UNIVERSITÀ DI PISA

CORSO DI LAUREA IN MATEMATICA

Conteggio di punti razionali su curve ellittiche con 2-torsione razionale

TESI DI LAUREA TRIENNALE

CANDIDATO:
Francesco Naccarato

RELATORE:
Prof. Umberto Zannier

ANNO ACCADEMICO 2019/2020

Indice

1 Introduzione

1.1 Problemi di conteggio

I problemi di conteggio sono estremamente ricorrenti in matematica: una volta definite determinate proprietà in un certo contesto, è naturale chiedersi quanti siano (solitamente a meno di equivalenze) gli oggetti che le soddisfano. Molto spesso ciò si traduce in un teorema di esistenza e unicità, o di non esistenza in generale; volendo quindi includere questi casi nella definizione di problema di conteggio, una grossa fetta della matematica risulta da essi costituita.
Un'importante classe di problemi di conteggio è quella delle soluzioni alle equazioni polinomiali. Spesso il dominio in cui si cercano queste soluzioni è quello dei numeri razionali, ma esse possono essere di interesse anche su campi di numeri, campi finiti, o anelli come $\mathbb{Z}$ e $\mathbb{Z}[\sqrt{-d}]$.
L'interesse nello studio di questi problemi ha origini antichissime, in quanto le equazioni algebriche risultano lo strumento di modellizzazione più immediato per questioni di natura geometrica, da sempre al cuore dell'interesse dell'uomo per la matematica. E, forse non sorprendentemente, nei secoli scorsi la ricerca in questo ambito ha rivelato una profonda interconnessione tra questi problemi e la geometria, dando origine alla geometria algebrica, poi evolutasi in una branca ricchissima e a sé stante della matematica.
In particolare, si è trovato che generalmente è più conveniente studiare le soluzioni a queste equazioni negli spazi proiettivi, in sostanza per tenere conto dell'eventuale soluzione all'infinito e per questioni di compattezza.
Informalmente, una *curva algebrica piana* C è il luogo di zeri di un polinomio omogeneo in tre variabili in uno spazio proiettivo $\mathbb{P}^2(K)$, quasi sempre $\mathbb{P}^2\mathbb{C}$. Più in generale, se la dimensione dello spazio è N, una curva è una varietà algebrica proiettiva di dimensione 1.
In questa tesi ci occupiamo di conteggio di punti **razionali** sulle curve **ellittiche**, oggetti con una struttura matematica molto ricca che definiremo a breve.

Definizione 1.1.1 *Un punto razionale su C è un punto sulla curva con tutte le coordinate razionali.*

Se, come nel caso delle curve ellittiche, accade che l'insieme dei punti razionali possiede in modo naturale una struttura aggiuntiva, ad esempio una particolare struttura di gruppo, questa può essere sfruttata per il conteggio. Non sarà difficile vedere che in generale l'insieme dei punti razionali su una curva *non è finito*. Il significato di "conteggio" in questo caso non risulta dunque immediato. E' tuttavia naturale l'idea di introdurre sullo spazio delle soluzioni una funzione che ne misuri, in qualche senso, la complessità, e contare il numero di soluzioni al di sotto di una certa complessità (ammesso che siano finite). Nella prossima sezione andiamo dunque a introdurre il concetto di *altezza*, che farà le veci di questa misura di complessità.

1.2 Altezze

Come detto nella sezione precedente, un'altezza è una funzione che misura la complessità di un punto. Indipendentemente dal fatto che il concetto di altezza sia nato, grazie al lavoro di Weil e Northcott, per contare gli elementi in determinati insiemi di soluzioni, non è necessario alcun riferimento a problemi di conteggio per definire un'altezza, in quanto è sufficiente definirla come funzione su $\bar{\mathbb{Q}}$ e si avrà automaticamente che a ogni punto razionale, o appartenente a un campo di numeri, su una curva si potrà associare la sua altezza, definendola come l'altezza di una delle sue coordinate.
Andiamo dunque a definire l'altezza di Weil; per gli scopi di questa tesi sarà quasi sempre sufficiente lavorare con la definizione su $\mathbb{Q}$, tuttavia diamo un'idea della definizione anche su arbitrari campi di numeri, che ci sarà utile nel capitolo 6.

Definizione 1.2.1 (Altezza di Weil) *Per a, b interi coprimi sia:*

$$H\left(\frac{a}{b}\right) \coloneqq max\{|a|, |b|\}$$

l'altezza di Weil di $\frac{a}{b}$;
e $h \coloneqq logH$ la relativa altezza logaritmica.

E' possibile generalizzare questa definizione a un qualunque campo di numeri K. Per fare ciò notiamo che posto $r = \frac{a}{b}$, la funzione $h(r) = logmax(|a|, |b|)$ si può scrivere, in modo apparentemente più complicato, come:

$$h(r) = \sum_p max(0, -ord_p(r))logp + logmax(1, |r|)$$

dove la somma è estesa a tutti i primi e $ord(\frac{a}{b}) := \upsilon_p(a) - \upsilon_p(b)$ con $\upsilon_p(k)$ la massima potenza di p che divide k (e $\upsilon_p(0) := \infty$).
Se definiamo ora su $\mathbb{Q}$, per ogni primo p, il valore assoluto $p-$adico:

$$|r|_p \coloneqq p^{-ord_p(r)}$$

e denotiamo $M_{\mathbb{Q}}$ l'insieme dei valori assoluti su $\mathbb{Q}$ (ovvero quello standard e quelli $p-$adici), otteniamo la formula

$$h(r) = \sum_{|\cdot|_v \in M_{\mathbb{Q}}} logmax(1, |r|_v) \tag{1}$$

Questa scrittura è utile perché ogni campo di numeri K possiede un unico insieme di valori assoluti normalizzati M_K che concettualmente "rispecchia" quello che abbiamo definito per $\mathbb{Q}$, da cui possiamo estendere a $\bar{\mathbb{Q}}$ la definizione di *altezza di Weil* come in (1):

$$h(\alpha) \coloneqq \sum_{|\cdot|_y \in M_K} logmax(1, |\alpha|_v)$$

per un qualunque campo di numeri K contenente α. Definendo gli M_K si può trovare che quella data è una buona definizione.
Il seguente risultato mostra che il conteggio di punti razionali con altezza limitata da B su qualunque curva darà un risultato finito, in quanto vale in generale:

Teorema 1.2.1 (Northcott) *per ogni $B > 0$, il numero di punti $P \in \bar{\mathbb{Q}}$ tali che $H(P) < B$ è finito*

Dimostrazione: (nel caso di $\mathbb{Q}$) abbiamo al più $\lfloor B+1 \rfloor$ scelte per numeratore e denominatore. Chiaramente lo stesso risultato vale per l'altezza logaritmica. □

Come vedremo nel capitolo 4, l'altezza di Weil non è lo strumento più preciso per il controllo dei punti razionali su una curva ellittica, ma andrà in un certo senso "raffinata".

1.3 Curve Ellittiche

Diremo che una curva $\mathcal{C}$ è *definita su un campo* K se i coefficienti dei polinomi nell'ideale che la definisce sono in K. Ricordiamo che una curva non singolare in $\mathbb{P}^2\mathbb{C}$ è naturalmente una varietà complessa con le carte date dal Teorema del Dini.
Una curva ellittica E su un campo K (indicata come E/K) è una curva cubica non singolare definita su K (presa solitamente come sottoinsieme di $\mathbb{P}^2\bar{K}$).
Si può dimostrare che se $charK \neq 2, 3$ (e per noi questo sarà il caso, perché lavoreremo sempre in sottocampi di $\mathbb{C}$) è possibile portare ogni tale curva nella forma

$$ZY^2 = X^3 + aXZ^2 + bZ^3$$

che in forma affine diventa

$$y^2 = x^3 + ax + b \tag{2}$$

tramite isomorfismi esprimibili come funzioni razionali delle coordinate con anche l'inversa esprimibile in questo modo. Questa forma è detta *forma di Weierstrass* e il polinomio in x è detto polinomio di Weierstrass della curva; lavoreremo con la forma affine, ricordando però che sulla curva c'è anche il punto all'infinito.
Notiamo che se E è definita su $\mathbb{Q}$, applicando un'ulteriore trasformazione del tipo

$$x \mapsto q^2 s^2 x,\ y \mapsto q^3 s^3 y \tag{3}$$

dove $a = \frac{p}{q},\ b = \frac{r}{s}$ ottieniamo una rappresentazione per E del tipo

$$y^2 = x^3 + Ax + B \tag{4}$$

con $A, B \in \mathbb{Z}$. Lavoreremo da adesso con curve in questa forma, cui ci riferiremo all'occorrenza come *forma di Weierstrass intera*, se non diversamente specificato. Possiamo inoltre definire l'*altezza della curva* in forma di Weierstrass intera

$$H(E) := max\{4|A|^3, 27B^2\} \tag{5}$$

e la relativa altezza logaritmica $h(E) := log(H(E))$.

La definizione data non rivela molto sulla ricca varietà di caratteristiche possedute da questi oggetti. Attraverso lo studio delle funzioni meromorfe biperiodiche sui complessi (chiamate, non a caso, funzioni ellittiche) è possibile mostrare che le curve ellittiche su $\mathbb{C}$ sono in corrispondenza con i reticoli complessi di dimensione 2, ovvero con le possibili strutture di superificie di Riemann sul toro. Tutti questi insiemi (quello delle curve ellittiche su $\mathbb{C}$, quello dei reticoli e quello delle strutture complesse sul toro) vanno in realtà presi a meno di equivalenze, che enuncieremo in maniera precisa (insieme al significato di corrispondenza) nel prossimo capitolo, quando affronteremo più nel dettaglio questo argomento.
Questa corrispondenza ci permetterà di "trasportare" la legge di gruppo sul toro, a sua volta indotta dal + in $\mathbb{C}$ attraverso il quoziente, sulla curva ellittica. L'aver determinato che i punti di una curva ellittica su $\mathbb{C}$ formino un gruppo non ci assicura *a priori* che lo stesso valga per i suoi punti razionali: vedremo infatti che ciò è vero per curve ellittiche definite su $\mathbb{Q}$ quando esamineremo più nel dettaglio la legge di gruppo nel prossimo capitolo.
Questa profonda connessione tra l'analisi complessa e un oggetto di natura algebrico-geometrica ci consentirà di utilizzare una vasta gamma di strumenti per dimostrare i nostri risultati ed è uno dei motivi per cui personalmente ritengo estremamente interessante questo ambito di ricerca.
In questo lavoro, così come nella maggior parte della letteratura sul problema del conteggio di punti razionali, lavoriamo, a meno di dichiarare esplicitamente il contrario, con curve ellittiche $E/\mathbb{Q}$. Questo sostanzialmente perché, come detto sopra, in questo caso i punti razionali formano un gruppo: sarà proprio questa struttura aggiuntiva che ci permetterà di controllarne la distribuzione.

Soffermiamoci brevemente sul titolo di questa tesi: la 2-torsione di una curva ellittica E è la sua 2-torsione nel senso dei gruppi, ovvero il sottogruppo degli elementi con ordine che divide 2. Vedremo che questo sottogruppo sarà formato dal punto all'infinito e dai punti con ascissa uno dei tre zeri del polinomio di Weierstrass (e dunque ordinata nulla); per 2-*torsione razionale* si intende che questi tre punti sono razionali; l'obiettivo di questa tesi è delineare la dimostrazione del risultato ottenuto da E. Bombieri e U. Zannier nel paper [1], che stabilisce la miglior stima conosciuta per il conteggio di punti razionali su curve di questo tipo. Inoltre, qui impieghiamo una tecnica da loro suggerita nel medesimo lavoro per formalizzare il risultato nel caso solo una radice sia razionale. Il caso generale pare sfortunatamente al di fuori della portata degli

strumenti al momento disponibili.
Denotiamo:

$$N(B) = N_E(B) := |\{P \in E(\mathbb{Q}) : H(P) \leq B\}| = |\{P \in E(\mathbb{Q}) : h(P) \leq logB\}|$$

Congettura 1.3.1 *Sia $\epsilon > 0$. Allora per ogni curva ellittica $E/\mathbb{Q}$ in forma di Weierstrass e per ogni $B > 0$ si ha:*

$$N(B) \leq c(\epsilon)(max(H(E), B))^{\epsilon} \tag{6}$$

dove $c(\epsilon)$ è una costante che dipende solo da ϵ.

Teorema 1.3.2 *Sia $E : y^2 = A(x),\ A \in \mathbb{Q}[x]$ una curva ellittica in forma di Weierstrass tale che A abbia una radice razionale. Sia $M := max(e^3, H(E), B)$. Allora esiste una costante assoluta $c_0 > 0$ tale che:*

$$N(B) \leq M^{\frac{c_0}{loglogM}} \tag{7}$$

Corollario 1.3.2.1 *Per le curve ellittiche con un punto di 2-torsione (diverso dal punto all'infinito) razionale vale la Congettura 1.3.1.*

Osservazione 1.3.0.1 *Nel dimostrare il Teorema 1.3.2 possiamo assumere $B \geq H(E)$: infatti se $B < H(E)$ allora $N(B) \leq N(H(E))$ e quindi la tesi è falsa anche contando i punti con altezza logaritmica fino a $h(E)$, avendo i due insiemi la stessa maggiorazione nell'enunciato.*

Osservazione 1.3.0.2 *Vediamo che lavorare con un modello di curva intero (come in (4)) non è restrittivo rispetto all'enunciato del Teorema* 1.3.2*: infatti da (3) è immediato che il polinomio di Weierstrass del modello come in (2) ha una radice razionale se e solo se ce l'ha quello del relativo modello intero (e questa sarà in particolare intera). Inoltre per un modello come in (2) il numero di punti razionali con altezza limitata da B è al più pari a quello dei punti razionali con altezza limitata da $BH(a)^2H(b)^2$ per il relativo modello intero. Quindi, applicando la sostituzione $B \mapsto BH(a)^2H(b)^2$, dal Teorema otteniamo che per un modello come in (2) la stima è*

$$N(B) \leq exp(c_0\frac{M'}{logM'}) \leq exp(c_1\frac{M}{logM}) \tag{8}$$

con le stesse notazioni di sopra e definendo opportunamente $H(E)$ per un modello come in (2) e c_1. Ad esempio, scegliendo $H(E) := (H(a)H(b))^2$, per l'assunzione $B \geq H(E)$ possiamo prendere $c_1 = 2c_0$. Quindi cambiando il modello cambia solo la costante assoluta.

1.4 Struttura del lavoro

Come anticipato, nel secondo capitolo costruiamo la teoria alla base della legge di gruppo sulle curve ellittiche, ovvero vediamo la corrispondenza tra esse e

i tori tramite le funzioni ellittiche. Questa teoria non ci sarà utile solo per costruire la legge di gruppo, ma anche per comprendere le tecniche utilizzate nei risultati moderni esposti nei capitoli 5 e 6. Nel terzo capitolo sviluppiamo la necessaria aritmetica del gruppo dei punti razionali, introducendo una serie di quantità fondamentali, mentre nel quarto presentiamo l'altezza canonica, strumento cruciale per ottenere le stime desiderate. Gli ultimi due capitoli sono dedicati a conclusioni e approfondimenti.
E' importante notare (anche se verrà rimarcato più volte) che l'unico punto in cui si utilizza la razionalità delle 2-torsione è la stima per il rango nel capitolo 3: tutti gli altri risultati, inclusi quelli moderni, valgono per ogni curva ellittica definita su $\mathbb{Q}$ (o addirittura su un campo di numeri K).

