\,550\,111}{855\,210\,823\,488}\right\}, -21\,349\,431,\right.$$
$$\left. 19\,485\,153, 283\,810\,532\,473\,521, \left\{\frac{63\,473\,089}{90\,098\,064}, \frac{2\,092\,306\,550\,111}{855\,210\,823\,488}\right\}, \{\text{True}, \text{True}\}, 0\right\}$$

In[44]:=
```
F[-21349431, 19485153, 283810532473521]
```

Out[44]=
$$\left\{-21\,349\,431, 19\,485\,153, 283\,810\,532\,473\,521,\right.$$
$$\left\{\frac{63\,473\,089}{90\,098\,064}, \frac{2\,092\,306\,550\,111}{855\,210\,823\,488}\right\}, \left\{\frac{3\,710\,327\,303\,892\,830\,603\,933\,267\,543\,025\,409}{1\,577\,706\,009\,278\,875\,005\,318\,653\,442\,586\,176},\right.$$
$$-353\,501\,064\,436\,928\,880\,249\,966\,373\,674\,668\,207\,595\,571\,343\,213\,951\,/$$
$$\left. 62\,667\,031\,016\,032\,031\,207\,423\,081\,316\,204\,939\,202\,955\,367\,335\,424\right\},$$
$$301\,143\,307\,828\,005\,262\,829\,604\,984\,357\,787\,739\,849\,049\,273,$$
$$783\,828\,079\,380\,921\,779\,127\,658\,922\,777\,798\,845\,903\,662\,825,$$
$$-864\,128\,031\,433\,083\,820\,062\,511\,734\,086\,485\,202\,520\,338\,380\,849\,852\,249\,786\,393\,522\,768\,221\,525\,480\,/$$
$$466\,606\,390\,677\,903, \left\{\frac{3\,710\,327\,303\,892\,830\,603\,933\,267\,543\,025\,409}{1\,577\,706\,009\,278\,875\,005\,318\,653\,442\,586\,176},\right.$$
$$-353\,501\,064\,436\,928\,880\,249\,966\,373\,674\,668\,207\,595\,571\,343\,213\,951\,/$$
$$\left. \left. 62\,667\,031\,016\,032\,031\,207\,423\,081\,316\,204\,939\,202\,955\,367\,335\,424\right\}, \{\text{True}, \text{True}\}, 0\right\}$$

In[45]:=
```
F[301 143 307 828 005 262 829 604 984 357 787 739 849 049 273,
 783 828 079 380 921 779 127 658 922 777 798 845 903 662 825,
 -864 128 031 433 083 820 062 511 734 086 485 202 520 338 380 849 852 249 786 393 522 768 221 525 480 ÷
   466 606 390 677 903]
```

