Università degli Studi Roma Tre
Facoltà di Scienze M.F.N.
Corso di Laurea in Matematica

Tesi di Laurea Magistrale in Matematica

Elliptic Curves over $\mathbb{Q}$ and the Conjecture of Birch and Swinnerton-Dyer

(una sintesi)

Candidata
Marianna Coletta

Relatore
Prof. Francesco Pappalardi

Anno Accademico 2008-2009
Febbraio 2010

Introduzione

Nella tesi ``*Elliptic Curves over* $\mathbb{Q}$ *and the Conjecture of Birch and Swinnerton-Dyer*´´studieremo, appunto le curve ellittiche sul campo dei razionali. Una curva ellittica è una curva proiettiva data da un'equazione affine della forma $y^2 = P(x)$, dove P è un polinomio monico di grado tre a coefficienti razionali e distinte radici complesse.

I punti su tale curva, uniti a un punto ``all'infinito´´, formano un gruppo abeliano secondo una opportuna definizione geometrica di addizione. Come afferma il Teorema di Mordell-Weil, questo gruppo abeliano è finitamente generato. Cioè, è della forma $\mathbb{Z}^r \oplus T$, dove r è il rango della curva ellittica e T è un gruppo finito, i suoi elementi sono punti della curva ellittica di ordine finito. Un Teorema di Lutz e Nagell descrive T e cioè il sottogruppo di torsione completamente, mentre il rango non è ancora del tutto compreso.

Nelle ultime tre decadi, le curve ellittiche hanno giocato un ruolo sempre più importante sia in teoria dei numeri che in campi affini, come la crittografia. In particolare, nel 1980 e 1990, le curve ellittiche sul campo dei razionali sono state un importante strumento per la dimostrazione dell'Ultimo Teorema di Fermat.

In questa tesi proveremo il Teorema di Mordell-Weil e vedremo che la dimostrazione posa le sue origini nel metodo della discesa infinita di Fermat. Inoltre, mostreremo come i punti di torsione possono essere trovati in maniera davvero semplice.

Gli ultimi capitoli riguardano le connessioni tra le curve ellittiche e alcuni interessanti e profondi problemi presenti in teoria dei numeri come l'Ultimo Teorema di Fermat, il Problema dei Numeri Congruenti, la Congettura di Taniyama-Shimura, dimostrata da Andrew Wiles e Richar Taylor nel 1994 nel caso particolare delle curve ellittiche semi-stabili e completamente dimostrata unitamente da Breuil, Conrad, Diamond e Taylor nel 2001, e la Congettura di Birch e Swinnerton-Dyer. Quest'ultima verrà verificata per una particolare curva di rango tre nel capitolo finale.

1 Il Teorema di Mordell-Weil

Partiamo con una curva ellittica E della forma

$$y^2 = (x - e_1)(x - e_2)(x - e_3) \tag{1}$$

con $e_1, e_2, e_3 \in \mathbb{Z}$ e $e_i \neq e_j$ dove $i \neq j$.

Poiché il prodotto di $(x - e_1)$, $(x - e_2)$ e $(x - e_3)$ è un quadrato, l'intuizione suggerisce che ognuno di questi fattori sia, in qualche senso, vicino ad essere anch'esso un quadrato. Assumendo che $x, y \in \mathbb{Q}$, scriviamo

$$x - e_1 = au^2 \qquad x - e_2 = bv^2 \qquad x - e_3 = cw^2$$

con $a, b, c, u, v, w \in \mathbb{Q}$. Allora $y^2 = abc(uvw)^2$, quindi abc è un quadrato. Per opportuni u, v, w, possiamo assumere che a, b, c siano privi di fattori quadratici. Questa procedura è detta **discesa**, o, più precisamente, **2-discesa**.

Proposizione 1.1. *Sia*

$$S = \{p \mid p \text{ è primo e } p \mid (e_1 - e_2)(e_1 - e_3)(e_2 - e_3)\}.$$

Se p è un primo e $p \mid abc$, allora $p \in S$.

Dal fatto che S è un insieme finito, si deduce che possono esserci solo finite combinazioni (a, b, c) possibili. Il seguente teorema mostra che l'insieme delle combinazioni che di fatto provengono da punti (x, y) ha una struttura di gruppo modulo quadrati.

Teorema 1.2. *Sia E una curva ellittica nella forma* (1)*. La mappa*

$$\phi : E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2} \oplus \mathbb{Q}^*/\mathbb{Q}^{*2} \oplus \mathbb{Q}^*/\mathbb{Q}^{*2}$$

definita da

$$\begin{aligned}
(x, y) &\mapsto (x - e_1, x - e_2, x - e_3) \text{ dove } y \neq 0 \\
\mathcal{O} &\mapsto (1, 1, 1) \\
(e_1, 0) &\mapsto ((e_1 - e_2)(e_1 - e_3), e_1 - e_2, e_1 - e_3) \\
(e_2, 0) &\mapsto (e_2 - e_1, (e_2 - e_1)(e_2 - e_3), e_2 - e_3) \\
(e_3, 0) &\mapsto (e_3 - e_1, e_3 - e_2, (e_3 - e_1)(e_3 - e_2))
\end{aligned}$$

è un omomorfismo. Il nucleo di ϕ è $2E(\mathbb{Q})$.

Questo teorema ha un importante corollario.

Teorema 1.3 (Debole di Mordell-Weil). *Sia E una curva ellittica su $\mathbb{Q}$. Allora $E(\mathbb{Q})/2E(\mathbb{Q})$ è finito.*

Teorema 1.4 (**Mordell-Weil**). *Sia E una curva ellittica su $\mathbb{Q}$. Allora $E(\mathbb{Q})$ è un gruppo abeliano finitamente generato.*

Il teorema afferma che esiste un insieme di punti su E dal quale tutti gli altri punti possono essere ottenuti disegnando più volte rette tangenti o passanti per punti, rispettando la definizione della legge del gruppo.