2 Tori e legge di gruppo

Come accennato, la possibilità di controllare fortemente il numero di punti razionali ad altezza fissata sulle curve ellittiche deriva dal fatto che queste possiedono un'intrinseca struttura di gruppo: sarà quindi di interesse osservare come si comporta l'altezza dei punti sotto l'azione della legge di gruppo, ad esempio degli endomorfismi di moltiplicazione.
Vedremo inoltre che le curve ellittiche sono gruppi *finitamente generati* (questo risultato si estende in realtà a tutte le varietà abeliane, grazie al lavoro di Weil), il che sarà la vera chiave per il nostro controllo dei punti razionali.
Data una certa operazione binaria su una curva ellittica

$$E : y^2 = x^3 + ax + b \tag{9}$$

è ovviamente possibile dimostrare che essa vi definisce una struttura di gruppo (se è effettivamente così) utilizzando solamente la definizione che abbiamo dato; tuttavia, per la struttura che a breve descriveremo, questo risulta particolarmente laborioso da un punto di vista "computazionale" ma, soprattutto, procedere in questo modo non ci dà alcuna indicazione sul *perché* abbiamo scelto quell'operazione binaria: la dobbiamo in un certo senso "indovinare". Per questo abbiamo deciso di seguire la strada più profonda ed elegante della corrispondenza coi tori complessi. Non solo, questa corrispondenza ci permetterà di riformulare anche nel framework dei tori tutti i problemi che dovremo affrontare.
Dobbiamo quindi fare un leggero *détour.*

2.1 Superfici di Riemann e tori

Definizione 2.1.1 (Superficie di Riemann) *Uno spazio topologico connesso di Hausdorff si dice Superficie di Riemann se esiste un suo ricoprimento aperto* $(U_\alpha)_{\alpha\in A}$ *e una collezione* $\{\phi_\alpha : U_\alpha \to \mathbb{C}\}_{\alpha\in A}$ *di omeomorfismi sull'immagine tali che per ogni* α_1, α_2 *con* $U_{\alpha_1} \cap U_{\alpha_2} \neq \emptyset$ *la mappa (di transizione)* $\phi_{\alpha_2} \circ \phi_{\alpha_1}^{-1} : \phi_{\alpha_1}(U_{\alpha_1} \cap U_{\alpha_2}) \to \mathbb{C}$ *sia olomorfa.*

Definizione 2.1.2 (Mappa olomorfa tra Superfici di Riemann) *Date* M, N *Superfici di Riemann,* $f : M \to N$ *si dice olomorfa in* $x \in M$ *se esistono* α, β *e un aperto* A *con* $x \in A \subseteq U_\alpha$, $f(x) \in V_\beta$ *tali che* $\psi_\beta \circ f \circ \phi_\alpha^{-1} : \phi_\alpha(A) \to \mathbb{C}$ *sia olomorfa (con ovvie notazioni per le carte).* $f : M \to N$ *si dice olomorfa se lo è in ogni punto di* M*.*

Osservazione 2.1.2.1 *Quella data una buona definizione (non dipende dalla carta scelta) grazie all'olomorfia delle mappe di transizione.*

Osservazione 2.1.2.2 *Una mappa olomorfa è continua come mappa tra spazi topologici.*

Definizione 2.1.3 (Biolomorfismo di Superfici di Riemann) *Date M, N Superfici di Riemann e $f : M \to N$ biettiva tale che f, f^{-1} siano olomorfe, allora f si dice biolomorfismo e M, N si dicono biolomorfe.*

Come usuale in matematica, è utile studiare le Superfici di Riemann a meno di equivalenza, nel caso specifico a meno di biolomorfismo. Risulta di fondamentale importanza il seguente Teorema:

Teorema 2.1.1 (Riemann-Poincaré-Koebe) *Ogni Superficie di Riemann semplicemente connessa è biolomorfa a una delle seguenti:*

- $\mathbb{P}^1\mathbb{C}$ *con le due carte standard di proiezione;*
- $\mathbb{C}$ *con le carte banali;*
- $D = \{|z| < 1\}$ *con le carte date dall'inclusione in* $\mathbb{C}$*.*

Come già accennato, è possibile dotare una curva ellittica di una struttura complessa grazie alla non singolarità: questa ci permette infatti di applicare il **Teorema del Dini** e dunque trovare, per ogni punto sulla cubica, un suo intorno nel quale una delle due variabili è esplicitabile in funzione dell'altra. Dunque, le carte date da questi intorni con le proiezioni da essi in $\mathbb{C}$ della variabile implicita rendono la curva una Superficie di Riemann: dati due intorni con intersezione non vuota, se la proiezione è della stessa variabile le due mappe di transizione sono l'identità, altrimenti sono proprio le relazioni tra le due varibili, che essendo nell'intersezione sono entrambe olomorfe.

Remark 2.1.1 *In realtà bisogna anche verificare che una curva ellittica come spazio topologico è $T2$ sia connessa, ma questo è un semplice esercizio.*

Definizione 2.1.4 (Reticolo in $\mathbb{C}$) *Un reticolo nel piano complesso è un sottoinsieme della forma $Span_{\mathbb{Z}}(\omega_1, \omega_2)$ con $\mathrm{Im}(\frac{\omega_1}{\omega_2}) \neq 0$*

Osservazione 2.1.4.1 *Coppie distinte di numeri complessi possono generare lo stesso reticolo: non è difficile mostrare che $u = (\omega_1, \omega_2)$ e $v = (\eta_1, \eta_2)$ generano lo stesso reticolo $\iff \exists M \in \mathbb{SL}_2\mathbb{Z} \mid Mu = v$*

Possiamo dotare il toro di una struttura di Superficie di Riemann (o *struttura complessa*) scegliendo un reticolo e prendendo le carte indotte dal quoziente per quel reticolo (formalmente il quoziente è per il sottogruppo di automorfismi generato da $+\omega_1$ e $+\omega_2$).
E' naturale chiedersi se al variare del reticolo scelto le risultanti Superfici di Riemann siano biolomorfe. La risposta è quasi sempre negativa; in particolare, lo sono se e solo se i reticoli sono omotetici.

Notiamo che con questa classe di strutture complesse, il toro eredita da $\mathbb{C}$ anche una struttura di gruppo, tramite il quoziente.

Definizione 2.1.5 (Isogenie) *Dati due tori T_1, T_2, un'isogenia $\phi : T_1 \to T_2$ è un'omomorfismo di gruppi che sia olomorfo come mappa tra superfici di Riemann.*

Esempio 2.1.5.1 *Sia L_1 generato da ω_1, ω_2 e sia L_2 generato da $\frac{\omega_1}{2}, \omega_2$. Allora la proiezione $\pi : T_1 \to T_2$ è un'isogenia, con $\ker \pi = \{0, \frac{\omega_1}{2}\} \subset T_1$*

Questo esempio non è scelto a caso, bensì vedremo che questa isogenia, detta 2-isogenia, ci è utile quando il punto $\frac{\omega_1}{2} \in T_1$ viene mandato dal rispettivo esponenziale di Weierstrass (si veda la prossima sezione) in un punto razionale della curva ellittica relativa a T_1.

Proposizione 2.1.2 *Dati due reticoli L_1, L_2, esiste un'isogenia tra i rispettivi tori $\phi : T_1 \to T_2$ se e solo se esiste $\mu \in \mathbb{C} : \mu L_1 \subset L_2$.*

2.2 Funzioni ellittiche

Per le dimostrazioni di alcuni classici risultati che vengono qui omesse per ragioni di spazio, si rimanda al capitolo 1 dell'ottimo testo di Lang [2].
Prima di proseguire, diamo un semplice risultato sui reticoli che ci sarà utile per quanto segue;

Lemma 2.2.1 *Sia L un reticolo in $\mathbb{C}$. Denotiamo per comodità $L' = L - \{0\}$. Allora:*

1. $\sum_{l \in L'} l^{-s}$ *converge assolutamente se e solo se* $\mathrm{Re}(s) > 2$
2. $\sum_{l \in L'} l^{-d} = 0$ *per $d > 1$ dispari*

Dimostrazione: il primo punto segue dal teorema di confronto serie-integrale; per il secondo, grazie alla convergenza possiamo riarrangiare i termini raggruppando a coppie quelli con l e $-l$, da cui segue la tesi. □
Per comprendere il legame tra tutto ciò e le curve ellittiche è necessario introdurre le funzioni ellittiche. E' una semplice conseguenza del Teorema di Liouville che le uniche funzioni olomorfe periodiche modulo un reticolo L, ovvero tali che

$$f(z + l) = f(z) \ \forall \ l \in L$$

siano le costanti. Fissato un reticolo, possiamo però chiederci quali sono le funzioni meromorfe e rispetto ad esso periodiche.

Definizione 2.2.1 (Funzione ellittica relativa a un reticolo) *Dato un reticolo $L \subset \mathbb{C}$, un funzione meromorfa $f : \mathbb{C} \to \mathbb{C}$ tale che $f(z + l) = f(z)$ $\forall z \in \mathbb{C}, l \in L$ è detta funzione ellittica relativamente a L.*

Da ora ometteremo di frequente la dipendenza dal reticolo, che non dovrà comunque essere dimenticata.
Non è difficile mostrare che l'insieme di queste funzioni è un campo con il $+$ e il $\cdot$ di $\mathbb{C}$: abbiamo dunque definito il **campo delle funzioni ellittiche**. Non abbiamo però ancora dato alcun esempio di funzione ellittica non costante: introduciamo ora la fondamentale funzione di Weierstrass:

Definizione 2.2.2 (Funzione di Weierstrass) *Dato un reticolo L, sia*

$$\wp_L(z) = \wp(z) := \frac{1}{z^2} + \sum_{l \in L'} \frac{1}{(z-l)^2} - \frac{1}{l^2} \tag{10}$$

la funzione di Weierstrass.

Proposizione 2.2.2 *L'espressione in* (10) *definisce una funzione meromorfa su $\mathbb{C}$, con poli precisamente in L.*

Proposizione 2.2.3 *La $\wp$ di Weierstrass è pari e periodica modulo L.*

La parità segue scambiando formalmente l con $-l$ in (10), ma, per la periodicità, la questione è più complicata, non essendoci convergenza assoluta. Consideriamo dunque la derivata $\wp'(z) = -2\sum_{l \in L} \frac{1}{(z-l)^3}$ che si vede analogamente essere dispari. In questo caso c'è invece convergenza assoluta per il Lemma 2.2.1 e quindi si ha che $\wp'$ è periodica modulo L. Ma allora $\wp(z+l_0) - \wp(z) = c(l_0)$ e scegliendo $z = -\frac{l_0}{2}$ si ottiene $c(l_0) = 0 \ \forall \ l_0 \in L$ grazie alla parità.
Prima di proseguire, notiamo che $\wp$ e $\wp'$ hanno poli soltanto in 0 come funzioni $\mathbb{C}/L \to \mathbb{C}$, rispettivamente di ordine 2 e 3.

Teorema 2.2.4 (Campo delle funzioni ellittiche) *Il campo delle funzioni ellittiche è $\mathbb{C}(\wp, \wp')$.*

Per la dimostrazione di questo importante risultato rimandiamo alla letteratura citata; specifichiamo solo che le idee principali sono:

1. ogni funzione ellittica è somma di una pari e una dispari;
2. ogni funzione ellittica pari con poli solo in 0 sta in $\mathbb{C}[\wp]$;
3. si possono "aggiustare" gli altri poli con fattori del tipo $(\wp(z) - \wp(z_0))^j$.

In particolare il primo punto è la classica scrittura $f(z) = \frac{f(z)+f(-z)}{2} + \frac{f(z)-f(-z)}{2}$.
Il punto davvero importante è il secondo, che si basa sul fatto che ogni funzione ellittica senza poli è costante, come già detto, e sul Teorema dei Residui.

Lemma 2.2.5 (Relazione tra $\wp$ e $\wp'$) *Vale la relazione*

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3 \tag{11}$$

con $g_2, g_3 \in \mathbb{C}$ dipendenti dal reticolo

Dimostrazione: $\wp'^2$ è una funzione ellittica pari, dunque per il secondo punto di sopra è identicamente uguale a un polinomio in $\wp$, e guardando l'ordine del polo in 0 segue che il grado di questo polinomio è 3. Per trovarlo, espandiamo in serie di potenze $\wp$: notiamo che

$$\frac{1}{(z-l)^2} = \frac{1}{l^2}\frac{1}{(1-\frac{z}{w})^2} = \frac{1}{l^2}\cdot\frac{d}{dz}\frac{1}{1-\frac{z}{l}}$$

da cui segue

$$\frac{1}{(z-l)^2} - \frac{1}{l^2} = \sum_{n=1}^{\infty}(n+1)\frac{z^n}{l^{n+2}} \tag{12}$$

Da (12) si ha, posto

$$G_k = \sum_{l\in L} l^{-2k} \tag{13}$$

e scambiando le sommatorie in l e z e usando il punto 2 del Lemma 2.2.1,

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{n+1}z^{2n} \tag{14}$$

Da (14) possiamo ricavare analoghe espansioni per $\wp'$ e $\wp'^2$, dalle quali segue che la funzione

$$\wp'^2(z) - 4\wp^3(z) + g_2\wp(z) + g_3$$

con

$$g_2 = 60G_2,\ g_3 = 140G_3 \tag{15}$$

è una funzione ellittica con espansione del tipo

$$c_1 z + c_2 z^2 + ...$$

ed è perciò nulla. □

Chiameremo anche $4x^3 - g_2(L)x - g_3(L)$ **Polinomio di Weierstrass** relativo al reticolo L, confidando che questo non crei confusione con quello delle curve ellittiche, essendo ormai chiaro il collegamento tra i due oggetti. E' importante menzionare che applicando il Teorema dei Residui alle funzioni ellittiche si trova, grazie alla periodicità, che queste hanno lo stesso numero di zeri e poli, contati con molteplicità. Questo in particolare implica che $\wp$ ha esattamente due zeri in $\mathbb{C}/L$, opposti rispetto all'origine.
Notiamo che essendo $\wp'$ dispari, questa si annulla nei tre punti $\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}$ (non avendo poli in questi punti), ed esattamente in questi tre, avendo un unico polo di ordine 3. Dunque le radici del polinomio di Weierstrass sono $\wp(\frac{\omega_1}{2}), \wp(\frac{\omega_2}{2}), \wp(\frac{\omega_1+\omega_2}{2})$ che sono numeri complessi distinti non essendo nessuna coppia di questi punti simmetrica rispetto all'origine (quanto detto sopra per $\wp$ vale chiaramente anche per $\wp$ traslata di una costante).

2.3 Legge di gruppo

Dalla relazione ricavata nella sezione precedente appare chiaro il legame con le curve ellittiche. Lo formalizziamo con il seguente:

Teorema 2.3.1 *Sia* $E = \{(X, Y, Z) \in \mathbb{P}^2\mathbb{C} \mid ZY^2 = 4X^3 - g_2Z^2X - g_3Z^3\}$ *e sia* $exp_E : \mathbb{C}/L \to \mathbb{P}^2\mathbb{C}$ *la mappa di Weierstrass definita da*

$$exp_E(z) = \begin{cases} (\wp(z) : \wp'(z) : 1), & se\ z \neq 0 \\ (0 : 1 : 0) & se\ z = 0 \end{cases} \tag{16}$$

Allora exp_E *è un biolomorfismo tra* $\mathbb{C}/L$ *ed* E.

Se vogliamo avere come immagine una curva ellittica in forma di Weierstrass ci è sufficiente applicare poi la mappa $y \mapsto \frac{y}{2}$, che induce un biolomorfismo tra le rispettive curve, come ogni trasformazione lineare (o semplicemente cambiare $\wp'$ con $\frac{\wp'}{2}$ nella definizione di exp_E e verificare che anche con questa definizione induce un biolomorfismo).
La mappa di Weierstrass mette dunque in corrispondenza reticoli a meno di omotetia, ovvero strutture complesse sul toro a meno di biolomorfismo, con curve ellittiche in forma di Weierstrass a meno di trasformazioni lineari delle coordinate: questo è il parallelismo che cercavamo. Ciò non è però ancora sufficiente, perché non ci assicura che ogni curva ellittica "venga da" un toro: questo fatto, per la cui comprensione è necessario sviluppare la teoria delle Funzioni Modulari e in particolare dell'*invariante j* (si veda sempre il testo di Lang), verrà qui assunto senza dimostrazione.
Sul toro abbiamo la legge di gruppo indotta da $\mathbb{C}$ nella maniera naturale: $[z_1]_L +_L [z_2]_L = [z_1 + z_2]_L$. Vogliamo ora vedere questa legge sulla curva ellittica E_L associata tramite la mappa di Weierstrass. E' chiaro che l'elemento neutro sarà il punto all'infinito O. Sommare due punti $P_1 = (x_1, y_1) = (\wp(z_1), \wp'(z_1)), P_2 = (x_2, y_2) = (\wp(z_2), \wp'(z_2))$ equivale a scrivere $\wp(z_1 + z_2)$ e $\wp'(z_1 + z_2)$ in funzione di $\wp(z_1), \wp'(z_1), \wp(z_2), \wp'(z_2)$. Non è difficile dimostrare che vale la formula

$$\wp'(-z_1 - z_2) = a\wp(-z_1 - z_2) + b \tag{17}$$

con

$$a = \frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}$$

e

$$b = \frac{\wp(z_1)\wp'(z_2) - \wp(z_2)\wp'(z_1)}{\wp(z_1) - \wp(z_2)}$$

Guardando i coefficienti e ricordando la parità di $\wp$ e la disparità di $\wp'$ notiamo che (17) vuol dire che $(\wp(z_1 + z_2), -\wp'(z_1 + z_2))$ sta sulla retta per $(\wp(z_1), \wp'(z_1))$

e $(\wp(z_2), \wp'(z_2))$, e quindi è la terza intersezione della retta per P_1 e P_2 con la curva, da cui P_1+P_2 è il *simmetrico* di questa terza intersezione rispetto "all'asse x" (siamo in realtà in campo complesso, si intende con seconda coordinata cambiata di segno), che infatti sta ancora sulla curva. Nei casi degeneri in cui uno dei due punti è O oppure $P_1 = P_2 = P$ si trova che le rette da considerare sono rispettivamente quella verticale (i.e. con x costante) e la tangente in P.

