# SOME COMPUTATIONAL PROBLEMS MOTIVATED BY THE BIRCH AND SWINNERTON-DYER CONJECTURE

by

Iftikhar A. Burhanuddin

A Dissertation Presented to the
FACULTY OF THE GRADUATE SCHOOL
UNIVERSITY OF SOUTHERN CALIFORNIA
In Partial Fulfillment of the
Requirements for the Degree
DOCTOR OF PHILOSOPHY
(COMPUTER SCIENCE)

August 2007

# Dedication

To Mom, Dad, Beauty and Dreams.

I need to live life

Like some people never will

So find me kindness

Find me beauty

Find me truth

When temptation brings me to my knees

And I lay here drained of strength

Show me kindness

Show me beauty

Show me truth

— 'Learning to Live' by Dream Theater

## Acknowledgements

*At times our own light goes out and is rekindled by a spark from another person. Each of us has cause to think with deep gratitude of those who have lighted the flame within us.* A. Schweitzer

I would like to thank Ming-Deh Huang for guiding my doctoral research, teaching me about algorithms, cryptography and elliptic curves, listening patiently to my naïve ideas and helping shape them into theorems, and most importantly giving me the freedom to pursue the questions which captured my imagination.

It is a pleasure to thank William Stein for sharing his ideas and enthusiasm with me, providing me opportunities and encouragement, treating me as a peer and being an immense source of inspiration.

Special thanks to Sheldon Kamienny for always being enthusiastic about discussing number theory and for his support, and to Thomas Geisser, Solomon Golomb, David Kempe and Wayne Raskind for providing me with excellent career advice. Leonard Adleman is an exemplar of how to be courageous in the pursuit of research, be it on codewords of RSA or strands of DNA. I am grateful for his time and encouragement.

Ashish Goel's contagious fondness for theory left an impression on at least one budding theoretician at USC and I appreciate his guidance. I would like to thank Charles Denis Xavier for "remotely" sparking my interest in the theory of computation and enabling me to posit "inspiration is an equivalence relation."

Stimulating discussions with R. Balasubramanian, Henri Cohen, Brain Conrad, Luis Dieulefait, Noam Elkies, Gerhard Frey, Marc Hindry, Kiran Kedlaya, David Joyner, David Kohel, Kristin Lauter, Kapil Paranjape, Dinakar Ramakrishnan, Karl Rubin, Samir Siksek, Joseph Silverman, Alice Silverberg, Kannan Soundararajan, Jon Voight, Felipe Voloch, Mark Watkins, and Benjamin de Weger sparked new questions and directions of research, and I express my gratitude to them.

I am especially thankful to S.S. Ranganathan, M.V. Tamhankar, and H. Subramanian at BITS, Pilani and the teachers at Don Bosco, Madras for piquing my interest, as an undergraduate student and a high-schooler, in mathematical structures of the discrete kind.

I am extremely grateful to the organizers of workshops and conferences, who made my travel to their events financially possible: Yves Aubry, Nils Bruin, Tanush Shaska and the organizers of the Arizona Winter Schools and the SAGE workshops among others. Each such trip introduced me to people who often sparked new questions to ponder, and less often but no less importantly, provided the answers I was seeking.

I would like to thank Ming-Deh Huang, Gary Rosen and the Departments of Computer Science and Mathematics for providing me with financial support during my years at USC via NSF grants CCR-0306393 and CNS-0627458, and departmental graduate assistantships. I would like to thank William Stein for creating SAGE and for providing me with access to the software systems PARI/GP, MAGMA, mwrank and SAGE via the computers `meccah.math.harvard.edu` (funded in large part by William R. Hearst III) and `sage.math.washington.edu` (funded by NSF Grant No. 0555776), without which the computational aspects of this dissertation would not have seen the light of day. I am lucky to have undertaken my doctoral studies in the City of Angels, where I had easy access to the resources and faculties of Caltech, UCI, UCLA and UCSD, and I appreciate their hospitality.

I am fortunate to have crossed paths the following wonderful people in Madras, Pilani, Bangalore and Los Angeles: B.N. Anand, Arun Bruce, Amyn Dhala and Mario Sundar; K.L.Arvind, Mitesh Agarwal, V.T. Bharadwaj, Sutanu Bhowmick, Naresh Chandran, Saugata Chatterjee, Sandeep Dath, Prashant Gupta, Srivatsa Kedlaya, Ganesh Kumar, Deepak Limaye, V.T. Mani, Prakash Math, Gaurav Mittal, Shailesh Murali, Prashant Pandey, Kishore Patil, Shilpa Ranganathan, Rishi Sinha, Arvind Srinivasan and Srividya Subramanian; Pradeep Abraham, Raju V. Kamal, T.S.R. Prasad and Raj Vallabhaneni; Vanessa Carson, Frédéric Chast, Karthik Dantu, Siva Jayaraman, Péter Molnár, Seema Pai, Diana Popa, Deepak Ravichandran, Narayanan Sadagopan, Srikanth Saripalli and Bilal Shaw; and certain pursuers of trivia around the world. Many thanks for the wonderful memories.