Dal Teorema debole di Mordell-Weil, sappiamo che $E(\mathbb{Q})/2E(\mathbb{Q})$ è finito. Solo questo non ci è sufficiente, per dedurne il risultato completo. Infatti, ad esempio, $\mathbb{R}/2\mathbb{R} = 0$, quindi finito, ma $\mathbb{R}$ non è finitamente generato. Torniamo al nostro caso, supponiamo di avere $R_1, \ldots, R_n$ punti rappresentanti le finite classi di $E(\mathbb{Q})/2E(\mathbb{Q})$. Sia $P \in E(\mathbb{Q})$. Possiamo scrivere

$$P = R_i + 2P_1$$

per qualche i e qualche P_1. Poi scriviamo

$$P_1 = R_j + 2P_2,$$

ecc. Se dimostriamo che questo processo si ferma, possiamo concludere e ottenere il teorema. La teoria delle altezze mostrerà che i punti $P_1, P_2, \ldots$ tendono a farsi, in qualche senso, più piccoli, quindi il processo porterà alla fine ad un punto P_k che appartiene ad un insieme di punti piccoli. Questi punti, con gli R_j, saranno i generatori di $E(\mathbb{Q})$.

***Definizione* 1.5.** *Sia $a/b \in \mathbb{Q}$, dove a, b sono interi con MCD(a,b)=1. Definiamo*

$$H(a/b) = Max(|a|, |b|)$$

e

$$h(a/b) = \log H(a/b).$$

La funzione h è chiamata ***altezza logaritmica****. Data una curva ellittica E su $\mathbb{Q}$ e un punto $(x, y) \in E(\mathbb{Q})$, definiamo*

$$h(x, y) = h(x), \quad h(\mathcal{O}) = 0, \quad H(x, y) = H(x), \quad H(\mathcal{O}) = 1.$$

*L'**altezza canonica** $\hat{h}$ è definita usando un limite dei valori di $\frac{1}{2}h$.*

Teorema 1.6. *Sia E una curva ellittica su $\mathbb{Q}$. Esiste una funzione*

$$\hat{h} : E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$$

con le seguenti proprietà:

1. *$\hat{h} \geq 0$ per ogni $P \in E(\mathbb{Q})$;*
2. *esiste una costante c_0 tale che $|\frac{1}{2}h(P) - \hat{h}(P)| \leq c_0$ per ogni P;*
3. *data una costante c, esistono solo finiti punti $P \in E(\mathbb{Q})$ con $\hat{h}(P) \leq c$;*

4. $\hat{h}(mp) = m^2\hat{h}(P)$ *per ogni intero* m *e ogni* P*;*
5. $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$ *per ogni* P, Q*;*
6. $\hat{h}(P) = 0$ *se e solo se* P *è un punto di torsione.*

Lemma 1.7. *Sia B>0 un numero reale tale che*

$$S = \left\{P \in E(\mathbb{Q}) : \hat{h}(P) \leq B\right\}$$

contiene un insieme di generatori di $E(\mathbb{Q})/2E(\mathbb{Q})$*. Allora S genera* $E(\mathbb{Q})$*.*

Se abbiamo $P_1, \ldots, P_r$ punti sulla curva ellittica e vogliamo provare che sono indipendenti il seguente teorema ci fornisce un metodo per dimostrarlo.

Teorema 1.8. *Sia E una curva ellittica su* $\mathbb{Q}$ *e sia* $\hat{h}$ *l'altezza canonica. Per* $P, Q \in E(\mathbb{Q})$*, definiamo l'accoppiamento secondo l'altezza (height pairing) come*

$$\langle P, Q\rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q).$$

Allora $\langle\cdot,\cdot\rangle$ *è bilineare in ogni variabile. Se* $P_1, \ldots, P_r$ *sono punti in* $E(\mathbb{Q})$ *e il determinante* $r \times r$

$$\det(\langle P_i, P_j\rangle) \neq 0,$$

allora $P_1, \ldots, P_r$ *sono indipendenti.*

2 Il Sottogruppo di Torsione

Definizione* 2.1.** *Un elemento P di un gruppo si dice avere* ***ordine m *se*

$$mP = \underbrace{P + P + \cdots + P}_{m \text{ volte}} = 0,$$

e $m'P \neq 0$ *per ogni intero* $1 < m' < m$*. Se tale intero m esiste, allora P ha* ***ordine finito****; altrimenti ha* ***ordine infinito****. Definiamo*

$$E(\mathbb{Q})_{tors} = \{P \in E(\mathbb{Q}) \mid P \text{ ha ordine finito}\}.$$

Proposizione 2.2. *Sia E una curva ellittica non singolare.*

1. *Un punto* $P = (x, y) \neq O \in E$ *ha ordine due se e solo se* $y = 0$*.*
2. *E ha esattamente quattro punti il cui ordine divide due su* $\overline{\mathbb{Q}}$*. Questi quattro punti formano un gruppo che è prodotto di due gruppi ciclici di ordine due.*
3. *Un punto* $P = (x, y) \neq O \in E$ *ha ordine tre se e solo se x è una radice del polinomio*

$$\psi_3(x) = 3x^4 + 6Ax^2 + 12Bx - A^2.$$

4. *E ha esattamente nove punti il cui ordine divide tre su* $\overline{\mathbb{Q}}$*. Questi nove punti formano un gruppo che è prodotto di due gruppi ciclici di ordine tre.*

Il seguente teorema è stato provato indipendentemente da Lutz e Nagell nel 1930. Molto spesso consente una veloce determinazione dei punti di torsione di una curva ellittica su $\mathbb{Q}$.

Teorema 2.3 (**Lutz-Nagell**)**.** *Sia E una curva ellittica su* $\mathbb{Q}$ *data da* $y^2 = x^3 + Ax + B$*. Sia* $P = (x, y) \in E(\mathbb{Q})$*. Supponiamo che P abbia ordine finito. Allora* $x, y \in \mathbb{Z}$*. Se* $y \neq 0$ *allora*

$$y^2 \mid 4A^3 + 27B^2.$$

Corollario 2.4. *Sia E una curva ellittica su* $\mathbb{Q}$*. Allora il sottogruppo di torsione è finito.*

Supponiamo di usare il Teorema di Lutz-Nagell e ottenere da questo un possibile punto di torsione P. Un problema è decidere se questo sia o no un vero punto di torsione. E' possibile che moltiplicando P per un intero si ottenga un punto di non torsione, allora si può dedurre che P era a sua volta di non torsione. In generale, il Teorema di Lutz-Nagell produce una lista esplicita di possibili punti di torsione. Se P è un punto di torsione, allora, per ogni n, il punto nP dovrà essere O oppure appartenere a questa lista, quindi avremo $nP = mP$ per qualche $m \neq n$, in tal caso P sarà di torsione e $(n-m)P = O$. In alternativa, possiamo usare il Teorema di Mazur (Teorema 2.7), che afferma che l'ordine di un punto di torsione in $E(\mathbb{Q})$ può essere al più 12. Comunque, in alcuni casi il discriminante risulta difficile da fattorizzare oppure contiene un alto numero di fattori. In questi casi, altri algoritmi possono essere utilizzati.