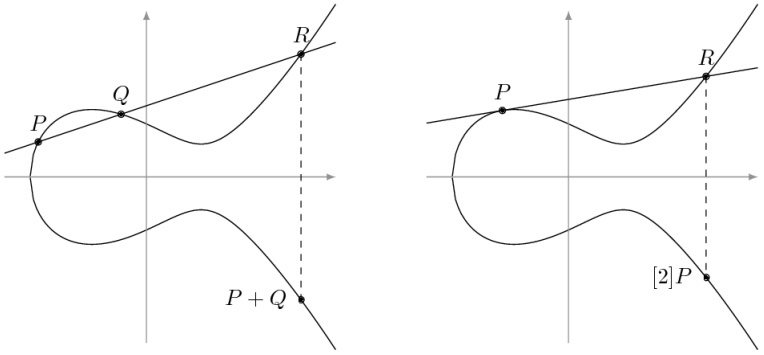

Figura 1: Legge di gruppo su una curva ellittica

Abbiamo dunque trovato la legge di gruppo indotta sulla curva, e non dobbiamo verificare che sia tale in quanto viene dal biolomorfismo (in generale, da una mappa biettiva). Inoltre, essendo il $+$ su $\mathbb{C}$ abeliano, anche la curva risulta con questa struttura un gruppo abeliano. Per familiarizzare con la legge, rispondiamo alle seguenti domande:

- Qual è l'inverso $-P$ di un punto P?
- Quali sono i punti di 2-torsione?

Per la prima, notiamo che $-P$ è quel punto tale che $(-P) + P = O$, ovvero la retta per P e $-P$ interseca la curva nel simmetrico del punto all'infinito O, ovvero in O stesso, dunque è la retta verticale e $-P$ è il simmetrico di P.
Per la seconda, ricordiamo che la n-torsione di un gruppo abeliano è il sottogruppo degli elementi con ordine che divide n. Dunque in questo caso abbiamo l'elemento neutro e gli elementi di ordine esattamente 2; questi ultimi soddisfano $2P = O \iff P = -P$ e quindi dal punto precedente sono i punti con $y = 0$, ovvero i punti con ascissa una delle 3 radici del polinomio di Weierstrass. E' un'immediata verifica dalla definizione della legge di gruppo che il sottogruppo di 2-torsione è isomorfo a $(\mathbb{Z}/2\mathbb{Z})^2$.
Osserviamo che sul toro, ovvero su un parallelogramma fondamentale per il reticolo L (che è unico a meno di omotetia) corrispondente a E, la 2-torsione, e in generale la n-torsione, è molto semplice da descrivere: sia L generato da ω_1, ω_2, allora i punti di ordine n sono tutti e soli quelli della forma

$$k\frac{\omega_1}{n} + l\frac{\omega_2}{n},\ 0 \leq k, l < n \tag{18}$$

mentre quelli di ordine esattamente n sono quelli come in (18) con almeno uno tra k e l coprimo con n.
Vedremo nel prossimo capitolo l'importanza della 2-torsione.

Consideriamo ora una curva $E/\mathbb{Q}$ definita su $\mathbb{Q}$. Dalla descrizione della legge di gruppo, segue immediatamente che l'insieme dei punti razionali è un sottogruppo: lo chiameremo *Gruppo di Mordell-Weil* della curva, e lo denoteremo con $E(\mathbb{Q})$.

3 Il gruppo di Mordell-Weil

Questo capitolo ricalca molto fedelmente il capitolo 3 del testo [3] di Silverman e Tate, a cui si rimanda per le dimostrazioni che verranno talvolta omesse.
In queso capitolo lavoriamo con curve ellittiche definite su $\mathbb{Q}$.

3.1 Il Teorema di Mordell

Il nostro obiettivo è comprendere il meglio possibile la struttura del gruppo di Mordell-Weil di una curva ellittica. Il teorema principale in questo senso è il seguente:

Teorema 3.1.1 (Mordell, 1922) *Sia $E/\mathbb{Q}$ una curva ellittica definita su $\mathbb{Q}$. Allora $E(\mathbb{Q})$ è un gruppo abeliano finitamente generato.*

La dimostrazione di questo risultato, a cui dedichiamo gran parte di questo capitolo, fa estensivamente uso dell'altezza di Weil.

Lemma 3.1.2 (di discesa) *Sia $(G,+)$ un gruppo abeliano tale che esista una funzione $h : G \to [0,\infty)$ che soddisfi le seguenti proprietà:*

1. *$\forall M \geq 0$, l'insieme $\{g \in G \mid h(g) \leq M\}$ è finito (Proprietà di Northcott)*
2. *$\forall g_0 \in G \ \exists\ k_0 \geq 0 \ : \ h(g+g_0) \leq 2h(g) + k_0 \ \forall g \in G$*
3. *$\exists\ k \geq 0 \ : \ h(2g) \geq 4h(g) - k \ \forall g \in G$*
4. *L'indice di $2G$ in G è finito*

Allora G è finitamente generato.

Dimostrazione: da (4) possiamo scegliere n elementi $\gamma_1, ..., \gamma_n$ di G come rappresentanti delle classi laterali di $2G$. Dato $g_0 \in G$ vale dunque che

$$\exists i_1 \in \{1, ..., n\},\ g_1 \in G \ : \ g_0 - \gamma_{i_1} = 2g_1$$

Possiamo ripetere questo procedimento per g_1 ottenendo γ_{i_2} e g_2; iterando N volte otteniamo la scrittura

$$g_0 = \gamma_{i_1} + 2\gamma_{i_2} + ... + 2^{N-1}\gamma_{i_{N-1}} + 2^N g_N$$

Ora è sufficiente mostrare che esiste $K \geq 0$ con la proprietà che per ogni $g_0 \in G$ esista N tale che $h(g_N) \leq K$ (dove g_N è quello definito dal procedimento sopra). In questo caso, g_0 sta nel sottogruppo generato dai γ_i e dai $\{g \in G \mid h(g) \leq K\}$. Anche questo secondo insieme è finito per la proprietà 1 e quindi per arbitrarietà di g_0 si ha la tesi.
Per mostrare la parte mancante, usiamo (2) e (3). Consideriamo la relazione

$$g_{j-1} - \gamma_{i_j} = 2g_j$$

Applicando h e usando 3 otteniamo

$$4h(g_j) \leq h(2g_j) + k = h(g_{j-1} - \gamma_{i_j}) + k$$

Tuttavia grazie a (2) possiamo stimare RHS in funzione solo di $h(g_{j-1})$: siano $k_1, ..., k_n$ le costanti come in (2) relative ai $\gamma_1, ..., \gamma_n$ e sia $\tilde{k} := max\{k_i\}$. Allora

$$h(g_{j-1} - \gamma_{i_j}) \leq 2h(g_{j-1}) + \tilde{k}$$

da cui

$$4h(g_j) \leq 2h(g_{j-1}) + k + \tilde{k} \Rightarrow h(g_j) \leq \frac{3}{4}h(g_{j-1}) - \frac{1}{4}(h(g_{j-1} - (k + \tilde{k}))$$

e quindi se $h(g_{j-1}) \geq k + \tilde{k}$ allora

$$h(g_j) \leq \frac{3}{4}h(g_{j-1})$$

che implica quanto voluto con $K = k + \tilde{k}$. $\square$

Come anticipato, per un punto $P = (x, y) \in E(\mathbb{Q})$ definiamo:

$$h(P) := h(x)$$

con h l'altezza logaritmica di Weil. Sappiamo quindi che per $(E(\mathbb{Q}), +)$ con questa altezza la proprietà 1 è soddisfatta per il Teorema di Northcott. Ci rimangono da verificare le altre tre prorietà.
Vediamo la 2:

Proposizione 3.1.3 *Sia $E : y^2 = x^3 + Ax + B$ una curva ellittica, allora per ogni $P_0 \in E$ $\exists C_0 \geq 0 : h(P + P_0) \leq 2h(P) + C_0$ $\forall P \in E$.*

Dimostrazione: Preliminarmente, facciamo la ben nota osservazione che ogni punto razionale su E, con numeratore e denominatore ridotti ai minimi termini, si scrive nella forma

$$P = (\frac{m}{e^2}, \frac{n}{e^3}) \tag{19}$$

Infatti posto $(\frac{m}{p}, \frac{n}{q}) \in E(\mathbb{Q})$, sostituendo nell'equazione è immediato trovare $q^2|p^3$ e $p^3|q^2$, da cui $p^3 = q^2$ che è quanto detto.
Innanzitutto fissiamo $C_0 \geq max\{h(P_0), h(2P_0)\}$ per avere la tesi nei casi $P \in \{O, P_0\}$. Inoltre notiamo che se $P_0 = O$ la tesi è vera per qualunque C_0.
Sia dunque

$$P_0 = (\frac{a_0}{d_0^2}, \frac{b_0}{d_0^3}) = (x_0, y_0),\ P = (\frac{a}{d^2}, \frac{b}{d^3}) = (x, y) \tag{20}$$

Abbiamo visto nel capitolo precedente la formula di somma per la quale, nei casi non degeneri come quello in esame,

$$x(P+P_0) = \left(\frac{y-y_0}{x-x_0}\right)^2 - x - x_0 \tag{21}$$

Sostituendo in (20) e usando l'equazione della curva per i termini y_0^2, y^2 otteniamo

$$x(P+P_0) = \frac{(aa_0 + Ad^2d_0^2)(ad_0^2 + a_0d^2) + 2Bd^4d_0^4 - 2bdb_0d_0}{(ad_0^2 - a_0d^2)^2}$$

da cui

$$H(x(P+P0)) \leq C_1 max\{|a|^2, |d|^4, |bd|\}. \tag{22}$$

Mentre

$$H(x) = max\{|a|, d^2\}. \tag{23}$$

Quindi ci serve soltanto controllare il quadrato dell'altezza della coordinata y di un punto in funzione di quella della sua coordinata x, ma questo si può fare, infatti poichè P appartiene alla curva, sostituendo nell'equazione e moltiplicando per il denominatore comune si ha $b^2 = a^3 + Aad^4 + Bd^6 \Rightarrow |b| \leq C_2 max\{|a|^{\frac{3}{2}}, |d|^3\}$ che unitamente a (22) dà

$$H(x(P+P0)) \leq C_3 max\{a^2, d^4\} = C_3 H(x(P))^2$$

e prendendo il logaritmo si ha quanto voluto.

L'idea della 3 è simile, si usa la formula di duplicazione e sempre il sostituire nell'equazione della curva, ma le manipolazioni algebriche e le stime sono più involute e dunque la omettiamo; è comunque riportata nel dettaglio nel testo indicato a inizio capitolo.

La 4 è invece più profonda e, come vedremo nella prossima sezione, ci permetterà di introdurre e stimare una quantità che sarà estrememente rilevante in seguito, il *rango*.
Non dimostreremo 4 per tutte le curve ellittiche definite su $\mathbb{Q}$, ma solo per quelle con almeno un punto di 2-torsione razionale, che sono quelle per cui otterremo il nostro risultato: il caso generale richiede infatti l'impiego di alcuni concetti di geometria algebrica che, seppur non particolarmente avanzati, non sono il tema di questa trattazione.

3.2 Discriminante e Discesa via 2-isogenia

Prima di procedere con la dimostrazione della proprietà 4 nel caso in esame, introduciamo una quantità che ci sarà particolarmente utile.

Definizione 3.2.1 *Dato un polinomio monico di terzo grado* $q(t) = t^3 + at^2 + bt + c$*, definiamo discriminante del polinomio la quantità* $\Delta(q) = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$ *dove* $\alpha_1, \alpha_2, \alpha_3$ *sono le radici di* q*.*

Osservazione 3.2.1.1 $\Delta(q) \neq 0 \iff q$ *ha radici distinte.*

Definizione 3.2.2 *Data una cubica in forma di Weierstrass (intera)* $y^2 = A(x)$ *definiamo il suo discriminante come* $\Delta_E = 16\Delta(A) = -16(4A^3 + 27B^2)$*.*

Osservazione 3.2.2.1 *Le curve ellittiche hanno discriminante non nullo.*

Vogliamo dunque dimostrare la seguente:

Proposizione 3.2.1 *Data una curva ellittica in forma di Weierstrass* $E : y^2 = A(x)$ *con* $A \in \mathbb{Q}[x]$ *avente almeno una radice razionale,* $E(\mathbb{Q})/2E(\mathbb{Q})$ *è un gruppo finito.*

Possiamo semplificare il problema innanzitutto portando la curva ad avere coefficienti interi con la trasformazione già vista e poi, con una traslazione, supponendo che la radice razionale sia $0 : E$ non sarà più dunque in forma di Weierstrass, bensì nella forma

$$y^2 = x^3 + ax^2 + bx, \ a, b \in \mathbb{Z} \tag{24}$$

Osservazione 3.2.2.2 *Notiamo che il discriminante è lo stesso della forma di Weierstrass in quanto non viene alterato dalle traslazioni per la Definizione* 3.2.1*, e che in questa forma è dato da* $\Delta = b^2(a^2 - 4b)$*.*

Prima di procedere diamo una rapida definizione:

Definizione 3.2.3 *Sia* $w : \mathbb{Z}^+ \to \mathbb{N}$ *la funzione che a ogni intero positivo associa il numero dei suoi fattori primi senza molteplicità, i.e.* $w(n) = |\{p \text{ primo} \mid p \text{ divide } n\}|$

Osservazione 3.2.3.1 *Se* $n = jk$ *si ha* $w(n) \leq w(j) + w(k) \leq 2w(n)$ *da cui* $w(\Delta) \leq w(b^2) + w(a^2 - 4b) = w(b) + w(a^2 - 4b) \leq 2w(\Delta)$

Vale:

Proposizione 3.2.2 *Sia* E *una curva ellittica come in* (124)*. Allora*

$$[E(\mathbb{Q}) : 2E(\mathbb{Q})] \leq 2^{2w(\Delta)+2} \tag{25}$$

Osservazione 3.2.3.2 *Grazie all'Osservazione* 3.2.2.2*, se* (25) *vale per curve come in* (24) *allora vale per ogni curva con un punto di* 2*-torsione razionale, in quanto ovviamente le mappe del tipo* $(x, y) \mapsto (x - r, y), r \in \mathbb{Q}$ *inducono isomorfismi dei rispettivi gruppi di Mordell-Weil.*

Dimostrazione: La dimostrazione è molto lunga e si basa su vari risultati intermedi, per cui vi dedicheremo l'intera sezione.

Lemma 3.2.3 *Siano* $(G,+),(H,+)$ *gruppi abeliani e siano* $\phi : G \to H$, $\psi : H \to G$ *due omomorfismi tali che*

- $\psi \circ \phi(a) = 2a \ \forall a \in A$
- $\phi \circ \psi(b) = 2b \ \forall b \in B$
- $\phi(A)$ *ha indice finito in* B
- $\psi(B)$ *ha indice finito in* A

Allora $[G : 2G] \leq [A : \psi(B)][B : \phi(A)]$.