Particular gratitude to my relatives for their love and encourgement. My parents provided me with the best education that the circumstances afforded. I am indebted to my dad, Dr. Kaleel Ahamath, for teaching me to dream, my mom, Parveen Kaleel, for driving me to chase those dreams and my sister, Ambereen Burhanuddin, for the support in realizing them. Thanks for believing in me.

I look forward to the exciting times ahead.

# Table of Contents

**Appendix C**

# List Of Tables

# List Of Figures

# Abstract

This dissertation revolves around the BSD (Birch and Swinnerton-Dyer) conjecture for elliptic curves defined over the rational numbers, a famous problem that has been open for over forty years and one of the seven Millennium Prize problems. The BSD conjecture is considered to be the first nontrivial number theoretic problem put forth as a result of explicit machine computation — in the late '50s at Cambridge University. The BSD conjecture relates the rank of the Mordell-Weil group, the group of rational points of an elliptic curve, a quantity which seems to be difficult to pin down, to the order of vanishing of the L-function of the elliptic curve at its central point.

We make algorithmic and theoretical advances with regards to some of the terms appearing in the BSD formula, namely the sizes of the torsion subgroup and the Shafarevich-Tate group.

Firstly, we introduce an algorithm to compute elliptic curve torsion subgroup. The randomized version of this procedure runs in expected time which is essentially linear in the number of bits required to write down the equation of the elliptic curve.

Next, we discuss a conjecture of Hindry, who proposed a Brauer-Siegel type formula for elliptic curves. Driven by a suggestion of Hindry, we prove assuming standard conjectures that there are infinitely many elliptic curves with Shafarevich-Tate group of size about as large as the square root of the minimal discriminant of the curve. This improves on a result of de Weger.

Thirdly, we consider certain quartic twists of an elliptic curve. We establish a reduction between the problem of factoring integers of a certain form and the problem of computing rational points on these twists. We illustrate that the size of Shafarevich-Tate group of these curves will make it computationally expensive to factor integers by computing rational points via the Heegner point method.

Finally, we sketch existing algorithms that compute the quantities appearing in the BSD formula and introduce strategies to parallelize them.

# Notation

The following standard notation will be used throughout this dissertation.

| | |
|---|---|
| $\mathbb{Z}$ | The integers. |
| $\mathbb{Q}$ | The rational numbers. |
| $\mathbb{Q}_p$ | The $p$-adic numbers. |
| $\mathbb{R}$ | The real numbers. |
| $\mathbb{C}$ | The complex numbers. |
| $\mathcal{H}$ | The upper half plane $\{z \in \mathbb{C} \mid \text{ im } z > 0\}$. |
| $\mathbb{Z}/n\mathbb{Z}$ | The ring of integers modulo $n$. |
| $\mathbb{F}_q$ | The finite field with $q$ elements. |
| $R^*$ | The group of units in a commutative ring $R$ with identity. |
| $\#S$ | The cardinality of a set $S$. |
| $char(R)$ | The characteristic of a ring $R$. |
| $f/R$ | A polynomial $f$ defined over a ring $R,$ that is, the coefficients of $f$ are in $R$. |

# Chapter 1

## Chapter One: Introduction

*At Kent he was curious about computer science but in just the introductory course Math 10 061 in Merrill Hall the math got to be too much for him.* J. Updike *in* Rabbit is Rich

Astronomers and biologists have had telescopes and microscopes respectively to aid in their research. With the advent of the computer, mathematicians acquired a powerful tool, using which they could generate data, make conjectures and try turning them into theorems — this was the dawn of the golden age of experimental mathematics.

This dissertation sits at the crossroads of number theory, algorithms and computation. Our excursion into number theory had a cryptographic motivation, namely trying to understand the Semaev-Smart-Satoh-Araki attack on the elliptic curve discrete logarithm problem [Sem98]. This naturally lead to the question of deciding whether the $p$-part of a certain group is nontrivial — see Appendix A. Proceeding from the above to computing elliptic curve rational torsion and in turn to the BSD conjecture has been a wonderful introduction to a world where conjectures abound and computations are indispensable.

The results which appear in this dissertation were obtained in collaboration with M.-D. Huang.

A major area of research in number theory is the study of solutions in $\mathbb{Q}$ to a system of polynomial equations defined over $\mathbb{Q}$. For instance, rational solutions to the Fermat equation $x^n + y^n = 1, n > 2$, which by a famous theorem of A. Wiles, do not exist. The problem of deciding the existence and computation of such solutions even when restricted to the one equation, two variable, degree 3 case becomes quite challenging and hence interesting. Elliptic curves arise naturally in this context.

Questions about rational solutions can be transformed into questions about integer solutions by switching to homogeneous coordinates, a process which "clears the denominators".

Now suppose the homogeneous equation $f(x_1, \ldots, x_n) = 0$ over $\mathbb{Q}$ has an integral solution, then trivially it has a real solution and moreover $f(X) \equiv 0 \bmod m$ for every integer $m$.

One might wonder if the converse holds true. In the case of quadratic forms it is a theorem (see [ST92, Page 15]).