Un'altra tecnica per la determinazione dei punti di torsione coinvolge la riduzione modulo primi. Il principale risultato è il seguente.

Teorema 2.5. *Sia E una curva ellittica su* $\mathbb{Q}$*. Sia p un primo dispari e assumiamo che* $p \nmid \Delta$*. Sia*

$$\rho_p : E(\mathbb{Q}) \to E(\mathbb{F}_p)$$

la mappa di riduzione modulo p. Se $P \in E(\mathbb{Q})$ *ha ordine finito e* $\rho_p(P) = O$*, allora* $P = O$*.*

Osservazione 2.6. *Il teorema afferma che esiste un isomorfismo tra* $E(\mathbb{Q})_{tors}$ *e un sottogruppo di* $E(\mathbb{F}_p)$*. Possiamo usare questo per dedurne la cardinalità di* $E(\mathbb{Q})_{tors}$*. Infatti, conoscendo la cardinalità di* $E(\mathbb{F}_p)$*, possiamo dedurre che* $|E(\mathbb{Q})_{tors}| \mid |E(\mathbb{F}_P)|$*.*

Teorema 2.7 (**Mazur**)**.** *Sia E una curva ellittica su* $\mathbb{Q}$*. Allora* $E(\mathbb{Q})_{tors}$ *può essere uno dei seguenti:*

$$\mathbb{Z}_n \qquad \text{con } 1 \leq n \leq 10 \text{ oppure } n = 12,$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_{2n} \qquad \text{con } 1 \leq n \leq 4.$$

Osservazione 2.8. *Per ogni gruppo del teorema, ci sono infinite curve ellittiche E aventi quel gruppo come sottogruppo di torsione. Facciamo riferimento alla Tabella 1 qui di seguito per un esempio di ogni possibilità.*

E	$E(\mathbb{Q})_{tors}$	Δ
$y^2 = x^3 + 2$	0	$-2^6 3^3$
$y^2 = x^3 + x$	$\mathbb{Z}_2$	-2^6
$y^2 = x^3 + 4$	$\mathbb{Z}_3$	$-2^8 3^3$
$y^2 = x^3 + 4x$	$\mathbb{Z}_4$	-2^{12}
$y^2 + y = x^3 - x^2$	$\mathbb{Z}_5$	-11
$y^2 = x^3 + 1$	$\mathbb{Z}_6$	$-2^4 3^3$
$y^2 - xy + 2y = x^3 + 2x^2$	$\mathbb{Z}_7$	$-2^7 13$
$y^2 + 7xy - 6y = x^3 - 6x^2$	$\mathbb{Z}_8$	$2^8 3^4 17$
$y^2 + 3xy + 6y = x^3 + 6x^2$	$\mathbb{Z}_9$	$-2^9 3^5$
$y^2 - 7xy - 36y = x^3 - 18x^2$	$\mathbb{Z}_{10}$	$-2^5 3^{10} 11^2$
$y^2 + 43xy - 210y = x^3 - 210x^2$	$\mathbb{Z}_{12}$	$2^{12} 3^6 5^3 7^4 13$
$y^2 = x^3 - x$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	2^6
$y^2 = x^3 + 5x^2 + 4x$	$\mathbb{Z}_2 \oplus \mathbb{Z}_4$	$2^8 3^2$
$y^2 + 5xy - 6y = x^3 - 3x^2$	$\mathbb{Z}_2 \oplus \mathbb{Z}_6$	$2^2 3^6 5^2$
$y^2 = x^3 + 337x^2 + 20736$	$\mathbb{Z}_2 \oplus \mathbb{Z}_8$	$2^{20} 3^8 5^4 7^2$

Tabella 1: Esempi di sottogruppi di torsione di $E(\mathbb{Q})$

3 Il Rango

E' stato provato da Andrew Wiles e altri che tutte le curve ellittiche sono modulari. Questo risultato ha fornito un potente strumento per lo studio delle curve ellittiche su $\mathbb{Q}$. Due importanti conseguenze sono che L'Ultimo Teorema di Fermat è vero e che la Congettura di Birch e Swinnerton-Dyer per il rango di $E(\mathbb{Q})$ coinvolge oggetti che sono definiti.

Definizione* 3.1.** *Sia E una curva ellittica definita da una equazione di Weierstrass. Per ogni primo $p \nmid \Delta$, poniamo $a_p = p+1-|E(\mathbb{F}_p)|$. Sia $N = |\Delta|$, allora E è* ***modulare *se esiste una forma modulare cuspidale*

$$f(z) = \sum_{n=1}^{\infty} b_n q^n \in S_2(\Gamma_0(N))$$

tale che $b_p = a_p$ per ogni $p \nmid \Delta$, dove $q = e^{2\pi i z}$ e $S_2(\Gamma_0(N))$ è il sottospazio delle forme cuspidali nel sottospazio delle forme modulari di peso 2 per $\Gamma_0(N)$, tali che la funzione $(f(z)dz)|_\alpha/dz$ si annulla all'infinito per ogni $\alpha \in SL_2(\mathbb{Z})$.

Yutaka Taniyama e Goro Shimura per primi hanno suggerito, nel 1955, che ogni curva ellittica fosse modulare, ma i matematici erano inizialmente dubbiosi. André Weil diede, poi, un'evidenza teorica alla congettura. Motivato dalla profonda connessione tra questa congettura e l'Ultimo Teorema di Fermat, Andrew Wiles ha dimostrato buona parte della congettura per dedurne l'Ultimo Teorema di Fermat. Una prova completa della congettura è stata finalmente completata nel 1999, ed è una delle conquiste della teoria dei numeri.

Teorema 3.2 (**Breuil, Conrad, Diamond, Taylor, Wiles**). *Ogni curva ellittica su* $\mathbb{Q}$ *è modulare.*

Per definire la funzione L di una curva ellittica E su $\mathbb{Q}$ assumiamo che E sia data da un'equazione di Weierstrass globalmente minimale. Questa condizione non ci fa perdere generalità.