La dimostrazione di questo Lemma, che si trova nella letteratura indicata a inizio capitolo, è un esercizio di teoria dei gruppi elementare.
L'aver enunciato questo Lemma suggerisce che il prossimo passo sia *spezzare* l'omomorfismo di moltiplicazione per 2 sulla curva con l'ausilio di una curva *gemella,* mostrare che gli indici delle immagini sono finiti e applicare il Lemma, che è infatti la strada che seguiremo.
La tecnica che utilizziamo per spezzare la moltiplicazione per 2 è la discesa via 2-isogenia: considerando solo la nostra curva ellittica, non risulta immediato come trovare quest'altra curva e queste due mappe che stiamo cercando. Tuttavia, se ci ricordiamo della provenienza complessa delle curve ellittiche, tutto diventa più chiaro: gli endomorfismi di moltiplicazione hanno in questo caso un'interpretazione geometrica molto più semplice che è possibile visualizzare, ad esempio considerando un parallelogramma fondamentale D. La moltiplicazione per 2 induce un rivestimento di grado 4 dato dalle 4 copie contenute in D del parallelogramma D_2 con generatori dati da metà di quelli di partenza. Notiamo che D_2 si ottiene in due passaggi prima dimezzando lungo un generatore e poi dimezzando anche lungo l'altro. Per quanto visto sulle isogenie nel secondo capitolo, in particolare la Proposizione 2.1.2, le curve ellittiche $E, \tilde{E}$ raltive a D e D_2 sono isomorfe, mentre esiste un omomorfismo da E a $\tilde{E}$, quella relativa a D_1, (e viceversa), perché esiste tra i rispettivi tori: questo omomorfismo è la 2-isogenia.
L'idea adesso è che possiamo dimezzare rispetto al generatore il cui punto medio M corrisponde tramite l'esponenziale di Weierstrass al nostro punto di 2-torsione razionale; grazie alla teoria delle funzioni ellittiche è possibile ricavare i coefficienti di $\tilde{E}$ e una formula per le due mappe di proiezione considerate, in sostanza sfruttando il fatto, di natura puramente combinatorica, che

$$\wp_1(z) = \wp(z) + \wp(z+M) - \wp(M) \tag{26}$$

Notiamo che il punto medio Q dell'altro generatore viene mandato da $\wp_1$ in una radice del polinomio di Weierstrass per $\tilde{E}$, perciò da (26) si ha $\wp_1(Q) = \wp(Q) + \wp(P+Q) - \wp(P) = -2\wp(P)$ che è ancora razionale.
Si trova dunque che se E viene portata nella forma (24), allora i coefficienti di $\tilde{E}$ sempre in questa forma sono

$$\tilde{a} = -2a, \tilde{b} = a^2 - 4b \tag{27}$$

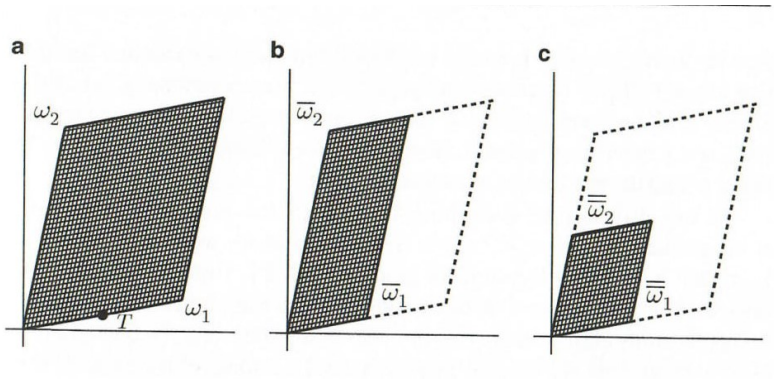

Figura 2: I parallelogrammi fondamentali coinvolti nella discesa via 2-isogenia

Algebricamente possiamo riassumere tutto nel modo seguente:

Lemma 3.2.4 *Date $E, \tilde{E}$ nella forma di (24) e dati $T = (0,0) \in E, \tilde{T} = (0,0) \in \tilde{E}$,*

1. *La funzione ϕ definita da*

$$\phi(P) = \begin{cases} (\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}) & \text{se } P = (x,y) \neq O, T \\ \tilde{O} & \text{altrimenti} \end{cases} \tag{28}$$

   è un omomorfismo da E in $\tilde{E}$ con kernel $\{O, T\}$

2. *La funzione $\tilde{\phi} : \tilde{E} \to \tilde{\tilde{E}}$ definita algebricamente in modo analogo (ma con i coefficienti di $\tilde{E}$) è un omomorfismo con kernel $\{\tilde{O}, \tilde{T}\}$ da $\tilde{E}$ alla curva $\tilde{\tilde{E}} : y^2 = x^3 + 4ax^2 + 16bx$ che è isomorfa a E tramite la mappa $u : (x,y) \mapsto (\frac{x}{4}, \frac{y}{8})$.*

3. *Posto $\psi = u \circ \tilde{\phi}$, la composizione $\psi \circ \phi : E \to E$ è l'endomorfismo di moltiplicazione per 2 (e lo stesso vale per $\phi \circ \psi : \tilde{E} \to \tilde{E}$).*

Remark: Omettiamo la dimostrazione algebrica che ϕ è effettivamente un omomorfismo e che mappa E in $\tilde{E}$, che consiste in laboriose verifiche non partacolarmente illuminanti. Rimarchiamo invece che questa mappa è la "traduzione" algebrica della 2-isogenia che abbiamo visto sui tori corrispondenti alle curve, che è chiaramente un omomorfismo con le proprietà desiderate, e che può essere ottenuta senza bisogno di verifiche algebriche scrivendo la trasformazione delle funzioni di Weierstrass dei due rispettivi reticoli. Inoltre, supposto ϕ sia un omomorfismo, è immediato verificare che il kernel sia quello indicato. Il secondo punto segue immediatamente dal primo notando che $-2(-2a) = 4a$ e $(4a)^2 - 4(a^2 - 4b) = 16b$. Omettiamo anche la dimostrazione di 3, per la stassa ragione di 1.

Dunque abbiamo spezzato la mappa di moltiplicazione per 2 nel modo desiderato. Dalle definizioni è chiaro che ϕ mappa $E(\mathbb{Q})$ in $\tilde{E}(\mathbb{Q})$ e ψ viceversa. Enunciamo dunque l'ultimo risultato necessario per la dimostrazione della Proposizione 3.2.2:

Proposizione 3.2.5 *Posti $s = w(a^2 - 4b)$ e $t = w(b^2) = w(b)$, vale*

$$[B : \phi(A)] \leq 2^{s+1},\ [A : \psi(\tilde{B})] \leq 2^{t+1} \tag{29}$$

ove

$$A = E(\mathbb{Q}),\ B = \tilde{E}(\mathbb{Q})$$

notazione che adotteremo per il resto del capitolo.

Dimostrazione: Chiaramente, per simmetria ($\tilde{b} = a^2 - 4b$) è sufficiente verificare la prima disuguaglianza. Per fare ciò diamo una completa descrizione di $\phi(A) \subset B$.

Lemma 3.2.6 *1. $\tilde{O} \in \phi(A)$*

2. Dato $(0,0) \neq \tilde{P} = (\tilde{x}, \tilde{y}) \in B$, $\tilde{P} \in \phi(A) \iff \tilde{x}$ è il quadrato di un numero razionale.

3. $\tilde{T} \in \phi(A) \iff a^2 - 4b$ è un quadrato perfetto.

Dimostrazione:

1. $\tilde{O} = \phi(O)$

2. L'implicazione $\Rightarrow$ segue immediatamente da (28). Per l'altra, sia $\tilde{x} = d^2$, $0 \neq d \in \mathbb{Q}$. Vogliamo trovare $(x, y) \in E$ tale che $\frac{y}{x} = d$. Messa a sistema con l'equazione per E, sfruttando $d \neq 0$, questa condizione dà

   $$x^2 + (a - d^2)x + b = 0$$

   Vogliamo dunque verificare che il discriminante $(a-d^2)^2-4b$ sia il quadrato di un razionale. Ma $(a - d^2)^2 - 4b = (a - \tilde{x})^2 - 4b = \tilde{x}^2 - 2a\tilde{x} + a^2 - 4b = \frac{\tilde{x}^3+\tilde{a}\tilde{x}^2+\tilde{b}\tilde{x}}{\tilde{x}} \overset{(27)}{=} \frac{\tilde{y}^2}{d^2}$ □

3. $\tilde{T} \in \phi(A) \iff \exists (x, y) \in A : y = 0,\ x \neq 0 \iff x^2 + ax + b$ ha radici razionali $\iff a^2 - 4b \neq 0$ □

Sappiamo dunque che l'immagine di A sotto ϕ è composta da tutti i punti con ordinata $\tilde{x}$ il quadrato di un razionale non nullo, dal punto all'infinito $\tilde{O}$ e anche da $\tilde{T}$ se e solo se $a^2 - 4b$ è un quadrato perfetto.
Sfruttiamo questa caratterizzazione per ottenere (29): Consideriamo l'omomorfismo

$$\pi : B \to \mathbb{Q}^*/\mathbb{Q}^{*2} : \tilde{P} = (\tilde{x}, \tilde{y}) \mapsto \begin{cases} \tilde{x}\ (mod\ \mathbb{Q}^{*2}) & \text{se } \tilde{P} \neq \tilde{O}, \tilde{T} \\ 1\ (mod\ \mathbb{Q}^{*2}) & \text{se } \tilde{P} = \tilde{O} \\ b\ (mod\ \mathbb{Q}^{*2}) & \text{se } \tilde{P} = \tilde{T} \end{cases} \tag{30}$$

Come consuetudine omettiamo la verifica che si tratti di un omomorfismo.

Lemma 3.2.7 *1.* $\ker \pi = \phi(A)$*, da cui* π *induce un omomorfismo iniettivo* $B/\phi(A) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$*.*

2. L'immagine di π *è il sottogruppo di* $\mathbb{Q}^*/\mathbb{Q}^{*2}$ *costituito dagli elementi della forma* $\pm p_1^{\upsilon_1} \cdot \ldots \cdot p_s^{\upsilon_s}$ *ove i* p_i *sono i primi che dividono* $a^2 - 4b$ *e* $\upsilon_i = 0$ *o* 1 $\forall i$

Dimostrazione: Le immagini di $\tilde{O}, \tilde{T}$ stanno nell'insieme indicato, quindi ci rimane da verificarlo per i punti $(\tilde{x}, \tilde{y})$ con $\tilde{x} \neq 0$. Sappiamo dalla sezione precedente che tali punti (si intende sempre con numeratore e denominatore coprimi) si scrivono come in (19) da cui, preso un punto in quella forma, sostituendo ancora nell'equazione otteniamo

$$n^2 = m(m^2 + \tilde{a}me^2 + \tilde{b}e^4) \tag{31}$$

Posto $d = mcd(m, m^2 + \tilde{a}me^2 + \tilde{b}e^4)$, essendo m ed e coprimi otteniamo $d|b$.
Perciò da (31) segue che essendo LHS un quadrato, m è un quadrato moltiplicato per un divisore di d, e quindi di b, con tutti gli esponenti dei primi che lo dividono al più 1, che è quanto voluto. Notiamo infine che dal Lemma 3.2.7 segue la Proposizione 3.2.5 perché per il punto 1 l'indice è al più la cardinalità dell'immagine di B sotto π, che per il 2 ha al più 2^{s+1} elementi perché ci sono s primi, 2 scelte di esponente per ciascuno e la scelta del segno.
Infine, la Proposizione 3.2.2 segue facilmente dal Lemma 3.2.3 applicato ai due gruppi di Mordell-Weil e agli omomorfismi costruiti nel Lemma 3.2.4, visto che per la Proposizione 3.2.5

$$[A : \psi(B)][B : \phi(A)] \leq 2^{w(b)+1} \cdot 2^{w(a^2-4b)+1} \overset{(3.2.3.1)}{\leq} 2^{2w(\Delta)+2} \tag{32}$$

Per quanto visto nella sezione precedente, questo in particolare ci dà il Teorema di Mordell. Tuttavia è proprio l'*effettività* della stima sull'indice di $2E(\mathbb{Q})$ in $E(\mathbb{Q})$ ottenuta grazie alla 2-torsione razionale che ci permetterà un controllo sul numero di generatori liberi che $E(\mathbb{Q})$ può avere, come vedremo nella sezione seguente.

3.3 Il rango

L'argomentazione presentata in questa sezione è breve, ma la stima che otteniamo è davvero fondamentale per il risultato finale, per questo vi riserviamo un'intera sezione.
Sappiamo ora che per una curva ellittica E con un punto di 2-torsione razionale, il gruppo di Mordell-Weil $E(\mathbb{Q})$ è finitamente generato. Come detto nella sezione precedente, ciò vale anche senza l'ipotesi sulla 2-torsione, ma quello che invece non vale in generale è la Proposizione 3.2.2.
Scriviamo dunque, grazie al Teorema di Classificazione dei gruppi abeliani finitamente generati,

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times T \tag{33}$$

con $r \in \mathbb{N}$ e T gruppo abeliano finito, detto *sottogruppo di torsione*.
Vedremo nel prossimo capitolo che ciò che è davvero importante controllare per stimare il numero di punti razionali ad altezza fissata è invece r, il *rango*.

Teorema 3.3.1 *Sia E una curva ellittica con un punto di 2-torsione razionale, con rango r e discriminante Δ. Allora si ha*

$$r \leq 2w(\Delta) + 2 \tag{34}$$

Dimostrazione: Sia di nuovo $E(\mathbb{Q}) = A$ per convenienza.
Guardiamo il gruppo quoziente $A/2A$: da (33) si ha

$$A/2A \simeq (\mathbb{Z}/2\mathbb{Z})^r \times \prod_{i=1}^{k} \mathbb{Z}_{p_i^{\varepsilon_i}}/2\mathbb{Z}_{p_i^{\varepsilon_i}} \tag{35}$$

dove abbiamo scritto $T = \prod_{i=1}^{k} \mathbb{Z}_{p_i^{\varepsilon_i}} := \prod_{i=1}^{k} \mathbb{Z}/p_i^{\varepsilon_i}\mathbb{Z}$ grazie al Teorema di Classificazione dei gruppi abeliani finiti.
Guardando (35) in termini di cardinalità otteniamo dunque $[A : 2A] \geq 2^r$, da cui, usando la Proposizione 3.2.2 per l'indice, si ha

$$2^r \leq 2^{2w(\Delta)+2} \Rightarrow r \leq 2w(\Delta) + 2 \tag{36}$$

Remark: Potremmo ottenere anche $r \leq 2w(\Delta) + 1$ notando che se $p \neq 2$, $\mathbb{Z}_{p_i^{\varepsilon_i}}/2\mathbb{Z}_{p_i^{\varepsilon_i}}$ è il gruppo banale, mentre se $p = 2$ esso è isomorfo a $\mathbb{Z}/2\mathbb{Z}$; ma è chiaro che a ognuno dei diversi fattori $\mathbb{Z}/2^{\varepsilon_i}\mathbb{Z}$ corrisponde un diverso punto di 2-torsione non banale in A, e sappiamo essercene 1 oppure 3, da cui il leggero miglioramento, che in ogni caso non è rilevante per le stime sul numero di punti razionali.

Notiamo che la disuguaglianza del Teorema 3.3.1 mette a confronto due quantità che hanno una natura *diversa*: infatti, fissata la curva ellittica E, il suo rango è ben definito, dipendendo solo dalla struttura astratta di $E(\mathbb{Q})$, mentre il discriminante dipende dal modello (intero), ovvero dall'equazione, che scegliamo per E. Chiaramente il Teorema vale indipendentemente dalla scelta del modello, non avendone usato uno particolare, ma è più interessante quando scegliamo un modello che minimizza $w(\Delta)$. Questo è sostanzialmente equivalente a minimizzare $|\Delta|$, in quanto c'è un insieme di primi di cui discuteremo nel capitolo 6, detti di *cattiva riduzione per E*, che dividono Δ in ogni modello. Chiameremo un modello che minimizza $|\Delta|$ *minimale* e il relativo discriminante *discriminante minimale per E*. Nel capitolo 6 vedremo che la scelta di un modello minimale è utile quando si vogliono stimare delle quantità *locali*, ovvero legate alla struttura della curva ellittica quando guardata "modulo p" con p primo.