Out[45]=
```
{301 143 307 828 005 262 829 604 984 357 787 739 849 049 273,
 783 828 079 380 921 779 127 658 922 777 798 845 903 662 825,
 -864 128 031 433 083 820 062 511 734 086 485 202 520 338 380 849 852 249 786 393 522 768 221 525 480 ÷
   466 606 390 677 903, {3 710 327 303 892 830 603 933 267 543 025 409 / 1 577 706 009 278 875 005 318 653 442 586 176,
  -353 501 064 436 928 880 249 966 373 674 668 207 595 571 343 213 951 /
   62 667 031 016 032 031 207 423 081 316 204 939 202 955 367 335 424},
 {37 782 182 883 765 333 541 744 191 931 239 757 870 434 787 033 802 989 971 978 344 936 194 121 303 109 ÷
   888 296 211 359 838 799 494 344 583 827 258 338 226 486 503 124 665 801 729 /
  788 619 520 293 415 557 109 402 746 065 767 078 790 302 862 101 135 365 600 117 930 746 786 719 348 ÷
   942 314 404 592 110 880 707 752 490 621 610 225 974 543 797 482 761 593 346 304,
 13 712 553 419 096 940 100 107 207 633 544 687 622 871 226 284 473 040 993 643 570 642 866 531 531 973 ÷
   032 152 336 680 149 389 248 193 994 293 688 441 029 291 426 148 619 344 442 227 223 958 455 174 797 ÷
   709 164 738 681 165 277 141 441 193 223 615 988 694 192 978 007 551 /
  22 146 305 375 410 825 529 735 386 513 631 083 541 025 838 408 834 832 366 556 940 110 198 231 976 ÷
   956 443 507 188 665 031 240 939 203 211 270 158 976 211 170 796 685 240 229 117 404 337 238 854 570 ÷
   168 488 629 081 465 984 992 693 671 572 337 129 276 522 908 832 878 592},
 -1 329 397 557 482 357 265 590 800 017 527 914 559 762 974 502 926 031 555 698 457 634 524 538 002 804 ÷
   720 401 554 920 901 023 530 955 872 079 443 226 566 069 268 214 611 086 434 594 859 054 386 374 421 ÷
   805 647 930 129 126 731 689 827 412 214 249 507 492 220 147 619 387 912 685 279 664 622 555 423 168 ÷
   326 935 870 533 539 984 133 350 986 451 728 220 460 155 111,
 1 179 397 675 377 193 508 912 491 562 958 603 149 116 293 680 959 286 324 819 080 972 185 066 815 330 ÷
  893 415 317 082 326 774 888 382 836 110 267 505 324 279 028 964 218 585 066 407 297 671 910 324 721 ÷
  069 144 256 671 595 199 491 405 675 108 725 594 002 088 095 858 637 709 644 176 627 386 318 390 010 ÷
  410 317 912 325 545 898 514 603 981 523 418 386 416 720 761,
 -863 888 143 318 114 488 935 022 022 948 190 138 706 890 004 320 483 012 208 714 591 829 469 648 863 ÷
   700 184 070 725 118 479 678 608 582 953 417 151 911 426 207 151 270 247 853 131 129 319 816 506 172 ÷
   550 113 958 149 710 935 127 698 565 299 429 256 174 429 954 528 153 679 567 913 977 002 460 057 215 ÷
   239 322 258 723 308 548 844 221 233 537 190 257 948 764 488 609 828 638 806 379 920 550 543 761 252 ÷
   943 280 539 335 254 462 683 365 649 395 648 092 865 390 850 942 471 501 781 528 482 243 717 052 725 ÷
   013 319 933 448 601 964 139 538 805 453 409 554 216 314 685 021 509 499 024 708 273 113 635 550 166 ÷
   204 982 910 474 053 022 628 008 869 939 458 287 311 598 323 152 695 406 057 830 365 055 963 729 921 ÷
   105 497 488 024 079,
 {37 782 182 883 765 333 541 744 191 931 239 757 870 434 787 033 802 989 971 978 344 936 194 121 303 109 ÷
   888 296 211 359 838 799 494 344 583 827 258 338 226 486 503 124 665 801 729 /
  788 619 520 293 415 557 109 402 746 065 767 078 790 302 862 101 135 365 600 117 930 746 786 719 348 ÷
   942 314 404 592 110 880 707 752 490 621 610 225 974 543 797 482 761 593 346 304,
 13 712 553 419 096 940 100 107 207 633 544 687 622 871 226 284 473 040 993 643 570 642 866 531 531 973 ÷
   032 152 336 680 149 389 248 193 994 293 688 441 029 291 426 148 619 344 442 227 223 958 455 174 797 ÷
   709 164 738 681 165 277 141 441 193 223 615 988 694 192 978 007 551 /
  22 146 305 375 410 825 529 735 386 513 631 083 541 025 838 408 834 832 366 556 940 110 198 231 976 ÷
   956 443 507 188 665 031 240 939 203 211 270 158 976 211 170 796 685 240 229 117 404 337 238 854 570 ÷
   168 488 629 081 465 984 992 693 671 572 337 129 276 522 908 832 878 592}, {True, True}, 0}
```