Per ogni primo p, consideriamo la riduzione E_p di E modulo p. Questa è singolare se e solo se $p \mid \Delta$. Sia nel caso singolare che nonsingolare, definiamo

$$a_p = p + 1 - |E_p(\mathbb{F}_p)|.$$

Il *fattore L locale* per il primo p è la serie formale di potenze data da

$$L_p(u) = \begin{cases} \frac{1}{1-a_p u+pu^2} & \text{if } p \nmid \Delta \\ \frac{1}{1-a_p u} & \text{if } p \mid \Delta. \end{cases}$$

La *funzione L* di E è il prodotto dei fattori locali, con u sostituito nel p-esimo fattore da p^{-s}:

$$L(E,s) = \prod_{p|\Delta}\Big[\frac{1}{1-a_p p^{-s}}\Big]\prod_{p\nmid\Delta}\Big[\frac{1}{1-a_p p^{-s}+p^{1-2s}}\Big].$$

Notiamo che

$$\prod_{p|\Delta}\Big[\frac{1}{1-a_p p^{-s}}\Big]$$

è un numero razionale.

Un risultato di convergenza per questo prodotto di Eulero è dato dalla prossima proposizione.

Proposizione 3.3. *(a) Per ogni primo* p, $|a_p| \le p$.

(b) Per $p \nmid \Delta$, *il reciproco delle radici di* $1 - a_p u + pu^2$ *sono in valore assoluto* $\le p$.

(c) Il prodotto di Eulero che definisce $L(E,s)$ *converge per* $Re(s) > 2$ *e in tale regione è data da una serie di Dirichlet assolutamente convergente.*

Teorema 3.4 (**Breuil, Conrad, Diamond, Taylor, Wiles**). $L(E,s)$ *si estende ad una funzione analitica su tutto il piano complesso.*

Definizione* 3.5.** *Il* ***rango algebrico *di E è l'unico intero non negativo tale che $E(\mathbb{Q})/E(\mathbb{Q})_{tors} \approx \mathbb{Z}^r$. La serie di Taylor di $L(E,s)$ in $s = 1$ ha la forma*

$$L(E,s) = c(s-1)^r + \textit{termini di ordine superiore}$$

con $c \neq 0$. Tale numero r è detto ***rango analitico*** *di E.*

Nel 1950 Birch e Swinnerton-Dyer iniziarono una serie di esperimenti tramite i quali si aspettavano di trovare relazioni tra le proprietà globali e locali di una curva ellittica; cioè, essi provarono a collegare il gruppo $E(\mathbb{Q})$ al gruppo $E(\mathbb{F}_p)$, o, al numero N_p. All'inizio, calcolarono $\prod_{p\leq 439} N_p/p$ per varie curve, e verificarono che questo prodotto era piccolo, medio o grande a seconda che il rango della curva fosse $r = 0$, $r = 1$, $r \geq 2$. Formularono, quindi, la congettura che $\pi_E(X) = \prod_{p<X} N_p/p \sim K(\log X)^r$ se $X \to \infty$. Sfortunatamente, nella gamma dei loro calcoli del prodotto $\pi_E(X)$ oscillava violentemente al crescere di X. La Figura 1 mostra il comportamento di $\pi_E(X)$ per $X \geq 1.5 \times 10^7$ per cinque curve differenti $E_d : y^2 = x^3 - d^2x$. L'asse orizzontale rappresenta $\log\log(X)$ e l'asse verticale è $\log(\pi_E(X))$.

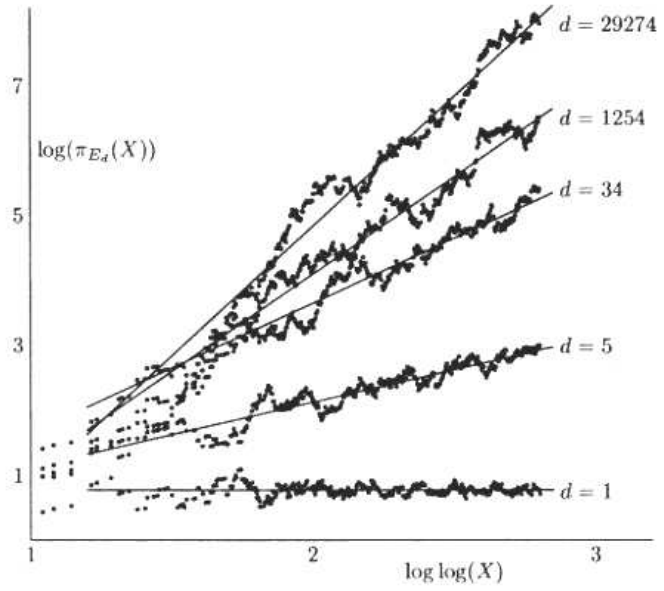

Figura 1: Dati di Birch e Swinnerton-Dyer $y^2 = x^3 - d^2x$

Comunque, esisteva un modo migliore di procedere. Sapendo che

$$L(E,s) = \prod \left|1 + (N_p - p - 1)p^{-s} + p^{1-2s}\right|^{-1},$$

sostituendo $s = 1$ otteniamo

$$L(E,1) = \prod (N_p/p)^{-1};$$

quindi era naturale per loro riformulare la congettura nel seguente modo:

Congettura 3.6 (**Birch e Swinnerton-Dyer**). *Il rango analitico e algebrico di E coincidono. Cioè, l'ordine di annullamento di $L^*(E,s)$ in $s = 1$ è uguale al numero minimo di generatori di $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$.*

Teorema 3.7. *Sia E una curva ellittica definita da $y^2 = x^3 + Ax + B$. Definiamo il* ***periodo reale*** *di E come*

$$\Omega_E = 2^n \int_\gamma^\infty \frac{dx}{\sqrt{x^3 + Ax + B}},$$

dove γ è la più grande radice reale di $x^3 + Ax + B$, e $n = 0$ se $\Delta < 0$, $n = 1$ se $\Delta > 0$. Allora

$$\frac{L(E,1)}{\Omega_E} \in \mathbb{Q},$$

e il denominatore è ≤ 24.