4 L'altezza canonica

4.1 Definizione e proprietà

L'idea che consente il controllo del numero di punti razionali ad altezza limitata è naturale: essendo il gruppo di Mordell-Weil finitamente generato, se troviamo che l'altezza dei punti cresce *molto* sotto gli endomorfismi di moltiplicazione, avremo chiaramente che non ci possono essere *troppi* punti ad altezza limitata. Cerchiamo di formalizzare questa strategia: abbiamo già detto che l'altezza di Weil soddisfa la proprietà $h(2P) = 4h(P) + O(1)$ con l'errore dipendente dalla curva. Usando il fatto che $\wp(mz)$ è una funzione razionale in $\wp(z)$ di grado m^2 (si veda 2.2.4), non è difficile generalizzare gli stessi metodi per mostrare che

$$h(mP) = m^2 h(P) + O_m(1) \tag{37}$$

La crescita di h sotto l'endomorfismo di moltiplicazione per m è dunque quadratica in m, tuttavia c'è un errore che dipende da m e dalla curva. Questo errore rende questa scelta di altezza, seppur naturale per introdurre il problema, non ottimale per ottenere i risultati accurati che cerchiamo (sebbene, come in sostanza visto, sia sufficiente per ricavare il Teorema di Mordell). Dobbiamo dunque introdurre un'altezza in un certo senso più fine:

Proposizione 4.1.1 *Data $E/\mathbb{Q}$ curva ellittica, per ogni $P \in E(\mathbb{Q})$ l'espressione*

$$lim_{n\to\infty} 4^{-n} h(2^n P)$$

è ben definita e finita.

Dimostrazione: mostriamo che la sequenza $a_n = 4^{-n}h(2^n P)$ è di Cauchy per ogni P. Prendendo $m = 2$ in (37), troviamo che esiste c_2 tale che

$$|h(2P) - 4h(P)| < c_2 \ \forall P \in E$$

Dunque, telescopizzando, troviamo

$$|a_n - a_m| = |\sum_{k=m}^{n-1} 4^{-k-1} h(2^{k+1}P) - 4^{-k}h(2^k P)| \leq |\sum_{k=m}^{n-1} 4^{-k} c_2| \leq 4^{-m+1}\frac{c_2}{3}$$

usando (37) su $2^k P$ □

Definizione 4.1.1 $\hat{h}(P) := lim_{n\to\infty} 4^{-n} h(2^n P)$ *è detta altezza canonica o altezza di Néron-Tate.*

Proposizione 4.1.2 *L'altezza canonica soddisfa le seguenti proprietà:*

1. $|\hat{h}(P) - h(P)| = O(1)$ *(sempre fissata E)*
2. $\hat{h}(mP) = m^2 h(P)$

3. $\hat{h}(P) = 0 \iff P$ *è di torsione*

4. $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$

Per ogni $P, Q \in E(\mathbb{Q}), m \in \mathbb{Z}$

Dimostrazione:

1. notiamo che nel dimostrare la Proposizione precedente abbiamo trovato che $|a_n - a_m| \leq 4^{-m} c_3 \ \forall n \geq m \geq 0$. Da ciò, ponendo $m = 0$ e notando che $a_0 = h(P)$ e $\hat{h}(P) = lim_{n\to\infty} a_n$ troviamo $|\hat{h}(P) - h(P)| \leq c_3$.

2. $\hat{h}(mP) = lim_{n\to\infty} 4^{-n} h(2^n(mP)) = lim_{n\to\infty} 4^{-n} h(m(2^n P)) = lim_{n\to\infty} 4^{-n}(m^2 h(2^n P) + O_m(1)) = m^2 \hat{h}(P)$.

3. Se P è di torsione esiste m tale che $mP = 0$, da cui segue $\Rightarrow$. Per $\Leftarrow$, notiamo che se P non è di torsione allora $\{\mathbb{N}P\} := \{Q \in E(\mathbb{Q}) | \ \exists m \in \mathbb{N} \mid Q = mP\}$ è infinito, dunque per il Teorema di Northcott esistono elementi di $\mathbb{N}P$ con altezza di Weil arbitrariamente alta, contraddicendo il punto 1 (perché avrebbero tutti altezza canonica 0 per il punto 2).

4. Si può mostrare che l'altezza di Weil soddisfa un analogo di questa formula con un termine di errore (per la dimostrazione si veda l'ulteriore testo di Silverman [4] a p. 235), al chè basta come per 1 applicare la definizione di $\hat{h}$ e il termine di errore scompare dividendo per 4^n.

Abbiamo quindi costruito il nostro strumento più fine, l'altezza canonica, con cui attaccare il problema. Prima di proseguire, facciamo l'importante osservazione che, grazie alle proprietà 2 e 4, l'altezza canonica è una forma quadratica (con relativa forma bilineare $b(P,Q) = \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q))$) semidefinita positiva sul gruppo di Mordell-Weil, e grazie alla terza è definita positiva sul quoziente per la torsione.
Ricordiamo ora però che la nostra questione è posta in termini di conteggio di punti con altezza di Weil limitata; il punto 1 della Proposizione 4.1.2 risponde alla domanda:

- Come sono legate $h(P)$ e $\hat{h}(P)$ per P un generico punto su una curva ellittica in forma di Weierstrass?

E in particolare ci dice che il Teorema 1.3.2 con $\hat{h}$ al posto di h implica il Teorema 1.3.2 standard, infatti ci basta osservare che

$$(Be^{c_3})^{c_0 \frac{1}{loglog(Be^{c_3})}} \leq B^{c_4 \frac{1}{loglogB}}$$

per un'altra costante assoluta che possiamo ad esempio prendere $c_4 = c_0(1 + c_3)$ in quanto $B > e$.

4.2 Applicazione al conteggio

Rimane in sospeso una questione più fondamentale:

- Come contiamo i punti con altezza canonica limitata da B?

Questa domanda è sicuramente più complicata da affrontare: l'approccio standard che si trova in letteratura consiste in sostanza di due idee distinte, applicate sinergicamente:

1. Ottenere dei bound per la quantità di punti con altezza *piccola*
2. Trasportare il problema in setting euclideo e utilizzare argomenti di ricoprimento per ottenere stime per B generico da quelli del punto 1.

Il punto 1 è sicuramente la parte più complessa a livello tecnico di questa tesi, trattandosi di risultati moderni, anche recenti. Tuttavia, le tecniche impiegate dai vari autori per ottenerli non richiedono lo sviluppo di teorie molto più profonde di quanto già esposto, bensì si basano su un impiego intelligente di tutte le sfaccettature geometriche, analitiche e complesse delle curve ellittiche, di cui speriamo di aver dato un'idea, di un concetto di *località* che sarà introdotto brevemente nel capitolo 6, e di un delicato controllo delle stime. Delineeremo dunque la dimostrazione dei due risultati che ci saranno utili, nel senso del primo punto, nei prossimi due capitoli.
Concentriamoci ora sul secondo punto: è qui che ci risulteranno davvero utili le proprietà che abbiamo dimostrato per l'altezza canonica. Impiegheremo l'operazione di prodotto tensore (su $\mathbb{Z}$) tra gruppi abeliani, che definiamo rapidamente:

Definizione 4.2.1 *Dati G, H gruppi abeliani, si definisce prodotto tensore di G e H, in simboli $G \otimes H = G \otimes_{\mathbb{Z}} H$ il quoziente del gruppo libero abeliano sull'insieme di simboli $\{g \otimes h,\ g \in G,\ h \in H\}$ per le relazioni:*

- $(g_1 + g_2) \otimes h = g_1 \otimes h + g_2 \otimes h \ \forall g_1, g_2 \in G,\ h \in H$
- $g \otimes (h_1 + h_2) = g \otimes h_1 + g \otimes h_2 \ \forall g \in G, h_1, h_2 \in H$

dove si è usato $+$ per denotare la legge di gruppo in ognuno dei tre gruppi coinvolti, perché non c'è ambiguità.

Osservazione 4.2.1.1 *Risulta immediato che $0_G \otimes h = 0 \ \forall h \in H$ (e analogamente $g \otimes 0_H = 0$), infatti $0_G \otimes h + 0_G \otimes h = (0_G + 0_G) \otimes h = 0_G \otimes h$.*

Osservazione 4.2.1.2 *Dall'osservazione precedente possiamo dedurre che, se in H è possibile la divisione per gli interi, nel senso che $\forall h \in H,\ n \in \mathbb{Z}^+ \ \exists h' \mid nh' = h$, allora la torsione di G va in 0, ovvero per ogni $g_0 \in G$ di torsione e per ogni $h \in H, g_0 \otimes H = 0$.*
Infatti $g_0 \otimes h = g_0 \otimes \frac{1}{m}h + ... + g_0 \otimes \frac{1}{m}h = mg_0 \otimes \frac{1}{m}h = 0_G \otimes \frac{1}{m}h = 0$ dove m è tale che $mg_0 = 0_G$ e nella seconda espressione la somma ha m addendi.

Consideriamo dunque $E(\mathbb{Q}) \otimes \mathbb{R}$ (sia $E(\mathbb{Q}) \equiv \mathbb{Z}^r \times T$). In $\mathbb{R}$ è possibile la divisione per m, da cui T va in 0 nel senso già descritto. E' dunque semplice costruire un isomorfismo di gruppi tra $(E(\mathbb{Q})/T) \otimes \mathbb{R}$ e $\mathbb{R}^r$: è sufficiente mandare gli elementi della forma $P_k \otimes 1$ in e_k, dove $P_1, ..., P_r$ sono generatori di $E(\mathbb{Q})/T$ e gli e_i sono gli elementi della base canonica. Le verifiche restanti sono meccaniche.
La forma quadratica definita positiva che $\hat{h}$ induceva su $E(\mathbb{Q})/T$ si trasporta naturalmente su $\mathbb{Z}^r \equiv E(\mathbb{Q}) \otimes 1 \hookrightarrow \mathbb{R}^r$. Possiamo dunque estenderla naturalmente a una forma quadratica su $\mathbb{Q}^r$ e poi per continuità a una su tutto $\mathbb{R}^r$. Non è tuttavia *a priori* detto che quest'estensione rimanga definita positiva, fatto che in generale è falso. Nel caso in esame però è vero, e lo dimostriamo grazie alla seguente Proposizione:

Proposizione 4.2.1 *Sia $L \subset \mathbb{R}^d$ un sottogruppo discreto (reticolo) contenente una base per $\mathbb{R}^d$ e sia $q : \mathbb{R}^d \to \mathbb{R}$ una forma quadratica che soddisfa:*

- $\forall\ P \in L, q(P) = 0 \iff P = 0$
- *l'insieme $\{P \in L \mid q(P) \leq C\}$ è finito per ogni $C \geq 0$*

Allora q è definita positiva.

Dimostrazione: La dimostrazione si basa su un celebre risultato di Geometria dei Numeri dovuto a Minkowski, a cui premettiamo un Lemma:

Lemma 4.2.2 (Blichfeldt) *Sia $\Sigma \subset \mathbb{R}^d$ Lebesgue-misurabile e sia $L \subset \mathbb{R}^d$ un reticolo $d-$dimensionale. Per semplicità denotiamo con $Vol(\cdot)$ la misura di Lebesgue in $\mathbb{R}^d$ e con $Vol(L)$ quella di un parallelepipedo fondamentale per L. Allora se $Vol(\Sigma) > kVol(L)$ con $k \in \mathbb{N}$, esiste un traslato di Σ che contiene almeno $k+1$ punti di L.*

Dimostrazione: il ruolo dell'intero k e del volume fa immediatamente pensare al *Pigeonhole principle*, che infatti andremo a usare.
Per trattare senza problemi con il volume supponiamo che Σ sia limitato, (mostrando la tesi per una sua intersezione per una palla sufficientemente grande da avere ancora l'ipotesi). Sia R un parallelepipedo fondamentale per L. Definiamo inoltre, per ogni $\mathbf{x} \in L,\ \Sigma_x := \Sigma \cap (R + \mathbf{x}) - \mathbf{x}$.
Essendo che gli insiemi $R+\mathbf{x}$ al variare di $\mathbf{x} \in L$ ricoprono Σ, si ha che la somma dei volumi degli insiemi $\Sigma_x \subset R$ è $Vol(\Sigma) > kVol(L)$, da cui per Pigeonhole esiste un punto $\mathbf{y} \in R$ che appartiene ad almeno $k+1$ di essi e quindi, per definizione di $\Sigma_x,\ \Sigma - \mathbf{y}$ contiene almeno $k+1$ punti di L. $\square$

Lemma 4.2.3 (Minkowski Convex Body) *Dato L come sopra e $B \subset \mathbb{R}^d$ convesso simmetrico rispetto all'origine con $Vol(B) > 2^d Vol(L)$, B contiene almeno un punto di L diverso dall'origine.*

Dimostrazione: Applichiamo il Lemma 4.2.2 a $\Sigma = \frac{1}{2}B$ con $k = 1$: le ipotesi sono soddisfatte ($Vol(\frac{1}{2}A) = 2^{-d}Vol(A)$ in $\mathbb{R}^d$) e otteniamo dunque che $\frac{1}{2}B$ contiene $w_1, w_2 \in L$, da cui per simmetria e convessità contiene $\frac{w_1 - w_2}{2}$ e quindi $w_1 - w_2 \in B$. $\square$

Tornando alla Proposizione 4.2.1, notiamo innanzitutto che le due condizioni nell'ipotesi implicano che esiste $0 < \lambda = min\{q(P) : P \in L - \{0\}\}$.
E' un risultato ben noto che data una forma quadratica $q(\mathbf{x})$ su $\mathbb{R}^d$ esistono $a, b \geq 0$ con $a + b \leq d$ e una base tale che $q(\mathbf{x}) = \sum_{i=1}^{a} x_i^2 - \sum_{i=1}^{b} x_{a+i}^2$. Supponiamo dunque la tesi sia falsa, e che dunque $a < d$. Allora se definiamo

$$B(\epsilon, \delta) := \{\mathbf{x} : \sum_{i=1}^{a} x_i^2 \leq \epsilon,\ \sum_{i=1}^{b} x_{a+1}^2 \leq \delta\}$$

vediamo che gli insiemi così definiti sono chiaramente simmetrici e convessi. Troviamo inoltre facilmente che, fissato $\epsilon, Vol(B(\epsilon, \delta))$ è infinito se $a + b < d$ (c'è una componente che posso prendere arbitrariamente grande) e cresce come $\delta^{\frac{b}{2}}$ altrimenti. In entrambi i casi, per il Lemma 4.2.3 esiste δ_0 tale che $B(\frac{1}{2}\lambda, \delta_0)$ contiene un punto $P \in L$; tuttavia allora $q(P) \leq \frac{1}{2}\lambda < \lambda$, da cui un assurdo.

Osservazione 4.2.1.3 *La forma quadratica che abbiamo definito su $\mathbb{R}^r$ soddisfa le ipotesi della Proposizione 4.2.1 con L l'immagine di $E(\mathbb{Q})/T$ sotto il tensore grazie alla prorietà di Northcott, da cui è definita positiva.*

Possiamo dunque utilizzare $\hat{h}$ per dotare il nostro spazio ambiente anche di una struttura metrica, oltra a quella di gruppo, che ricordiamo è l'unica avere al momento. Possiamo infatti porre senza perdita di generalità che $\hat{h}$ sia la norma euclidea $|.|^2$, da cui L è isomorfo a $\mathbb{Z}^r$ solo come gruppo, ma geometricamente è un reticolo $d-$dimensionale qualunque.
Il problema di conteggio che vogliamo affrontare è dunque ora riformulabile come stimare la cardinalità dell'insieme

$$|T| \cdot \{x \in L \cap \mathcal{B}(0, \sqrt{logB})\} \tag{38}$$

E' un risultato avanzato di B.Mazur (si veda [5]) che il sottogruppo di torsione del gruppo di Mordell-Weil di una curva ellittica definita su $\mathbb{Q}$ abbia solo un numero finito di possibilità (che in particolare si è anche in grado di classificare), da cui il valore di T è uniformemente limitato e quindi quando andremo a fare le stime conclusive lo tratteremo come una costante. Rimarchiamo che tutta l'argomentazione che segue, compresa la stima finale del Teorema 1.3.2, si può ottenere senza invocare il risultato di Mazur, ma semplicemente mostrando che in (38) il termine $|T|$ è trascurabile (nel senso del conteggio) rispetto all'altro fattore. Questo può essere dedotto come semplice corollario dei risultati esposti nel capitolo 6, ad esempio, ma abbiamo preferito non soffermarvici in quanto non è la parte interessante della stima.