Partendo da c=1, d=13, f=239, cioè P={8, 24}

In[46]:=
```
F[1, 13, 239]
```

Out[46]=
```
{1, 13, 239, {8, 24}, {49/36, 791/216}, -17 148 767,
 19 472 725, 448 422 145 921 777, {49/36, 791/216}, {True, True}, 0}
```

In[47]:=
```
F[-17 148 767, 19 472 725, 448 422 145 921 777]
```

Out[47]=
```
{-17 148 767, 19 472 725, 448 422 145 921 777, {49/36, 791/216},
 {63 473 089/90 098 064, -2 092 306 550 111/855 210 823 488}, -138 444 655 718 840 274 275 738 468 580 067 793 838 517 431,
 600 010 864 325 150 788 596 939 855 032 273 672 249 272 881,
 -508 774 412 817 797 647 834 966 476 785 800 727 973 200 165 287 445 923 186 439 257 713 201 775 027 \
   132 036 573 319 439, {63 473 089/90 098 064, -2 092 306 550 111/855 210 823 488}, {True, True}, 0}
```

In[48]:=
```
F[-138 444 655 718 840 274 275 738 468 580 067 793 838 517 431,
 600 010 864 325 150 788 596 939 855 032 273 672 249 272 881,
 -508 774 412 817 797 647 834 966 476 785 800 727 973 200 165 287 445 923 186 439 257 713 201 775 027 \
   132 036 573 319 439]
```

Out[48]=
```
{-138 444 655 718 840 274 275 738 468 580 067 793 838 517 431,
 600 010 864 325 150 788 596 939 855 032 273 672 249 272 881,
 -508 774 412 817 797 647 834 966 476 785 800 727 973 200 165 287 445 923 186 439 257 713 201 775 027 \
   132 036 573 319 439, {63 473 089/90 098 064, -2 092 306 550 111/855 210 823 488},
 {3 710 327 303 892 830 603 933 267 543 025 409/1 577 706 009 278 875 005 318 653 442 586 176,
  353 501 064 436 928 880 249 966 373 674 668 207 595 571 343 213 951 /
   62 667 031 016 032 031 207 423 081 316 204 939 202 955 367 335 424},
 -120 014 299 862 780 703 625 167 401 034 306 451 897 882 790 176 864 885 460 333 979 417 185 327 718 \
   734 994 851 295 876 349 020 783 519 044 383 410 364 015 114 655 117 517 189 413 019 444 914 848 969 \
   159 272 079 417 550 721 701 939 738 402 801 641 466 656 397 939 204 374 354 101 065 089 110 792 749 \
   548 813 501 191 762 139 882 006 527 105 552 310 725 701 319,
 200 186 926 004 219 136 746 623 296 389 807 796 084 702 497 414 016 508 144 648 858 306 618 353 212 457 \
   328 680 025 443 661 238 701 082 052 945 832 727 028 085 361 621 754 547 961 944 670 902 849 012 567 \
   420 038 608 609 036 929 779 241 705 233 002 177 209 277 184 234 204 523 143 528 717 316 383 166 630 \
   905 893 474 674 131 944 878 157 152 140 071 434 162 953,
 54 813 512 825 225 321 501 767 885 951 207 607 696 492 961 398 541 713 908 199 386 935 653 225 070 962 \
   486 047 881 930 710 721 709 124 764 336 323 411 616 368 899 677 524 362 507 954 464 465 846 716 341 \
   263 099 726 190 262 514 867 166 560 419 807 235 561 311 284 045 415 970 053 944 453 091 899 386 657 \
   662 315 072 265 059 730 198 242 095 941 029 129 416 519 730 780 389 053 930 015 753 830 633 626 884 \
   803 349 456 728 152 086 875 943 256 407 556 292 648 457 678 303 895 299 304 685 044 212 513 103 896 \
   124 513 763 988 055 614 080 946 535 593 649 431 128 367 230 203 869 164 190 119 510 943 692 786 766 \
   793 062 468 557 579 705 733 274 520 945 570 848 586 723 131 199 871 363 170 948 224 168 304 812 561 \
   924 183 271 921, {3 710 327 303 892 830 603 933 267 543 025 409/1 577 706 009 278 875 005 318 653 442 586 176,
  353 501 064 436 928 880 249 966 373 674 668 207 595 571 343 213 951 /
   62 667 031 016 032 031 207 423 081 316 204 939 202 955 367 335 424}, {True, True}, 0}
```