Congettura 3.8 (**Formula di Birch e Swinnerton-Dyer**). *Sia E una curva ellittica su $\mathbb{Q}$ di rango r. Allora*

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\Omega_E \cdot Reg(E) \cdot |Ш_E| \cdot \prod_p c_p}{|E(\mathbb{Q})_{tors}|^2}.$$

Con $L^{(r)}(E,1)$ denotiamo la derivata r-esima della L-serie di E calcolata in 1.

Per una definizione di $Reg(E)$ rimandiamo alla Definizione 4.2.

Qui, $|Ш_E|$ è l'ordine del gruppo di Shafarevich-Tate della curva ellittica E, un gruppo che, in generale, non è noto essere finito ma che si congettura sia tale. Questo gruppo ha la caratteristica di contare il numero di classi di equivalenza di spazi omogenei di E, che hanno punti in tutti i campi locali $\mathbb{Q}_p$ (per ogni $p \leq \infty$). Ci si augura che una dimostrazione della congettura porti anche ad una prova della finitezza di $Ш_E$.

I *numeri di Tamagawa* c_p sono 1 per tutti i primi $p \nmid \Delta$. Quando $p \mid \Delta$, c_p è una misura più raffinata della struttura di E a livello locale p.

Proposizione 3.9. *Sia E una curva ellittica su $\mathbb{Q}$. Se la Congettura 3.6 è vera, allora esiste un algoritmo per calcolare il rango di E.*

Proposizione 3.10. *Sia E una curva ellittica su $\mathbb{Q}$. Se la Congettura 3.6 è vera, allora esiste un algoritmo per calcolare $E(\mathbb{Q})$.*

Teorema 3.11 (**Gross, Kolyvagin, Zagier**). *Sia E una curva ellittica. Se il rango analitico di E è 0 o 1, allora la Congettura 3.6 è vera.*

Una congettura folcloristica asserisce che la "maggior parte"delle curve ellittiche soddisfino le ipotesi di questo teorema, cioè, che esse abbiano rango 0 o 1. Ad esempio, poco più del 95 % delle "prime 78.198"curve ellittiche hanno rango analitico al più 1. Molti matematici sospettano che le

curve con rango maggiore di 1 hanno densità 0. Comunque, nella pratica sono molto spesso le curve con rango più grande di 1 a destare maggiore interesse.

Congettura 3.12 (La Congettura sulla Parità). *Sia E una curva ellittica su $\mathbb{Q}$, siano rispettivamente $r_{E,an}$ e $r_{E,alg}$ il rango analitico e algebrico della curva. Allora*

$$r_{E,alg} \equiv r_{E,an} \pmod 2.$$

Congettura 3.13. *Esistono curve ellittiche definite su $\mathbb{Q}$ di rango arbitrariamente grande.*

4 La Congettura di Birch e Swinnerton-Dyer per una Curva Ellittica di Rango 3

Nel presente capitolo verificheremo numericamente la Congettura di Birch e Swinnerton-Dyer per la curva ellittica:

$$E : y^2 = 4x^3 - 28x + 25. \tag{2}$$

***Definizione* 4.1.** *Il **conduttore** di una curva ellittica è un numero molto simile al discriminante di E cioè è divisibile solo per i primi che dividono il discriminante di E. Più precisamente se E è curva ellittica su $\mathbb{Q}$, per ogni primo $p \in \mathbb{Z}$ definiamo la quantità f_p come segue:*

$$\begin{cases} 0 & \text{se } p \text{ è un primo di buona riduzione per } E \\ 1 & \text{se } p \text{ è un primo di riduzione moltiplicativa per } E \\ 2 & \text{se } p \text{ è un primo di riduzione additiva per } E, \text{ e } p \neq 2,3 \\ 2+\delta_p & \text{se } p \text{ è un primo di riduzione additiva per } E, \text{ e } p = 2,3 \end{cases} \tag{3}$$

dove la definizione di δ_p coinvolge oggetti che non sono inerenti all'argomento trattato nella tesi.

Il conduttore di E è 5077, che sembra essere il più piccolo conduttore per una curva ellittica di rango 3 su $\mathbb{Q}$.

L'altezza Canonica

***Definizione* 4.2.** *Il **regolatore** di una curva ellittica E è il determinante della matrice che esprime l'accoppiamento rispetto all'altezza canonica per $E(\mathbb{Q}) \otimes \mathbb{R}$ rispetto alla $\mathbb{Z}$-base di $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$.*

Cercheremo, ora, di descrivere come calcolare l'altezza canonica di un punto $P \in E(\mathbb{Q})$. Il modello minimale globale per la curva E ha la forma

$$y^2 + y = x^3 - 7x + 6, \tag{4}$$

ottenuta sostituendo y con $2y+1$ nella (2) e dividendo per 4; quest'equazione ha discriminante $\Delta = 5077$. La definizione di $\hat{h}$ implica la formula $\hat{h} = \lim_{n\to\infty} n^{-2}h(nP)$, ma non è comoda ai fini della computazione. Una formula più pratica risulta

$$\hat{h}(P) = \log b + F(x(P)), \tag{5}$$

dove $P \in E(\mathbb{Q})$, $P = (x, y)$ e $x(P) = a/b$, $b > 0$, $\mathrm{MCD}(a, b) = 1$ e $F(x)$ è una funzione a valori reali definita da

$$\begin{gathered} F(x) = \log|x| + \sum_{n=0}^{\infty} 4^{-n-1} \log z_n, \\ z_n = 1 + \frac{14}{x_n^2} - \frac{50}{x_n^3} + \frac{49}{x_n^4}, \qquad x_0 = x,\ x_{n+1} = \frac{x_n^4 + 14x_n^2 - 50x_n + 49}{4x_n^3 - 28x_n + 25}. \end{gathered} \tag{6}$$

In un intorno di $x = 0$ i primi due termini della (6) diventano infiniti, ma possiamo combinarli insieme per ottenere

$$F(x) = \frac{1}{4}\log(x^4 + 14x^2 - 50x + 49) + \sum_{n=1}^{\infty} 4^{-n-1} \log z_n, \tag{7}$$

una formula che ora ha senso per ogni x. Notiamo che tale formula ricorsiva relaziona $x(2P)$ a $x(P)$ per ogni $P \in E(\mathbb{Q})$, quindi $x_n = x(2^nP)$. In particolare, $x_n \geq e_3 = 1.946\ldots$ per $n \geq 1$, dove $e_1 < e_2 < e_3$ denotano le radici del polinomio $4x^3 - 28x + 25$, quindi z_n sta tra 1 e $1.328\ldots$ e $\log z_n$ tra 0 e $0.284\ldots$. Quindi le serie in (6) e (7) convergono molto rapidamente e possiamo calcolare $\hat{h}(P)$ con la precisione che desideriamo.