5 Un risultato di Masser: punti con altezza ridotta

L'obiettivo principale di questa sezione sarà enunciare e delineare la dimostrazione di un importante risultato di D.Masser riguardo alla quantità di punti razionali con altezza canonica *piccola*, cruciale per lo sviluppo della nostra esposizione. Vale il seguente:

Teorema 5.0.1 (Masser, 1989) *: Esiste una costante assoluta $K > 0$ tale che per ogni curva ellittica $E/\mathbb{Q}$ in forma di Weierstrass con altezza logaritmica $w = log(H(E))$, il numero di punti $P \in E(\mathbb{Q})$ con altezza $\hat{h}(P) < 1/K$ è al più $Kw^{3/2}$.*

5.1 Preliminari: quantità e funzioni notevoli

In questa sezione vengono presentati degli oggetti legati non solo alla teoria delle funzioni ellittiche nel setting di un parallelogramma fondamentale, che abbiamo anche già affrontato, ma in piccola parte anche a quella delle funzioni modulari. Per i pochissimi prerequisiti, come il concetto di Gruppo Modulare e di dominio fondamentale per la sua azione, si rimanda sempre a [2].
Si specifica che in questo capitolo vengono impiegate molte costanti assolute di non particolare importanza (non ci si riferisce ovviamente a quella del Teorema 5.0.1): per queste impiegheremo la notazione c_k, senza ulteriori specifiche.
La dimostrazione del Teorema utilizza la tecnica standard delle funzioni ausiliarie in teoria della trascendenza, ma prima di vederne l'applicazione abbiamo bisogno di un set-up: sappiamo che esistono ω_1, ω_2 complessi con $Im(\frac{\omega_1}{\omega_2}) \neq 0$ che generano un reticolo Ω il cui toro associato è biolomorfo a E tramite la mappa di Weierstrass exp_E. Possiamo nella maniera usuale trovare $\tau \in D \subset H$ tale che $(1, \tau)$ generi Ω, con D il dominio fondamentale standard per l'azione del gruppo modulare. Data A l'area di un dominio fondamentale per Ω, definiamo:

$r(z) = \pi|z|/A$ e

$r(P) = min\{r(z) : exp_E(z) = P\}$

Sia inoltre $\frac{\sqrt{3}}{2} \leq \nu = \mathrm{Im}(\tau)$ e sia $\wp$ la funzione di Weierstrass relativa a Ω.
Il seguente Lemma è dunque una conseguenza del *Pigeonhole principle*:

Lemma 5.1.1 *: Dati $A \leq B$ interi positivi e $P_0, ..., P_B$ punti su E, esistono $A+1$ indici $0 \leq i_0 < ... < i_A$ e una costante assoluta c_{15} tali che*

$$r(P_{i_j} - P_{i_l}) \leq c_{15} max\{\frac{A}{B}, \nu(\frac{A}{B})^2\}$$

Definiamo inoltre

$$\gamma = max\{\sqrt{\frac{|g_2|}{4}}, \sqrt[3]{\frac{|g_3|}{4}}\}$$

Osservazione 5.1.0.1 *Vale*

$$c_5^{-w} \leq \gamma \leq c_5^w \tag{39}$$

per la definizione di altezza della curva.

Vale il seguente:

Lemma 5.1.2 *Esiste una funzione intera $\theta_0(z)$ tale che anche $\theta(z) = \wp(z)\theta_0(z)$ sia intera e che $m(z) \coloneqq logmax(|\gamma\theta_0(z)|, |\theta(z)|)$ soddisfi*

$$|m(z) - r(z)| \leq c_5 w \ \forall z \in \mathbb{C} \tag{40}$$

per la cui dimostrazione, così come per quella del prossimo, rimandiamo al paper originale [6].

Lemma 5.1.3 $\nu \leq c_{16} w$.

5.2 Dimostrazione del Teorema

La chiave per la dimostrazione del Teorema è la seguente:

Proposizione 5.2.1 *: Esiste una costante assoluta $C_0 > 1$ tale che la quantità di punti $P \in E(\mathbb{Q})$ tali che*

$$max(\hat{h}(P), r(P)) < \frac{1}{C_0} \tag{41}$$

è al più $2C_0 w$.

Dimostrazione: suddividiamo la dimostrazione in diversi passi, delineandone prima la struttura. Mostriamo che per C_0 sufficientemente grande supporre falsa la tesi porta a un assurdo. Definiamo:

$$C = \sqrt[4]{C_0}, S = \lfloor C_0 w \rfloor, N = \lfloor \sqrt{S} \rfloor, L = \lfloor C^3 w \rfloor, T = \lfloor Cw \rfloor \tag{42}$$

E' immediato che $N^2 \leq S$. Eliminando dunque eventuali punti di N-torsione, abbiamo S punti $P_i = exp_E(u_i), 1 \leq i \leq S$ che soddisfano (41) e tali che $NP_i \neq 0$, dove le controimmagini u_i sono quelle che soddisfano la condizione $r(u_i) < \frac{1}{C_0}$.
Notiamo che le altezze di $\wp(u_s), \wp(Nu_s)$ sono limitate da w in quanto la prima è $< \frac{1}{C_0} < 1$ e la seconda è $\leq \frac{N^2}{C_0} \leq \frac{S}{C_0} \leq w$ (da cui i loro moduli sono limitati da c_7^w, fatto che utilizzeremo).

Consideriamo una funzione ausiliaria della forma:

$$f(z) = \sum_{l_1=0}^{L} \sum_{l_2=0}^{L} a(l_1, l_2) \wp(z)^{l_1} \wp(Nz)^{l_2} \tag{43}$$

Mostriamo innanzitutto che esiste un'opportuna scelta dei coefficienti $a(l_1, l_2)$, con modulo controllato da $exp(c_8 C^3 w^2)$, tale che f ha zeri di ordine almeno T su questi S punti. Ciò si traduce in un sistema di ST equazioni in $(L+1)^2$ incognite per i coefficienti, poichè avere uno zero di ordine T può essere riformulato come avere anche le prime $T-1$ derivate nulle. Chiaramente essendo $(L+1)^2 > ST$ una soluzione esiste. Per controllare il modulo dei coefficienti utiliziamo il seguente Lemma:

Lemma 5.2.2 (Siegel) *Siano $N > M$ interi positivi e sia dato un sistema*

$$a_{11} X_1 + ... + a_{1N} X_N = 0$$

...

$$a_{M1} X_1 + ... + a_{MN} X_N = 0$$

di M equazioni in N incognite, con i coefficienti A_{ij} interi limitati in modulo da B. Allora esiste una soluzione non banale negli interi con modulo limitato da $(NB)^{\frac{M}{N-M}}$.

Possiamo applicarlo al nostro problema dopo aver trasformato i coefficienti di tutte le equazioni da razionali a interi moltiplicando per i relativi denominatori comuni. Abbiamo dunque $N = (L+1)^2, M = ST$; trovare una buona stima per B è leggermente complicato: l'idea è che possiamo scrivere ogni derivata della $\wp$ come polinomio nella $\wp$ e nella $\wp'$, i cui coefficienti possiamo controllare in svariati modi, ad esempio con l'espansione di Eisenstein. Il modulo delle $\wp(u_s), \wp(Nu_s)$ e delle derivate lo controlliamo con $exp(c_9 w)$ come spiegato prima. Sostituendo in (43) (tralasciamo i conti specifici, abbastanza involuti e non di particolare interesse nel nostro contesto, per i quali rimandiamo al paper originale), si trova che possiamo prendere

$$B = c_{10}^{w(T+L+1)} T! N^T$$

Applicando il Lemma otteniamo la stima voluta.

Stimeremo dunque prima dall'alto e poi dal basso la derivata di un qualche ordine di f in uno di questi punti ottenendo un assurdo.
Notiamo che con questa scelta di coefficienti f è una funzione ellittica relativamente a Ω, e non è identicamente nulla perché per i punti che seguono il

Teorema 2.2.4, $\wp(Nz)$ è una funzione razionale in $\wp(z)$ di grado N^2 avendo un polo di ordine 2 su ogni punto di N-torsione, ed essendo che gli esponenti di $\wp(z), \wp(Nz)$ in f sono al più $L \overset{(42)}{\leq} N^2$, allora f dovrebbe essere identicamente nullo come polinomio in $\wp(z), \wp(Nz)$, che è assurdo. L'ordine di f è facilmente stimabile dall'alto contando i poli come

$$ord(f) \leq 2L + 2LN^2 \leq 2C^7w^2$$

ed essendo che $S^2 \geq \frac{C^8w^2}{2}$ e che gli zeri sono nello stesso numero dei poli, otteniamo che per C e quindi C_0 sufficientemente grande esistono $0 \leq t \leq S, 1 \leq s \leq S$ tali che:

$$f^{(t)}(u_s) \neq 0 \tag{44}$$

Per la stima dall'alto, introduciamo l'ulteriore funzione ausiliaria:

$$g(z) = f(z)(\theta_0(z))^L(\theta_0(Nz))^L \tag{45}$$

Vediamo che attraverso il Lemma di Schwartz è possibile controllare dall'alto il modulo delle prime S derivate di g nei punti di interesse. Unendo ciò alla stima precedente di non nullità otterremo il controllo dall'alto voluto. Da (43), (45) segue che

$$g(z) = \sum_{l_1=0}^{L}\sum_{l_2=0}^{L} a(l_1,l_2)(\theta(z))^{l_1}(\theta_0(z))^{L-l_1}(\theta(Nz))^{l_2}(\theta_0(Nz))^{L-l_2} \tag{46}$$

e che g ha tutti gli zeri di f con molteplicità maggiore o uguale, quindi almeno ST zeri nel disco di centro 0 e raggio $R_0 = C^{-2}\sqrt{(\frac{A}{\pi})}$. Posto $M(F,r) = max\{(F(z) : |z| = r\}$, applicando Schwarz otteniamo:

$$M(g, 2R) \leq \frac{M(g, 22R)}{5^{ST}} \tag{47}$$

Possiamo controllare il modulo di g grazie a (46) e usando le stime per i coefficienti, per γ e il Lemma 5.1.2, unitamente all'ipotesi per assurdo, ottenendo:

$$M(g, 22R) \leq exp(c_8C^3w^2)c_9^{wL}exp\left(\frac{22^2L(N^2+1)}{C^4}\right) \leq exp(c_{10}C^3w^2) \tag{48}$$

e dato che $ST \geq \frac{\tilde{C}^5w^2}{2}$, per $\tilde{C}$ sufficientemente grande da (47) si ha:

$$M(g, 2R) \leq 4^{-ST}$$

che unitamente alla Formula Integrale di Cauchy dà:

$$M(g^{(t)}, R) \leq 3^{-ST} \tag{49}$$

Preso ora u_s come in (44) e t minimale per esso, dalla derivata del prodotto si ha:

$$f^t(u_s) = \frac{g^t(u_s)}{(\theta_0(u_s))^L(\theta_0(Nu_s))^L} \tag{50}$$

e dal Lemma 5.1.2 otteniamo $|\theta_0(nu_s)| \geq c_{12}^{-w}$, essendo che le $\wp(u_s), \wp(Nu_s)$ hanno modulo al più c_7^w come già osservato. Dunque assieme a (49), (50) ciò ci dà finalmente:

$$f^t(u_s) \leq 2^{-ST} \leq exp(-c_{13}C^5w^2) \tag{51}$$

La stima dal basso segue direttamente da quella sui coefficienti $a(l_1, l_2)$ e su quelli che si ottengono derivando f, come fatto nell'applicazione del Lemma di Siegel. Questi stime ci danno un lower bound di

$$f^t(u_s) \geq exp(c_{14}C_0w^2) = exp(c_{14}C^4w^2)$$

che unitamente a (51) dà un assurdo per C e dunque C_0 sufficientemente grande.

Siamo ora pronti a dimostrare il Teorema 5.0.1: sia C_0 come nella Proposizione 5.2.1 e siano $P_0, ..., P_B$ i punti $P \in E(\mathbb{Q})$ con $\hat{h}(P) < \frac{1}{4C_0}$.
Sia $A = \lfloor 2C_0w \rfloor$. Se $B < A$, essendo $A < 4C_0w^{\frac{3}{2}}$, si ha la tesi. Sia dunque $B \geq A$.
Possiamo applicare il Lemma 5.1.2 e trovare $A+1$ punti $P_{i_0}, ..., P_{i_A},\ 0 \leq i_0 < ... < i_A \leq B$ tali che

$$r(P_{i_a} - P_{i_0}) \leq c_{15}max\{\frac{A}{B}, \nu(\frac{A}{B})^2\},\ 0 \leq a \leq A$$

Guardiamo però ora le altezze di queste differenze: dato che l'altezza di Neròn-Tate è una forma quadratica, vale :

$$\hat{h}(P_{i_a} - P_{i_0}) \leq \left(\sqrt{\hat{h}(P_{i_a})} + \sqrt{\hat{h}(P_{i_0})}\right)^2 < \frac{1}{C_0}$$

e visto che $S + 1 > 2C_0w$, per la Proposizione si ha per forza

$$c_{15}max\{\frac{A}{B}, \nu(\frac{A}{B})^2)\} \geq \frac{1}{C_0}$$

da cui vale una delle seguenti:
$B \leq c_{15}C_0A$, oppure $B \leq \sqrt{c_{15}C_0\nu}A$
e avendo già visto che $\nu \leq c_{16}w$, da entrambe segue il Teorema con

$$K = max\{2c_{15}C_0^2, 2\sqrt{c_{15}c_{16}C_0^3}\}$$

6 Lo *Szpiro ratio* e un risultato di Petsche

L'obiettivo di questo capitolo è dimostrare il seguente risultato:

Teorema 6.0.1 *Sia E una curva ellittica definita su $\mathbb{Q}$, con discriminante minimale Δ e Szpiro ratio σ. Allora per ogni punto $P \in E(\mathbb{Q})$ non di torsione vale*

$$\hat{h}(P) \geq \frac{log(|\Delta|)}{c_{17}\sigma^6} \tag{52}$$

con $c_{17} = 53729472000000$.

Remark: Il Teorema è sostanzialmente un risultato dovuto a C. Petsche, che tuttavia lo enuncia e dimostra, in [7], per curve ellittiche definite su un arbitrario campo di numeri K, e conseguentemente la stima dipende anche da $d = [K : \mathbb{Q}]$. Inoltre il suo risultato ha un denominatore più grande di quello dato qui, in particolare moltiplicato per un termine del tipo $log(d\sigma^2)$, che è però eliminabile nel caso $K = \mathbb{Q}$, in quanto emergente dall'analisi locale dell'altezza canonica sull'insieme dei valori assoluti archimedei diversi da quello standard, che è vuoto su $\mathbb{Q}$.
Come sempre, rimandiamo al paper originale per le dimostrazioni omesse dei risultati più tecnici.

6.1 Preliminari: curve ellittiche su campi locali

Prima di procedere con la dimostrazione è necessario definire lo *Szpiro ratio* e delineare un po' di teoria sulle curve ellittiche su campi locali.
Sia $E : y^2 = x^3 + Ax + B$ una curva ellittica nella forma usuale, con discriminante $\Delta = -16(4A^3 + 27B^2) \neq 0$. Notiamo che, fissato un primo p, possiamo considerare l'equazione

$$\tilde{E} : y^2 = x^3 + \tilde{A}x + \tilde{B} \tag{53}$$

di E ridotta *mod* p, che definisce naturalmente una cubica su $\mathbb{F}_p$ e quindi sul suo completamento rispetto al valore assoluto p-adico (si veda l'Introduzione) $\mathbb{Q}_p$. A questa curva possiamo associare un discriminante $\Delta_p \in \mathbb{F}_p$ in maniera analoga al caso di $\mathbb{Q}$.

Definizione 6.1.1 *Diciamo che E ha buona riduzione modulo p se $\Delta_p \neq 0$ (ovvero se $\tilde{E}$ è ancora una curva ellittica), altrimenti ha cattiva riduzione. In quest'ultimo caso, diciamo che la riduzione è:*

- *moltiplicativa se $48\tilde{A} \neq 0$*
- *additiva se $48\tilde{A} = 0$*

dove le uguaglianze sono da intendersi modulo p.