Partendo da c=1, d=-13, f=-239, cioè P={1, -3}

In[49]:=
```
F[1, -13, -239]
```

Out[49]=
```
{1, -13, -239, {1, -3}, {49/36, 791/216}, -17 148 767,
 19 472 725, 448 422 145 921 777, {49/36, 791/216}, {True, True}, 0}
```

In[50]:=
```
F[-17 148 767, 19 472 725, 448 422 145 921 777]
```

Out[50]=
$$\left\{-17\,148\,767,\ 19\,472\,725,\ 448\,422\,145\,921\,777,\ \left\{\frac{49}{36},\ \frac{791}{216}\right\},\right.$$
$$\left\{\frac{63\,473\,089}{90\,098\,064},\ -\frac{2\,092\,306\,550\,111}{855\,210\,823\,488}\right\},\ -138\,444\,655\,718\,840\,274\,275\,738\,468\,580\,067\,793\,838\,517\,431,$$
$$600\,010\,864\,325\,150\,788\,596\,939\,855\,032\,273\,672\,249\,272\,881,$$
$$-508\,774\,412\,817\,797\,647\,834\,966\,476\,785\,800\,727\,973\,200\,165\,287\,445\,923\,186\,439\,257\,713\,201\,775\,027 \setminus$$
$$\left.132\,036\,573\,319\,439,\ \left\{\frac{63\,473\,089}{90\,098\,064},\ -\frac{2\,092\,306\,550\,111}{855\,210\,823\,488}\right\},\ \{\text{True, True}\},\ 0\right\}$$

In[51]:=
```
F[-138 444 655 718 840 274 275 738 468 580 067 793 838 517 431,
 600 010 864 325 150 788 596 939 855 032 273 672 249 272 881,
 -508 774 412 817 797 647 834 966 476 785 800 727 973 200 165 287 445 923 186 439 257 713 201 775 027 \
  132 036 573 319 439]
```