Diamo, ora, una dimostrazione diretta della (5). Dalla definizione, è sufficiente mostrare che l'espressione sulla destra nella (5) differisca di qualcosa di limitato da $h(P)$ e che sia moltiplicata per 4 se P è sostituito da $2P$. La formula appena citata, sostituendo P con $2P$ sostituisce $x(P) = a/b$ con $x(2P) = a^*/b^*$, dove

$$a^* = a^4 + 14a^2b^2 - 50ab^3 + 49b^4, \qquad b^* = 4a^3b - 28ab^3 + 25b^4.$$

Asseriamo che b^* sia l'esatto denominatore di $x(2P)$. Infatti, $\mathrm{MCD}(a^*, b^*) = 1$ per qualsiasi interi a, b con $\mathrm{MCD}(a, b) = 1$, a meno che $a \equiv 92b \pmod{5077}$, in tal caso $5077 \mid \mathrm{MCD}(a^*, b^*)$. Questo, però, non può accadere nel nostro caso, perché $4x^3 - 28x + 25 = 4(x - 92)^2(x + 184) + 5077(20x - 1227)$ sarebbe divisibile per 5077 ma non per 5077^2 se x fosse $\equiv 92 \pmod{5077}$ e quindi, non potrebbe essere un quadrato. Ciò è vero perché

$$5077b^5a = a^*(300b^2 + 112ab) - b^*(75ab + 28a^2 + 588b^2),$$

quindi $\mathrm{MCD}(a^*, b^*) \mid 5077b^5a$ ma nessuno dei divisori di a o b può dividere sia a^*, b^*. Dall'altra parte, sostituendo P con $2P$ si sostituiscono x_n, z_n con

x_{n+1}, z_{n+1} nella (6), quindi

$$\begin{aligned} F(x(2P)) &= \log|x(2P)| + \sum_{n=0}^{\infty} 4^{-n-1}\log z_{n+1} \\ &= \log|x(2P)| + 4(F(x) - \log|x| - 4^{-1}\log z_0) \quad (x = x(P)) \\ &= 4F(x) - \log(4x^3 - 28x + 25) \\ &= 4(F(x(P)) + \log b) - \log b^*, \end{aligned}$$

prova la seconda affermazione. Per quanto riguarda la differenza tra h e $\hat{h}$, possiamo scrivere $h(P) = \log\max(|a|, b)$ come $h(P) = \log b + \log\max(|a|/b, 1)$, quindi

$$\hat{h}(P) - h(P) = F(x) - \log\max(|x|, 1) \quad (x = x(P)).$$

Se $x \geq e_3 = 1.94\ldots$ è nella componente destra di $E(\mathbb{R})$, allora lo stesso è vero per x_n $(n \geq 0)$, quindi $1 \leq z_n \leq 1.328\ldots$ per ogni n nella (6) e inoltre

$$0 \leq F(x) - \log x \leq \sum_{n=0}^{\infty} 4^{-n-1}\log(1.328\ldots) = 0.0947\ldots.$$

L'altra componente $e_1 \leq x \leq e_2$ di $E(\mathbb{R})$ è compatta e possiamo trovare il minimo e il massimo della funzione $F(x) - \log\max(|x|, 1)$, che sono rispettivamente

$$0.400693021249103961960555191 66\ldots$$

e

$$1.205081104185852151555511 3094\ldots$$

(ottenuti per $x = e_1$ e $x = -1$, vedere la Figura 2). Questi valori sono stati ottenuti notando che la funzione è monotona nei sottointervalli $[e_1, -1]$, $[-1, 1]$, $[1, e_2]$, abbiamo quindi confrontato i valori della funzione negli estremi dei suddetti intervalli usando un algoritmo implementato in PARI.

Pertanto, in tutti i casi abbiamo

$$h(P) \leq \hat{h}(P) \leq h(P) + 1.205\ldots. \tag{8}$$

Questo completa la dimostrazione della (5)

Il Gruppo di Mordell-Weil e il Regolatore

Sia N_p $(p \neq 5077)$ la cardinalità di $E(\mathbb{F}_p)$. Allora, per il Teorema 2.5, $|E(\mathbb{Q})_{tors}|$ deve dividere N_p per ogni $p > 2$; da $N_3 = 7$ e $N_5 = 10$ possiamo dedurre che $E(\mathbb{Q})$ sia un gruppo abeliano libero. Affermiamo che il rango è 3 e che $E(\mathbb{Q})$ sia generato dai seguenti 3 punti:

$$P_0 = (0, 2), \quad P_1 = (1, 0), \quad P_2 = (2, 0).$$

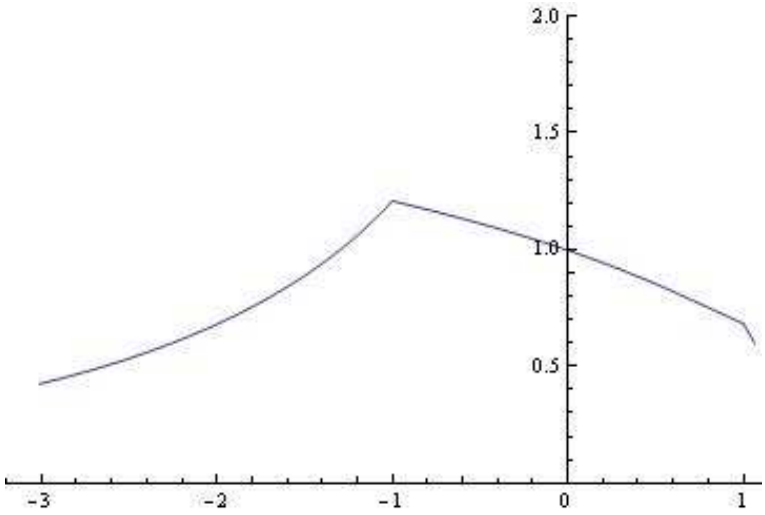

Figura 2: La funzione $F(x) - \log \max(|x|, 1)$

Segue dall'equazione (8) che questi sono i soli punti (a meno del segno) con altezza canonica minore di 1, questo perché $h(P) \leq \hat{h}(P) \leq 1$ implica che $\max(|a|, b) \leq e$ e quindi (dato che b è sempre un quadrato) $b = 1$, $a \in \{-2, -1, 0, 1, 2\}$; di questi cinque candidati, solo $a = 0, 1, 2$ conducono a punti con $\hat{h}(P) < 1$. D'altronde, tramite una 2-discesa si vede che P_0, P_1, P_2 generano $E(\mathbb{Q})/2E(\mathbb{Q})$, che ha rango 3 su $\mathbb{Z}/2\mathbb{Z}$. Questi due dati e il fatto che il gruppo $E(\mathbb{Q})_{tors}$ è banale implicano, tramite la usuale dimostrazione del Teorema di Mordell-Weil, che $E(\mathbb{Q}) = \mathbb{Z}P_0 + \mathbb{Z}P_1 + \mathbb{Z}P_2$, come affermato. Usando l'algoritmo della precedente discussione possiamo calcolare le componenti della matrice

$$A = \left(\left\langle P_i, P_j \right\rangle\right)_{0 \leq i,j \leq 2} = \begin{pmatrix} 0.9909\ldots & -0.2365\ldots & -0.2764\ldots \\ -0.2365\ldots & 0.6682\ldots & 0.0333\ldots \\ -0.2764\ldots & 0.0333\ldots & 0.7670\ldots \end{pmatrix}.$$

Il regolatore è il determinante di questa matrice:

$$R = \det A = 0.417143558758383969817119544618093\ldots. \tag{9}$$

Il Periodo Reale

Il gruppo $E(\mathbb{R})$ ha due componenti connesse. Sia $\omega = dx/(2y + 1)$ il differenziale di Néron di E su $\mathbb{Z}$, e $|\omega|$ la misura associata su $E(\mathbb{R})$. Il *periodo reale* Ω è definito come

$$\Omega = \int_{E(\mathbb{R})} |\omega| = 2 \int_{E(\mathbb{R})^0} |\omega|.$$

Se scriviamo (2) nella forma $y^2 = 4(x - e_1)(x - e_2)(x - e_3)$ con $e_1 < e_2 < e_3$, possiamo calcolare il periodo reale usando la sua media aritmetica-geometrica.

Questa è definita in due argomenti reali positivi x e y tramite la funzione $M(x,y) = \lim_{n\to\infty} x_n = \lim_{n\to\infty} y_n$, dove $x_0 = x$, $y_0 = y$, $x_{n+1} = (x_n + y_n)/2$, $y_{n+1} = \sqrt{x_n y_n}$. Troviamo che

$$\begin{aligned}\Omega = 4\int_{e_3}^{\infty} \frac{dx}{y} &= \frac{2\pi}{M\left(\sqrt{e_3-e_1},\, \sqrt{e_3-e_2}\right)} = \frac{2\pi}{M(2.22689\ldots, 0.938503\ldots)} \\ &= 4.151687983086933049884175683507286\ldots.\end{aligned} \tag{10}$$

La L-serie

La L-serie di E su $\mathbb{Q}$ è data da un prodotto di Eulero che converge nel semipiano destro $Re(s) > 3/2$:

$$L(E,s) = (1+5077^{-s})^{-1} \prod_{p\neq 5077} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1} = \sum_{n=1}^{\infty} a_n n^{-s},$$

($p \neq 5077$). Abbiamo

$$\Lambda(s) := N^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s) = \int_0^{\infty} f\left(\frac{iy}{\sqrt{N}}\right) y^{s-1} dy,$$

dove $N = 5077$ e $f(\tau) = \sum_{n=1}^{\infty} a_n e^{2\pi i n\tau} (\tau \in \mathbb{C},\ Im(\tau) > 0)$. Sappiamo che $f(\tau)$ è una forma cuspidale di peso 2 su $\Gamma_0(N)$. Quindi $f(\tau)$ soddisfa l'equazione funzionale $f(-1/N_\tau) = N_\tau^2 f(\tau)$ e il prolungamento analitico e l'equazione funzionale di $L(E,s)$ seguono:

$$\Lambda(s) = \int_1^{\infty} f\left(\frac{iy}{\sqrt{N}}\right)\left(y^{s-1} - y^{1-s}\right) dy = -\Lambda(2-s). \tag{11}$$

In particolare, l'ordine di $L(E,s)$ in $s = 1$ è dispari e la derivata r-esima ($r \geq 1$ dispari) è data da

$$\begin{aligned}\Lambda^{(r)}(1) &= 2\int_1^{\infty} f\left(\frac{iy}{\sqrt{N}}\right)(\log y)^r dy \\ &= 2\sum_{n=1}^{\infty} a_n \int_1^{\infty} e^{-2\pi n y/\sqrt{N}} (\log y)^r dy.\end{aligned} \tag{12}$$

Se $\Lambda(s)$ si annulla con un ordine $\geq r$ in $s = 1$, allora integrando una volta la (12) si ottiene

$$L^{(r)}(1) = \frac{2\pi}{\sqrt{N}}\Lambda^{(r)}(1) = 2r! \sum_{n=1}^{\infty} \frac{a_n}{n} G_r\left(\frac{2\pi n}{\sqrt{N}}\right), \tag{13}$$

dove

$$G_r(x) = \frac{1}{(r-1)!}\int_1^{\infty} e^{-xy}(\log y)^{r-1}\frac{dy}{y} \qquad (r \geq 1).$$

La serie (13) converge rapidamente, perché $G_r(x) \sim x^{-r}e^{-x}$ quando $x \to \infty$, quindi può essere usata per calcolare $L^{(r)}(1)$ se abbiamo un buon algoritmo per calcolare $G_r(x)$.

La funzione $G_1(x)$ è l'integrale esponenziale $\int_1^\infty e^{-xy}dy/y$, che può essere calcolato per x piccole ($x < 3$) tramite la serie di potenze

$$G_1(x) = \log\frac{1}{x} - \gamma + \sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n\cdot n!}x^n \qquad (\gamma \text{ è la costante di Eulero})$$

e per x grandi ($x > 2$) tramite l'espansione della frazione continua

$$G_1(x) = \cfrac{e^{-x}}{x + \cfrac{1}{1 + \cfrac{1}{x + \cfrac{2}{1 + \cfrac{2}{x + \cfrac{3}{1 + \ldots}}}}}}$$

Prendendo 250 termini della serie in (13) abbiamo che $L'(1) \approx 0$ per le prime 13 cifre decimali. Ciò implica che $L'(1) = 0$ esattamente, dal fatto che un importante risultato di Gross e Zagier [9] asserisce che $L'(1)$ è un semplice multiplo dell'altezza di qualche punto razionale su E e, come abbiamo visto, E non contiene punti razionali di altezza piccola non zero. Dato che $L(s)$ ha ordine dispari, abbiamo $ord_{s=1}L(s) \geq 3$.