Proposizione 6.1.1 *E' possibile scegliere l'equazione per E in modo tale che i primi di cattiva riduzione siano esattamente quelli che dividono Δ.*

Definizione 6.1.2 *Se prendiamo inoltre l'equazione per E come sopra in modo tale da ottenere Δ con modulo minore possibile, abbiamo un modello minimale per E e Δ sarà il discriminante minimale.*

Da ora supporremo di essere in questo caso. Scriviamo dunque $\Delta = \prod_{p \in M_{\mathbb{Q}}^{Br}} p^{\delta_p}$ con $M_{\mathbb{Q}}^{Br}$ l'insieme dei primi di cattiva riduzione, che identifichiamo coi rispettivi valori assoluti.
La struttura locale di E sui primi di cattiva riduzione è importante per comprendere il gruppo di Mordell-Weil da un punto di vista globale, così come lo è il tipo di riduzione. Le precise motivazioni dietro a queste idee sono troppo profonde per essere qui discusse, come forse emergerà da dei remark su una quantità che andremo adesso a definire, ovvero il **Conduttore**. Tuttavia, l'idea di base, e sicuramente *naive* in questo contesto, è che guardare a un'equazione modulo un primo può dire davvero molto sulle sue soluzioni intere: un'istanza banale di questo è osservare che RHS e LHS hanno parità diversa, come nel caso di

$$x^5 - x = 1 + y^2 + y^4$$

Definiamo dunque la quantità che contiene tutte le informazioni sul comportamento locale di E:

Definizione 6.1.3 *Si dice conduttore di E l'intero $\mathcal{F} = \prod_{p|\Delta} p^{\eta_p}$ dove*

$$\eta_p = \begin{cases} 0, & \text{se } E \text{ ha buona riduzione modulo } p \\ 1, & \text{se } E \text{ ha riduzione moltiplicativa modulo } p \\ 2, & \text{se } p \neq 2,3 \text{ e } E \text{ ha riduzione additiva modulo } p \end{cases} \tag{54}$$

e nel caso $p = 2, 3$ con riduzione additiva, alla formula di sopra va aggiunto un ulteriore termine per tener conto di "quanto" sia cattiva la riduzione.

Remark 1: la definizione data non è quindi completa, tuttavia quando andremo a stimare lo *Szpiro ratio* nel prossimo capitolo, il non conoscere la valutazione 2 e 3-adica non influenzerà il risultato.
Remark 2: La definizione del termine aggiuntivo nei casi $p = 2, 3$ richiede nozioni avanzate di Teoria di Galois delle estensioni su campi locali.
Remark 3: Per risultati moderni, in primis quello celebre di Wiles, è noto che ogni curva ellittica è *modulare* nel senso che è un quoziente della Jacobiana Modulare $J_0(N)$ per qualche N. Il minimo tale N è proprio il conduttore.

Proposizione 6.1.2 $\eta_p \leq \delta_p \ \forall p$ *primo*

Possiamo finalmente definire lo *Szpiro ratio*:

Definizione 6.1.4 *Lo Szpiro ratio σ è dato da*

$$\sigma = \frac{log(|\Delta|)}{log(\mathscr{F})} \tag{55}$$

Osservazione 6.1.4.1 *Per la Proposizione* 6.1.2*, $\sigma \geq 1$*

Passiamo adesso all'ultimo strumento di cui abbiamo bisogno per delineare la dimostrazione del Teorema 6.0.1. Abbiamo visto nell'Introduzione, precisamente in (1), come l'altezza di Weil si decomponga in altezze locali. E' naturale chiedersi se lo stesso valga per l'altezza canonica.
La risposta è sì: esistono funzioni $\{\lambda_v\}_{v \in M_{\mathbb{Q}}} : \mathbb{Q}_p \to \mathbb{R}$ con p il primo relativo a v che sono *quasi* forme quadratiche tali che

$$\sum_{v \in M_{\mathbb{Q}}} \lambda_v(P) = \hat{h}(P) \quad \forall P \in E(\mathbb{Q}) \tag{56}$$

L'essere quasi forme quadratiche va inteso in un senso simile a quello dell'altezza di Weil: c'è un termine correttivo che dipende dal punto e dalla curva, ma è comunque possibile controllare molto il loro comportamento. Ovviamente la definizione data è informale, non è minimamente detto che con questi requisiti le altezze locali siano uniche, infatti esse sono uniche una volta imposto di soddisfare anche altre proprietà di regolarità. Tuttavia non definiamo esplicitamente nè ci addentriamo in una trattazione approfondita delle altezze locali, ma menzioniamo solo che le suddette proprietà di regolarità consentono di dimostrare risultati come il Lemma 6.2.2 che seguirà.

6.2 Dimostrazione del Teorema

Adesso possiamo passare alla dimostrazione del Teorema 6.0.1: la nostra strategia è la seguente: per un generico $\mathscr{Z} = \{P_1, ..., P_N\} \subset E(\mathbb{Q})$ definiamo:

$$\Lambda(\mathscr{Z}) := \frac{1}{N^2} \sum_{1 \leq i,j, \leq N} \hat{h}(P_i - P_j) = \frac{1}{N^2} \sum_{v \in M_{\mathbb{Q}}} \sum_{1 \leq i,j, \leq N} \lambda_v(P_i - P_j) \tag{57}$$

Notiamo che, definendo

$$\Lambda_v(\mathscr{Z}) := \frac{1}{N^2} \sum_{1 \leq i,j, \leq N} \lambda_v(P_i - P_j) \tag{58}$$

si ha

$$\Lambda(\mathscr{Z}) = \sum_{v \in M_{\mathbb{Q}}} \Lambda_v(\mathscr{Z}) \tag{59}$$

Consideriamo ora l'insieme

$$\mathscr{Z}_0 \coloneqq \{P \in E(\mathbb{Q}) : \hat{h}(P) \leq \frac{clog(|\Delta|)}{\sigma^2}\} \tag{60}$$

con c una costante assoluta che fisseremo in seguito in modo da far funzionare il ragionamento.
Otterremo che $\mathcal{Z}_0$ non può essere troppo grande stimando dal basso e dall'alto il valore di Λ di un particolare sottoinsieme di $\mathcal{Z}_0$ e mostrando che queste stime portano a un assurdo se $\mathcal{Z}_0$ ha troppi elementi. Il risultato desiderato seguirà con un ulteriore ragionamento per assurdo, prendendo i multipli di un punto P con altezza troppo piccola e sfruttando la quadraticità di $\hat{h}$.
Osserviamo che lo *Szpiro ratio* è già presente nella definizione di $\mathcal{Z}_0$, per cui è naturale chiedersi se definendo questo insieme in maniera alternativa non si possa eliminare la dipendenza da questo parametro, ma in realtà σ appare naturalmente nella stima dal basso indipendentemente da come sia definito $\mathcal{Z}_0$, come si vedrà, e la sua presenza nella definizione di quest'ultimo è unicamente necessaria a far funzionare il ragionamento per assurdo.
Iniziamo con la stima dal basso, che è sicuramente la più complicata: come con il lavoro di Masser, è utile tenere a mente la corrispondenza tra curve e tori, infatti anche in questo caso utilizziamo dei risultati enunciati nel setting di un dominio fondamentale $\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$ per la nostra curva; in particolare, valgono i seguenti Lemmi, che non dimostriamo per via della loro natura tecnica:

Lemma 6.2.1 (Hindry, Silverman) *Sia E la curva ellittica relativa al reticolo $\mathbb{Z}+\tau\mathbb{Z}, 0<\epsilon\leq 1$ e $z=\alpha+\beta\tau\in\mathbb{C}$ tale che $max\{|\alpha|,|\beta|\}\leq\frac{\epsilon}{22}$. Sia inoltre $P=exp_E(z)$. Allora $\lambda_\infty(P)\geq\frac{1-\epsilon}{4}$*

Lemma 6.2.2 (Petsche) *Sia $E/\mathbb{Q}$ una curva ellittica, p un primo e v il valore assoluto p-adico di $\mathbb{Q}$. Posto Δ_p il discriminante di un modello minimo per $E/\mathbb{Q}_p$ (ovvero quello con $|\cdot|_v$ minimo), allora se $\mathcal{Z}$ è un insieme di N punti di $E(\mathbb{Q}_p)$ si ha:*

$$\Lambda_v(\mathcal{Z})\geq\frac{1}{12}\left(\frac{1}{a_p}-\frac{1}{N}\right)log\left(|\frac{1}{\Delta_p}|_v\right) \tag{61}$$

con $a_p:=max\{16,\delta_p\}$.

Il Lemma 6.2.1 si può trovare in [8]. Il Lemma 6.2.2 è il vero contributo dovuto a Petsche, che consente di ottenere la dipendenza polinomiale del denominatore in σ in (52). La miglior stima precedente per l'altezza minima, dovuta sempre a Hindry e Silverman ([9]) e impiegata in [1], aveva invece una dipendenza da σ del tipo $e^{-c_{18}\sigma}$ e dà una stima leggermente più debole di quella in (4), ovvero del tipo $M^{\frac{1}{\sqrt{loglogM}}}$.
Notiamo che questi lemmi ci forniscono delle stime dal basso rispettivamente per il valore assoluto archimedeo e quelli p-adici, che è ciò che cerchiamo, tuttavia il primo si applica con un'ipotesi e non è già enunciato in termini di Λ come il secondo. Con un semplice ragionamento via *Pigeonhole principle* (come nel caso del risultato di Masser) possiamo però risolvere entrambe queste problematiche. Infatti, se suddividiamo il parallelogramma fondamentale in 23^2 sottoparallelogrammi nella maniera naturale (cioè tracciando rette parallele agli assi per i punti di 23-torsione) otteniamo che, posta N_0 la cardinalità di $\mathcal{Z}_0$, esiste

uno di questi sotto-parallelogrammi che contiene almeno $\frac{N_0}{23^2}$ punti di $\mathcal{Z}_0$; ma soprattutto, otteniamo che tutte le differenze tra coppie di questi punti sono nella forma $\alpha + \beta\tau$ con $max\{|\alpha|, |\beta|\} \leq \frac{1}{23}$, da cui possiamo applicare loro il Lemma 6.2.1 con $\epsilon = \frac{22}{23}$ e ottenere che esse hanno altezza canonica almeno $\frac{1}{92}$. Abbiamo dunque tutto l'occorrente per la stima dal basso. Enunciamo quindi la seguente:

Proposizione 6.2.3 *Nelle notazioni di sopra, esiste c tale che* $N_0 \leq 23^2 100\sigma^2$

Dimostrazione: Sia $N_1 = \frac{N_0}{23^2}$. Per quanto visto, abbiamo un insieme di almeno N_1 punti, sia esso $\mathcal{Z}_1$, per il quale possiamo stimare dal basso il valore $\Lambda(\mathcal{Z}_1)$ grazie ai due Lemmi sopra. Eseguendo questa stima otteniamo infatti, ricordando (59):

$$\Lambda(\mathcal{Z}_1) = \frac{1}{N_1^2}\left(\sum_{v \in M_{\mathbb{Q}}^0} \Lambda_v(\mathcal{Z}_1) + \sum_{P_i, P_j \in \mathcal{Z}_1} \lambda_\infty(P_i - P_j)\right) \tag{62}$$

La parte archimedea si stima dunque facilmente con

$$\frac{1}{N_1^2}(N_1(N_1-1))\frac{1}{92} \geq \frac{N_1 - 1}{92N_1} \tag{63}$$

mentre per quella non archimedea usiamo la Disuguaglianza di Jensen, che ricordiamo brevemente

Proposizione 6.2.4 *Siano* $w_1, ..., w_n$ *pesi positivi con* $\sum_{i=1}^n w_i = 1$ *e* $\phi(x)$ *una funzione convessa per* x *positivo. Allora se* $x_1, ..., x_n$ *sono positivi, vale*

$$\sum_{i=1}^n w_i \phi(x_i) \geq \phi\left(\sum_{i=1}^n w_i x_i\right) \tag{64}$$

Se prendiamo dunque $\phi(x) = \frac{1}{x}$ e $\{w_p\}_{p \in M_{\mathbb{Q}}^{Br}} = \frac{\eta_p log(p)}{log(\mathcal{F})}$ per i primi di cattiva riduzione, si ha $\sum_{p \in M_{\mathbb{Q}}^{Br}} w_p = 1$ per definizione di conduttore e ponendo $x_p = \frac{\eta_p}{\delta_p}$ per Jensen si ottiene

$$\sum_{p \in M_{\mathbb{Q}}^{Br}} \frac{\delta_p log(p)}{log(\mathcal{F})} \geq log(\mathcal{F})\left(\sum_{p \in M_{\mathbb{Q}}^{Br}} \frac{\eta_p^2}{\delta_p} log(p)\right)^{-1} \geq log(\mathcal{F})\left(\sum_{p \in M_{\mathbb{Q}}^{Br}} \delta_p log(p)\right)^{-1} \geq$$

$$\geq \frac{log(\mathcal{F})}{log(p)} \Rightarrow \sum_{p \in M_{\mathbb{Q}}^{Br}} \frac{\delta_p log(p)}{a_p} \geq \frac{(log(\mathcal{F}))^2}{16 log(|\Delta)|} \tag{65}$$

dove la seconda disuguaglianza vale per la Proposizione 6.1.2.
D'altra parte sicuramente $\Lambda(\mathcal{Z}_1) \geq \sum_{v \in M_{\mathbb{Q}}^{Br}} \Lambda_v(\mathcal{Z}_1)$ e per il Lemma 6.2.2 si ha,

notando che $log(|\frac{1}{\Delta_p}|_p) = \delta_p log(p)$,

$$\sum_{v \in M_{\mathbb{Q}}^{Br}} \Lambda_v(\mathcal{Z}_1) \geq \frac{1}{12} \left(\sum_{p \in M_{\mathbb{Q}}^{Br}} \frac{\delta_p}{a_p} log(p) - \frac{\delta_p log(p)}{N_1} \right) \geq \frac{1}{12} \left(\frac{1}{16\sigma^2} - \frac{1}{N_1} \right) log(|\Delta|) \tag{66}$$

Unendo (63) e (66) otteniamo

$$\Lambda(Z_1) \geq \frac{N_1 - 1}{92 N_1} + \frac{1}{12} \left(\frac{1}{16\sigma^2} - \frac{1}{N_1} \right) log(|\Delta|) \tag{67}$$

La maggiorazione non richiede un'analisi delle proprietà locali dell'altezza canonica, ma si basa invece sul fatto che essa è una forma quadratica definita positiva. Infatti per la legge del parallelogramma e la positività sicuramente $\hat{h}(P_i - P_j) \leq 2\hat{h}(P_i) + 2\hat{h}(P_j)$ e quindi

$$\Lambda(\mathcal{Z}_1) \leq 4 \frac{1}{N_1} \sum_{P \in \mathcal{Z}_1} \hat{h}(P) \leq \frac{4clog(|\Delta|)}{\sigma^2} \tag{68}$$

dove la primma disuguaglianza vale perché ogni punto compare in $2(N-1)$ somme e la seconda per definizione di $\mathcal{Z}_1 \subset \mathcal{Z}_0$.
Pertanto otteniamo

$$\frac{4clog(|\Delta|)}{\sigma^2} \geq \frac{N_1 - 1}{92 N_1} + \frac{1}{12} \left(\frac{1}{16\sigma^2} - \frac{1}{N_1} \right) log(|\Delta|) \tag{69}$$

Portando tutto allo stesso membro e guardando il coefficiente $\frac{1}{192} - 4c$ di $\frac{log(|\Delta|)}{\sigma^2}$ troviamo che se esso è positivo, ovvero $c < \frac{1}{768}$, allora N_1 non può essere arbitrariamente grande; infatti con semplici manipolazioni algebriche troviamo

$$N_1 \leq \frac{\sigma^2}{4(\frac{1}{192} - 4c)} \tag{70}$$

Dunque per esempio ponendo $c = \frac{13}{19200}$ otteniamo

$$N_0 \leq 100\sigma^2 \Rightarrow N_0 \leq 23^2 \cdot 100\sigma^2 \ \square \tag{71}$$