Out[51]=
$$\left\{-138\,444\,655\,718\,840\,274\,275\,738\,468\,580\,067\,793\,838\,517\,431,\right.$$
$$600\,010\,864\,325\,150\,788\,596\,939\,855\,032\,273\,672\,249\,272\,881,$$
$$-508\,774\,412\,817\,797\,647\,834\,966\,476\,785\,800\,727\,973\,200\,165\,287\,445\,923\,186\,439\,257\,713\,201\,775\,027 \setminus$$
$$132\,036\,573\,319\,439,\ \left\{\frac{63\,473\,089}{90\,098\,064},\ -\frac{2\,092\,306\,550\,111}{855\,210\,823\,488}\right\},$$
$$\left\{\frac{3\,710\,327\,303\,892\,830\,603\,933\,267\,543\,025\,409}{1\,577\,706\,009\,278\,875\,005\,318\,653\,442\,586\,176},\right.$$
$$\left.353\,501\,064\,436\,928\,880\,249\,966\,373\,674\,668\,207\,595\,571\,343\,213\,951\ /\ 62\,667\,031\,016\,032\,031\,207\,423\,081\,316\,204\,939\,202\,955\,367\,335\,424\right\},$$
$$-120\,014\,299\,862\,780\,703\,625\,167\,401\,034\,306\,451\,897\,882\,790\,176\,864\,885\,460\,333\,979\,417\,185\,327\,718 \setminus$$
$$734\,994\,851\,295\,876\,349\,020\,783\,519\,044\,383\,410\,364\,015\,114\,655\,117\,517\,189\,413\,019\,444\,914\,848\,969 \setminus$$
$$159\,272\,079\,417\,550\,721\,701\,939\,738\,402\,801\,641\,466\,656\,397\,939\,204\,374\,354\,101\,065\,089\,110\,792\,749 \setminus$$
$$548\,813\,501\,191\,762\,139\,882\,006\,527\,105\,552\,310\,725\,701\,319,$$
$$200\,186\,926\,004\,219\,136\,746\,623\,296\,389\,807\,796\,084\,702\,497\,414\,016\,508\,144\,648\,858\,306\,618\,353\,212\,457 \setminus$$
$$328\,680\,025\,443\,661\,238\,701\,082\,052\,945\,832\,727\,028\,085\,361\,621\,754\,547\,961\,944\,670\,902\,849\,012\,567 \setminus$$
$$420\,038\,608\,609\,036\,929\,779\,241\,705\,233\,002\,177\,209\,277\,184\,234\,204\,523\,143\,528\,717\,316\,383\,166\,630 \setminus$$
$$905\,893\,474\,674\,131\,944\,878\,157\,152\,140\,071\,434\,162\,953,$$
$$54\,813\,512\,825\,225\,321\,501\,767\,885\,951\,207\,607\,696\,492\,961\,398\,541\,713\,908\,199\,386\,935\,653\,225\,070\,962 \setminus$$
$$486\,047\,881\,930\,710\,721\,709\,124\,764\,336\,323\,411\,616\,368\,899\,677\,524\,362\,507\,954\,464\,465\,846\,716\,341 \setminus$$
$$263\,099\,726\,190\,262\,514\,867\,166\,560\,419\,807\,235\,561\,311\,284\,045\,415\,970\,053\,944\,453\,091\,899\,386\,657 \setminus$$
$$662\,315\,072\,265\,059\,730\,198\,242\,095\,941\,029\,129\,416\,519\,730\,780\,389\,053\,930\,015\,753\,830\,633\,626\,884 \setminus$$
$$803\,349\,456\,728\,152\,086\,875\,943\,256\,407\,556\,292\,648\,457\,678\,303\,895\,299\,304\,685\,044\,212\,513\,103\,896 \setminus$$
$$124\,513\,763\,988\,055\,614\,080\,946\,535\,593\,649\,431\,128\,367\,230\,203\,869\,164\,190\,119\,510\,943\,692\,786\,766 \setminus$$
$$793\,062\,468\,557\,579\,705\,733\,274\,520\,945\,570\,848\,586\,723\,131\,199\,871\,363\,170\,948\,224\,168\,304\,812\,561 \setminus$$
$$924\,183\,271\,921,\ \left\{\frac{3\,710\,327\,303\,892\,830\,603\,933\,267\,543\,025\,409}{1\,577\,706\,009\,278\,875\,005\,318\,653\,442\,586\,176},\right.$$
$$\left.353\,501\,064\,436\,928\,880\,249\,966\,373\,674\,668\,207\,595\,571\,343\,213\,951\ /\ 62\,667\,031\,016\,032\,031\,207\,423\,081\,316\,204\,939\,202\,955\,367\,335\,424\right\},\ \{\text{True, True}\},\ 0\Big\}$$

Partendo da c=1, d=-13, f=239, cioè P={ $\frac{288}{49}$, $\frac{5424}{343}$ }

In[52]:=
```
F[1, -13, 239]
```

Out[52]=
$$\left\{1,\ -13,\ 239,\ \left\{\frac{288}{49},\ \frac{5424}{343}\right\},\ \left\{\frac{63\,473\,089}{90\,098\,064},\ \frac{2\,092\,306\,550\,111}{855\,210\,823\,488}\right\},\ -21\,349\,431,\right.$$
$$\left.19\,485\,153,\ 283\,810\,532\,473\,521,\ \left\{\frac{63\,473\,089}{90\,098\,064},\ \frac{2\,092\,306\,550\,111}{855\,210\,823\,488}\right\},\ \{\text{True, True}\},\ 0\right\}$$