In generale, la funzione $G_r(x)$ soddisfa $G_0(x) = e^{-x}$, $G_r'(x) = -(1/x)G_{r-1}(x)$, così

$$G_r(x) = P_r\left(\log\frac{1}{x}\right) + \sum_{n=1}^{\infty}\frac{(-1)^{n-r}}{n^r n!}x^n$$

per qualche polinomio P_r di grado r. Per determinare P_r, usiamo la rappresentazione integrale:

$$G_r(x) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{\Gamma(s)}{s^r}x^{-s}ds \qquad \text{per qualche } c > 0. \tag{14}$$

Traslando il cammino d'integrazione nella (14) verso sinistra, il residuo in $s = -n$ dà il termine $(-1)^{n-r}x^n/n^r n!$ e il residuo in $s = 0$ dà $P_r(\log 1/x)$. Per cui

$$P_r(t) = \sum m = 0^r\gamma_{r-m}\frac{t^m}{m!} \quad \text{dove} \quad \Gamma(1+s) = \sum_{n=0}^{\infty}\gamma_n s^n.$$

Quindi dalla Formula di Eulero-Mclaurin

$$\log\Gamma(1+s) = -\gamma s + \sum_{n=2}^{\infty}\frac{(-1)^n}{n}\zeta(n)s^n,$$

troviamo, per $r = 3$, l'espressione

$$G_3(x) = \frac{1}{6}\left(\log\frac{1}{x} - \gamma\right)^3 + \frac{\pi^2}{12}\left(\log\frac{1}{x} - \gamma\right) - \frac{\zeta(3)}{3} + \sum_{n=1}^{\infty}\frac{(-1)^{n-1}x^n}{n^3 n!}$$

che converge per ogni x. Usandola troviamo il valore

$$\begin{aligned}\lim_{s\to 1}\frac{L(E,s)}{(s-1)^3} &= 2\sum_{n=1}^{\infty}\frac{a_n}{n}G_3\left(\frac{2\pi n}{\sqrt{5077}}\right) \\ &\approx 1.731849900119300689791975085 1\end{aligned} \tag{15}$$

usando i termini per $n \leq 600$.

La Congettura

La Congettura di Birch e Swinnerton-Dyer predice che $ord_{s=1}L(E,s) = r_E = 3$ e che

$$\lim_{s\to 1}\frac{L(E,s)}{(s-1)^3} = \Omega \cdot R \cdot |Ш|$$

dove Ш è il gruppo di Shafarevich-Tate di E su $\mathbb{Q}$. Le equazioni (9) e (10) forniscono

$$\Omega \cdot R = 1.731849900119300689791975085060154\ldots$$

il che concorda con la parte destra dell'equazione (15). Questo suggerisce solidamente che la congettura è vera e che Ш = (1).

Riferimenti bibliografici

[1] B. J. Birch. *Conjectures Concerning Elliptic Curves*. Proc. Symp. Pure Math, Volume 8, Pages 106-112. 1965.

[2] C. Breuil, B. Conrad, F. Diamond and R. Taylor. *On the Modularity of Elliptic Curves over* $\mathbb{Q}$*: wild 3-adic exercises*. 2001.

[3] J. P. Buhler, B. H. Gross and D. B. Zagier. *On the Conjecture of Birch and Swinnerton-Dyer for an Elliptic Curve of Rank 3*. Mathematics of Computation volume 44, number 170, 1985.

[4] J. W. S. Cassels. *Lectures on Elliptic Curves*. Cambridge University Press, 1991.

[5] J. Cotes and A. Wiles. *On the Conjecture of Birch and Swinnerton-Dyer*. Inventiones mathematicae by Springer-Verlag, 1977.

[6] J. E. Cremona *Elliptic Curves Data*. University of Nottingham, U.K. http://modular.fas.harvard.edu/cremona/INDEX.html

[7] A. Dujella. *History of Elliptic Curves Rank Records*. http://web.math.hr/˜duje/tors/rankhist.html/

[8] P-Y. Gaillard. Institut Èlie Cartan Université Enri Poincaré, Vandoeuvre, France. http://www.iecn.u-nancy.fr/˜gaillard/DIVERS/Euler-Maclaurin/euler-mclaurin.060420.pdf

[9] B. Gross and D. Zagier. *Points de Heegner et dérivées de fonctions L* C. R. Acad. Sci. Paris, v. 297, 1983, pp 85-87.

[10] A. W. Knapp. *Elliptic Curves*. Princeton University Press, 1992.

[11] A. P. Ogg. *Rational Points Finite Order on Elliptic Curves*. Berkeley, California. Inventiones mathematicae by Springer-Verlag, 1971.

[12] R. C. Rhoades. *2-Selmer Groups and the Birch and Swinnerton-Dyer Conjecture for the Congruent Number Curve* arXive: 0706.4344v1. 2007.

[13] K. A. Ribet. *On modular representation of Gal*$(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*. 1990.

[14] K. Rubin and A. Silverberg. *Rank of Elliptic Curves*. Bulletin of the American Mathematical Society, Volume 39, Number 4, Pages 455-474.

[15] J. P. Serre. *A Course in Arithmetic*. Springer, 1973.

[16] J. H. Silverman, J. Tate. *Rational Points on Elliptic Curves*. Springer-Verlang, 1992.

[17] W. Stein. *Elementary Number Theory & Elliptic Curves*. 2002.

[18] W. Stein. *The Birch and Swinnerton-Dyer Conjecture, a Computational Approach*. Department of Mathematics, University of Washington. 1991 Mathematics Subject Classification.

[19] L. C. Washington. *Elliptic Curves Number Theory and Cryptography Second Edition*. Taylor & Francis Group, 2008.

[20] A. Wiles. *The Birch and Swinnerton-Dyer Conjecture*.