Dedurre il Teorema 6.0.1 dalla Proposizione 6.2.3 è nuovamente un semplice utilizzo del fatto che $\hat{h}$ è una forma quadratica. Notiamo infatti che dato $P \in E(\mathbb{Q})$ punto di non-torsione, la sequenza $\{a_m\}_{m \geq 0} := \hat{h}(mP) = m^2 \hat{h}(P)$ è strettamente crescente. Sia dunque M il più piccolo intero non negativo tale che $\hat{h}(MP) \geq \frac{log(\Delta)}{c\sigma^2}$. Allora i punti $O, P, ..., (M-1)P$ stanno in Z_0 e quindi per la Proposizione, $M \leq 23^2 \cdot 100\sigma^2$, dunque

$$\frac{log(|\Delta|)}{c\sigma^2} \leq \hat{h}(MP) = M^2 \hat{h}(P) \leq 23^4 \cdot 10^4 \sigma^4 \hat{h}(P)$$

da cui infine, ricordando il valore di c,

$$\hat{h}(P) \geq \frac{log(|\Delta|)}{2^{12} 3^1 5^6 23^4 \sigma^6} \tag{72}$$

7 Il conteggio

In questo capitolo continuiamo con la stessa notazione del capitolo 5 per le costanti assolute.
Nel capitolo 4 abbiamo riformulato il problema di conteggio in esame in contesto euclideo grazie alle proprietà dell'altezza canonica, e quello che dobbiamo fare è maggiorare la cardinalità dell'insieme

$$\{x \in L \cap \mathcal{B}(0, \sqrt{logB})\} \tag{73}$$

in funzione di B, dove $L \simeq \mathbb{Z}^r$ è l'immagine di $E(\mathbb{Q})/T$ nel prodotto tensore $E(\mathbb{Q}) \otimes \mathbb{R} \simeq \mathbb{R}^r$ imponendo che l'estensione della forma quadratica indotta dall'altezza canonica sia la norma euclidea, ed è dunque un r-reticolo.
L'approccio che seguiamo è di tipo locale-globale, come già anticipato alla fine del quarto capitolo:

- per un certo raggio $\rho > 0$ stimiamo quanti punti del reticolo ci sono al massimo in ogni palla di raggio ρ centrata in un punto del reticolo stesso
- stimiamo quante tali palle servono al massimo per ricoprire $L \cap \mathcal{B}(0, \sqrt{logB})$

Iniziamo con il secondo punto, per il quale utilizziamo un argomento elementare dovuto originariamente a Mumford:

Lemma 7.0.1 *Siano $R, \rho > 0$, n un intero positivo e sia S un sottoinsieme della palla $\mathcal{B}(0, R) \subset \mathbb{R}^n$. Allora è possibile ricoprire S con al più $(1 + \frac{2R}{\rho})^n$ palle di raggio ρ centrate in punti di S.*

Dimostrazione: Consideriamo un insieme di palle **disgiunte** di raggio $\frac{\rho}{2}$ centrate in punti di S che sia massimale nel senso che una palla di raggio $\frac{\rho}{2}$ centrata in un punto di S e non appartenente all'insieme interseca per forza una dell'insieme. Notiamo allora che l'unione di queste palle è contenuta in $\mathcal{B}(0, R + \frac{\rho}{2})$ da cui, per il principio Pigeonhole, $|S| \leq \frac{V_{R+\frac{\rho}{2}}}{V_{\frac{\rho}{2}}}$ con V_a il volume della palla di raggio a. Quindi $|S| \leq (1+\frac{2R}{\rho})^n$. Tuttavia notiamo se applichiamo un'omotetia di fattore 2 a ognuna di queste palle di centro il suo centro, otteniamo un insieme di palle di raggio ρ centrate in S che ricopre S, in quanto se un punto di S non appartenesse alla loro unione allora vi avremmo potuto centrare una palla di raggio $\frac{\rho}{2}$ che non intersecasse nessuna delle palle dell'insieme inizialmente definito, contraddicendone la massimalità. □

Chiaramente, andremo a sfruttare il Lemma con:

$$n = r, R = \sqrt{logB}, S = L \cap \mathcal{B}(0, \sqrt{logB})$$

e ρ che sceglieremo a seconda di in quale di due casi ci troviamo, come descritto in seguito.
Prima di passare al primo punto dell'approccio, notiamo che avendo a che fare

con un reticolo (e quindi originariamente grazie alla struttura di gruppo), il numero di punti di L nella palla di centro $l \in L$ e raggio ρ è lo stesso di quelli nella palla di centro 0 e raggio ρ, da cui la nostra maggiorazione sarà data da

$$N(B) \leq c_{19} \left(1 + \frac{2\sqrt{logB}}{\rho}\right)^r |L \cap \mathcal{B}(0,\rho)| \tag{74}$$

dove ricordiamo che c_{19} viene dalla Torsione.
Notiamo inoltre che da $B \geq H(E)$ segue $B \geq \frac{|\Delta|}{32}$.

Passiamo dunque al primo punto: l'idea adesso è di applicare il risultato di Masser, che ci assicura che esiste una costante assoluta K tale che il numero di punti razionali con altezza $\hat{h}(P) \leq \frac{1}{K}$ è al più $Kh(E)^{\frac{3}{2}} \leq K(logB)^{\frac{3}{2}}$, ovvero che il numero di punti in $L \cap \mathcal{B}(0, K^{-\frac{1}{2}})$ è al più $K(logB)^{\frac{3}{2}}$.
Unitamente a (74), scegliendo $\rho = K^{-\frac{1}{2}}$, otteniamo

$$N(B) \leq (c_{20} logB)^{\frac{r+3}{2}} \tag{75}$$

Osserviamo che per curve con r *piccolo* questa stima è molto buona, e implica ampiamente il Teorema 1.3.2. Tuttavia ricordiamo che dal Teorema 3.3.1, sappiamo che $r \leq 2w(\Delta) + 2$ con Δ il discriminante minimale. Ma grazie al *Teorema dei numeri primi (PNT)* sappiamo che la funnzione $P(n) := \prod_{p \leq n} p$ si comporta come $e^{n(1+o(1))}$, da cui otteniamo che

$$r \leq 2w(\Delta) + 2 \leq 3\frac{log(|\Delta|)}{loglog(|\Delta|)} \leq c_{21}\frac{log(B)}{loglog(B)} \tag{76}$$

Per valori di r grandi in questo range la stima non è più buona, ad esempio per $r = \frac{log(B)}{loglog(B)}$ otterremmo $N(B) \leq \sqrt{B(logB)^3}$.

Qui entra in gioco il risultato di Petsche: infatti, se r è *grande*, vuol dire che lo è anche il numero di fattori primi di Δ. Ricordando da (54) che il conduttore è divisibile da tutti i primi che dividono Δ eccetto al più 2 e 3, questo vuol dire che lo *Szpiro ratio* avrà un numeratore *grande*. Conseguentemente, sarà *grande* anche l'altezza minima $\hat{h}_0$ di un punto di non torsione, e sciegliendo $\rho = \sqrt{\hat{h}_0}$ nel Lemma 7.0.1 otterremo un numero contenuto di palle, con un solo punto di L in ciascuna di esse.
Formalizziamo questa strategia: scegliendo $\rho = \sqrt{\hat{h}_0}$ con $\hat{h}_0 = \frac{log(|\Delta|)}{2c_{17}\sigma^6}$ (si veda (52)) si ottiene, unitamente a (74),

$$N(B) \leq \left(c_{22}\sqrt{\frac{logB}{log|\Delta|}}\sigma^3\right)^r. \tag{77}$$

Poniamo ora

$$r = \alpha\frac{logB}{loglogB} \tag{78}$$

Allora (75) diventa

$$N(B) \leq B^{c_{23}\alpha} \tag{79}$$

(77) invece diventa

$$N(B) \leq \left(c_{24} \frac{\sqrt{logB}\sigma^3}{\sqrt{log(|\Delta|)}} \right)^{\alpha \frac{logB}{loglogB}} \leq \left(c_{25}\sigma^2 \frac{logB}{log\mathcal{F}} \right)^{\alpha \frac{logB}{loglogB}} \tag{80}$$

usando sempre $\Delta << B$.
Per ottenere una forma di (80) che dipenda solo da B e da α, dobbiamo stimare dall'alto $\mathcal{F}$ e σ. Per quanto detto sopra, otteniamo che $6\mathcal{F}$ ha almeno $\alpha \frac{logB}{3loglogB}$ fattori primi distinti da cui sempre per PNT:

$$log\mathcal{F} \geq \alpha \frac{logB}{3loglogB}(log\alpha + loglogB - logloglogB - log3) \tag{81}$$

Se

$$\alpha > (logB)^{-\epsilon} \tag{82}$$

per un qualunque $\epsilon < 1$ fissato allora da (82) si ha

$$log\mathcal{F} \geq c_{26}(\epsilon)\alpha logB \tag{83}$$

Δ lo controlliamo sempre con B da cui segue

$$\sigma \leq c_{27}(\epsilon)\frac{1}{\alpha} \tag{84}$$

e (80) diventa dunque, fissando ad esempio $\epsilon = \frac{1}{2}$ nell'ipotesi (81),

$$N(B) \leq \left(\frac{c_{28}}{\alpha} \right)^{3\alpha \frac{logB}{loglogB}} = B^{\frac{3\alpha log(\frac{c_{28}}{\alpha})}{loglogB}} \tag{85}$$

Notiamo che per $\alpha \in [\frac{1}{\sqrt{logB}}, c_{21}]$ la funzione $\alpha log(\frac{c_{28}}{\alpha})$ è controllata $c_{21}log(c_{28}) + \alpha log\frac{1}{\alpha}$ e il secondo addendo vale al più $\frac{1}{e}$, avendo la funzione $xlog\frac{1}{x}$ derivata positiva in $(0, \frac{1}{e})$, nulla in $x = \frac{1}{e}$ e positiva per $x > \frac{1}{e}$.
Dunque (85) diventa

$$N(B) \leq B^{\frac{c_{29}}{loglogB}} \tag{86}$$

Riassumendo: se $\alpha < \frac{1}{\sqrt{logB}}$ usiamo (79) ottenendo $N(B) \leq B^{\frac{c_{23}}{\sqrt{logB}}}$, mentre altrimenti usiamo (86), che è dunque il *worst case scenario* e ci dà esattamente il Teorema 1.3.2.

8 Approfondimenti

8.1 Lang, Szpiro e *abc*

Abbiamo visto che per una curva ellittica $E/\mathbb{Q}$ l'altezza canonica di ogni punto razionale non di torsione soddisfa

$$\hat{h}(P) > C\frac{log(|\Delta|)}{\sigma^6}$$

con Δ il discriminante di un modello minimale per E, $\sigma = \frac{log(|\Delta|)}{log(\mathcal{F})}$ il relativo *Szpiro ratio* e C una costante assoluta.
Risulta naturale chiedersi se questa stima sia ottimale, o se ad esempio la dipendenza dallo *Szpiro ratio* possa essere eliminata.

Congettura 8.1.1 (Lang) *Nelle ipotesi e notazioni di sopra,*

$$\hat{h}(P) > Clog(|\Delta|) \tag{87}$$

Rimarchiamo che C è assoluta, non dipende dalla curva. Nonostante sia stata dimostrata per alcune particolari famiglie di curve ellittiche, per esempio quelle con invariante j intero, da Silverman, il caso generale è ritenuto vero ma molto profondo.
Una possibile via per dimostrare la congettura di Lang è quella di mostrare che lo *Szpiro ratio* non può essere arbitrariamente grande:

Congettura 8.1.2 (Szpiro) *Per ogni $\epsilon > 0$ esiste una costante $C(\epsilon)$ tale che per ogni curva ellittica $E/\mathbb{Q}$,*

$$|\Delta| < C(\epsilon)\mathcal{F}^{6+\epsilon} \tag{88}$$

Osservazione 8.1.0.1 *La congettura di Szpiro implica che σ sia uniformemente limitato, e quindi implica la congettura di Lang*

Per concludere questa breve sezione, illustriamo quanto sia difficile (o almeno, considerato difficile) arrivare alla congettura di Lang per questa strada: infatti, la celebre *Congettura abc*

Congettura 8.1.3 (Oesterlé-Masser) *Per ogni $\epsilon > 0$ esiste solo un numero finito di triple (a, b, c) di interi positivi coprimi tali che $a + b = c$ e che $c > (rad(abc))^{1+\epsilon}$ con $rad(n)$ il prodotto dei fattori primi distinti di n.*

implica la congettura di Szpiro, ma è anche implicata da una versione leggermente modificata di quest'ultima. Inoltre, la congettura di Szpiro 8.1.2 implica 8.1.3 con un esponente del radicale di $\frac{6}{5}$ ([10]): insomma, la congettura di Szpiro è difficile *quasi* come *abc*.

8.2 Rimuovere l'ipotesi sulla 2-torsione

Senza assumere che E abbia un punto di 2-torsione razionale (diverso da O), la discesa via 2-isogenia non consente di ottenere la stessa stima per il rango, in sostanza perché per il nostro ragionamento abbiamo supposto che la curva avesse coefficienti interi anche portando la radice in 0, ma senza quell'ipotesi avremo coefficienti in un campo di numeri K e quindi l'omomorfismo di (30) avrà come codominio K/K^*; dunque i metodi descritti in questa tesi non sono *a priori* sufficienti per ottenere la congettura 1.3.1 rimuovendo l'ipotesi sulla 2-torsione.
Tuttavia, ricordando che abbiamo usato quest'ipotesi unicamente per maggiorare il rango, è naturale chiedersi se si possano ottenere maggiorazioni simili anche supponendo che la 2-torsione (o un suo punto) sia contenuta in un certo campo di numeri K, in funzione di K. Possiamo osservare ulteriormente che i punti di 2-torsione, se non sono razionali, stanno in un campo cubico, in quanto radici del polinomio di Weierstrass.
La risposta è affermativa: il rango infatti può essere maggiorato da un termine simile a quello che abbiamo nel caso di $\mathbb{Q}$ (al posto del numero di fattori primi del discriminante avremo il numero di valori assoluti su cui la curva ha cattiva riduzione), ma vi si aggiunge un termine che dipende da Cl_K, il Gruppo di Classe di K, in particolare all'incirca il logaritmo della cardinalità della 2-torsione di Cl_K (si rimanda a [1] per la formula esatta).
Le stime migliori attualmente disponibili, dovute a un grosso sforzo collaborativo di svariati autori ([11]), per quanto avanzate sfortunatamente non consentono di trascurare questo termine nemmeno per i campi quadratici e cubici, e quindi non è possibile applicare lo stesso ragionamento del caso di $\mathbb{Q}$.

Bibliografia

[1] E. Bombieri e U. Zannier. *On the number of rational points on certain elliptic curves.* Izvestiya Mathematics 68, 2004.

[2] S. Lang. *Elliptic functions.* Springer, 1987.

[3] J. H. Silverman e J. T. Tate. *Rational Points on Elliptic Curves.* Springer, 2015.

[4] J. H. Silverman. *The Arithmetic of Elliptic Curves.* Springer, 2009.

[5] B. Mazur. *Rational isogenies of prime degree.* Inventiones Mathematicae, 44 (2): 129–162, 1978.

[6] D.W. Masser. *Counting points of small height on elliptic curves.* Bulletin de la S. M. F., tome 117, no 2 (1989), p. 247-265, 1989.

[7] C. Petsche. *Small rational points on elliptic curves over number fields.* The New York Journal of Mathematics [electronic only] Volume: 12, page 257-268, 2006.

[8] M. Hindry e J. H. Silverman. *Sur le nombre de points de torsion rationnels sur une courbe elliptique.* C. R. Acad. Sci. Paris, t. 329, Serie I:97–100, 1999.

[9] M. Hindry e J. H. Silverman. *The canonical height and integral points on elliptic curves.* Invent. Math., 93:419–450, 1988.

[10] W. Stein. Elliptic curves, the abc conjecture, and points of small canonical height (notes from a seminar talk by matt baker), 2001. https://wstein.org/mcs/archive/Fall2001/notes/12-10-01/12-10-01/node2.html.

[11] M. Bhargava e A. Shankar e T. Taniguchi e F. Thorne e J. Tsimerman e Y. Zhao. *Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves.* arXiv:1701.02458, 2017.