In[53]:= **F[-21 349 431, 19 485 153, 283 810 532 473 521]**

Out[53]=
$$\Bigg\{-21\,349\,431,\ 19\,485\,153,\ 283\,810\,532\,473\,521,\ \Big\{\frac{63\,473\,089}{90\,098\,064},\ \frac{2\,092\,306\,550\,111}{855\,210\,823\,488}\Big\},\ \Big\{\frac{3\,710\,327\,303\,892\,830\,603\,933\,267\,543\,025\,409}{1\,577\,706\,009\,278\,875\,005\,318\,653\,442\,586\,176},$$
$$-353\,501\,064\,436\,928\,880\,249\,966\,373\,674\,668\,207\,595\,571\,343\,213\,951\ /$$
$$62\,667\,031\,016\,032\,031\,207\,423\,081\,316\,204\,939\,202\,955\,367\,335\,424\Big\},$$
$$301\,143\,307\,828\,005\,262\,829\,604\,984\,357\,787\,739\,849\,049\,273,$$
$$783\,828\,079\,380\,921\,779\,127\,658\,922\,777\,798\,845\,903\,662\,825,$$
$$-864\,128\,031\,433\,083\,820\,062\,511\,734\,086\,485\,202\,520\,338\,380\,849\,852\,249\,786\,393\,522\,768\,221\,525\,480\ \backslash$$
$$466\,606\,390\,677\,903,\ \Big\{\frac{3\,710\,327\,303\,892\,830\,603\,933\,267\,543\,025\,409}{1\,577\,706\,009\,278\,875\,005\,318\,653\,442\,586\,176},$$
$$-353\,501\,064\,436\,928\,880\,249\,966\,373\,674\,668\,207\,595\,571\,343\,213\,951\ /$$
$$62\,667\,031\,016\,032\,031\,207\,423\,081\,316\,204\,939\,202\,955\,367\,335\,424\Big\},\ \{\text{True},\ \text{True}\},\ 0\Bigg\}$$

In[54]:=
```
F[301 143 307 828 005 262 829 604 984 357 787 739 849 049 273,
 783 828 079 380 921 779 127 658 922 777 798 845 903 662 825,
 -864 128 031 433 083 820 062 511 734 086 485 202 520 338 380 849 852 249 786 393 522 768 221 525 480 /
  466 606 390 677 903]
```

Out[54]=
```
{301 143 307 828 005 262 829 604 984 357 787 739 849 049 273,
 783 828 079 380 921 779 127 658 922 777 798 845 903 662 825,
 -864 128 031 433 083 820 062 511 734 086 485 202 520 338 380 849 852 249 786 393 522 768 221 525 480 /
  466 606 390 677 903, {3 710 327 303 892 830 603 933 267 543 025 409 / 1 577 706 009 278 875 005 318 653 442 586 176,
  -353 501 064 436 928 880 249 966 373 674 668 207 595 571 343 213 951 /
   62 667 031 016 032 031 207 423 081 316 204 939 202 955 367 335 424},
 {37 782 182 883 765 333 541 744 191 931 239 757 870 434 787 033 802 989 971 978 344 936 194 121 303 109 /
   888 296 211 359 838 799 494 344 583 827 258 338 226 486 503 124 665 801 729 /
  788 619 520 293 415 557 109 402 746 065 767 078 790 302 862 101 135 365 600 117 930 746 786 719 348 /
   942 314 404 592 110 880 707 752 490 621 610 225 974 543 797 482 761 593 346 304,
  13 712 553 419 096 940 100 107 207 633 544 687 622 871 226 284 473 040 993 643 570 642 866 531 531 973 /
   032 152 336 680 149 389 248 193 994 293 688 441 029 291 426 148 619 344 442 227 223 958 455 174 797 /
   709 164 738 681 165 277 141 441 193 223 615 988 694 192 978 007 551 /
  22 146 305 375 410 825 529 735 386 513 631 083 541 025 838 408 834 832 366 556 940 110 198 231 976 /
   956 443 507 188 665 031 240 939 203 211 270 158 976 211 170 796 685 240 229 117 404 337 238 854 570 /
   168 488 629 081 465 984 992 693 671 572 337 129 276 522 908 832 878 592},
 -1 329 397 557 482 357 265 590 800 017 527 914 559 762 974 502 926 031 555 698 457 634 524 538 002 804 /
   720 401 554 920 901 023 530 955 872 079 443 226 566 069 268 214 611 086 434 594 859 054 386 374 421 /
   805 647 930 129 126 731 689 827 412 214 249 507 492 220 147 619 387 912 685 279 664 622 555 423 168 /
   326 935 870 533 539 984 133 350 986 451 728 220 460 155 111,
 1 179 397 675 377 193 508 912 491 562 958 603 149 116 293 680 959 286 324 819 080 972 185 066 815 330 /
  893 415 317 082 326 774 888 382 836 110 267 505 324 279 028 964 218 585 066 407 297 671 910 324 721 /
  069 144 256 671 595 199 491 405 675 108 725 594 002 088 095 858 637 709 644 176 627 386 318 390 010 /
  410 317 912 325 545 898 514 603 981 523 418 386 416 720 761,
 -863 888 143 318 114 488 935 022 022 948 190 138 706 890 004 320 483 012 208 714 591 829 469 648 863 /
   700 184 070 725 118 479 678 608 582 953 417 151 911 426 207 151 270 247 853 131 129 319 816 506 172 /
   550 113 958 149 710 935 127 698 565 299 429 256 174 429 954 528 153 679 567 913 977 002 460 057 215 /
   239 322 258 723 308 548 844 221 233 537 190 257 948 764 488 609 828 638 806 379 920 550 543 761 252 /
   943 280 539 335 254 462 683 365 649 395 648 092 865 390 850 942 471 501 781 528 482 243 717 052 725 /
   013 319 933 448 601 964 139 538 805 453 409 554 216 314 685 021 509 499 024 708 273 113 635 550 166 /
   204 982 910 474 053 022 628 008 869 939 458 287 311 598 323 152 695 406 057 830 365 055 963 729 921 /
   105 497 488 024 079,
 {37 782 182 883 765 333 541 744 191 931 239 757 870 434 787 033 802 989 971 978 344 936 194 121 303 109 /
   888 296 211 359 838 799 494 344 583 827 258 338 226 486 503 124 665 801 729 /
  788 619 520 293 415 557 109 402 746 065 767 078 790 302 862 101 135 365 600 117 930 746 786 719 348 /
   942 314 404 592 110 880 707 752 490 621 610 225 974 543 797 482 761 593 346 304,
  13 712 553 419 096 940 100 107 207 633 544 687 622 871 226 284 473 040 993 643 570 642 866 531 531 973 /
   032 152 336 680 149 389 248 193 994 293 688 441 029 291 426 148 619 344 442 227 223 958 455 174 797 /
   709 164 738 681 165 277 141 441 193 223 615 988 694 192 978 007 551 /
  22 146 305 375 410 825 529 735 386 513 631 083 541 025 838 408 834 832 366 556 940 110 198 231 976 /
   956 443 507 188 665 031 240 939 203 211 270 158 976 211 170 796 685 240 229 117 404 337 238 854 570 /
   168 488 629 081 465 984 992 693 671 572 337 129 276 522 908 832 878 592}, {True, True}, 0}
```

Bibliografia

[K] A. W. Knapp, *Elliptic Curves*. Princeton, N.J. : Princeton University Press, 1992.

[C] M. Cailotto, *Curve Algebriche Piane*. Note disponibili sul sito `http://www.math.unipd.it/~maurizio/`, 2009.

[M] D. A. Marcus, *Number fields*. Springer, 1977.

[A] G. M. Piacentini Cattaneo, *ALGEBRA un approccio algoritmico*. Decibel Zanichelli, 2007.

[F] P. de Fermat, *ŒUVRES DE FERMAT*. Paris, Imprimerie Gauthier-Villars et Fils, 1841. Library of Wellesley College.