**Theorem 1.0.1 (Hasse)** *A homogeneous quadratic equation in several variables is solvable by integers, not all zero, if and only if it is solvable in $\mathbb{R}$ and $\mathbb{Q}_p$ for each prime $p$.*

The field of *p-adic numbers* $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the $p$-adic absolute value. It can be viewed as a gadget which captures information about solutions of an equation modulo powers of the prime $p$.

Proceeding to an equation of degree greater than 2, we see that the projective plane curve over $\mathbb{Q}$ defined by the homogeneous equation $3x^3+4y^3+5z^3=0$ has a solution over every completion of $\mathbb{Q}$ but no solution in $\mathbb{Q}$. This is termed as the failure of the *Hasse local-global principle* and it is this phenomenon which renders "local" methods unusable and makes computing global points difficult in general.

The Birch and Swinnerton-Dyer conjecture can be viewed as an analogue of the Hasse principle for elliptic curves as it gives us a formula for the size of the Shafarevich-Tate group of an elliptic curve over $\mathbb{Q}$, an object which measures the extent of the failure of the global-local rule for the particular elliptic curve. But more importantly the conjecture gives information about the rank of the elliptic curve, a fundamental algebraic invariant via the order of zeros of the $L$-series of the elliptic curve, a complex analytic object.

Apart from the arithmetic problems which arise from the theory of elliptic curves, what makes these objects interesting to computer scientists is that they can be used to build cryptographic and coding theory systems [Kob94].

## 1.1 Elliptic Curves

*It is possible to write endlessly on elliptic curve. (This is not a threat.)* S. Lang *[Lan78]*

Our introductory definitions and theorems will closely follow J.H. Silverman's exposition on elliptic curves [Sil92]. The eager reader should consult his book for background material, proofs and further references.

**Definition 1.1.1** *An* elliptic curve *is a pair* $(E, O)$*, where* $E$ *is a curve of genus* 1 *and* $O \in E$*. (We just write E for the elliptic curve, the point O being understood.) The elliptic curve is* defined over $K$*, written* $E/K$*, if* $E$ *is defined over* $K$ *as a curve* $O \in E(K)$*.*

An elliptic curve over $K$ is given by the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.1}$$

where $a_i \in K$. If characteristic of $K$ is not 2 or 3 then $E$ can be transformed to be of the form

$$y^2 = x^3 + ax + b,$$

where $a, b \in K$. The smoothness (or non-singularity) condition above is equivalent to saying that the discriminant of $E$ $\Delta(E) = -16(4a^3 + 27b^2)$ is nonzero. In projective coordinates $[x, y, z]$, the elliptic curve equation is given by

$$y^2z = x^3 + axz^2 + bz^3,$$

and the point $O$ is taken to be the so-called *point at infinity* $[0, 1, 0]$, the point of intersection of the elliptic curve and $z = 0$, the line at infinity.

The chord-tangent construction *Chord-tangent construction* (namely $P, Q, R \in E(K)$ satisfy $P + Q + R = O$ if and only if they are collinear), can be used to turn $E(K)$, the set of $K$-rational points,

$$E(K) = \{(x_0, y_0) \in K \times K \mid y_0^2 = x_0^3 + ax_0 + b\} \cup \{O\} \tag{1.2}$$

into an abelian group with the point $O$ acting as the identity of the group. The fact that makes elliptic curves friendly to computation is that the geometric construction turns out to give a group law which is algebraic in nature [Sil92, Group Law Algorithm III.2.3].

### 1.1.1 Isogenies

After having presented the basic properties of the object, we now turn to the study relationships of objects via maps between them. In particular, we are interested in maps called *morphisms* which take $O$ of one elliptic curve to that of another [Sil92, §III.3].

**Definition 1.1.2** *An* isogeny *between elliptic curves $E_1, E_2$ is a morphism*

$$\phi : E_1 \to E_2$$

*satisfying $\phi(O) = O$. $E_1, E_2$ are said to be* isogenous *if there is a nontrivial isogeny between them, that is an isogeny s.t. $\phi(E_1) \neq \{O\}$.*

An important example of an isogeny is the *multiplication by $m$* morphism

$$[m] : E \to E$$

defined as follows: $[0]P = O$, if $m > 0$ then $[m]P = \underbrace{P + \ldots + P}_{m \text{ times}}$, otherwise $[m]P = [-m](-P)$. It is a fact that if $m \neq 0$, then $[m] \neq [0]$. Another important result is that the kernel of a nonzero isogeny is a finite group.

If $E$ is an elliptic curve over a field of characteristic zero, then the *degree* of $\phi$, a nonzero isogeny can be defined to be $\deg(\phi) := \# \ker \phi$ [Sil92, Theorem 4.10].

**Theorem 1.1.1** *Let $\phi : E_1 \to E_2$ be a non-constant isogeny of degree $m$. There exists a unique isogeny*

$$\hat{\phi} : E_2 \to E_1$$

*satisfying*

$$\hat{\phi} \circ \phi = [m].$$

$\hat{\phi}$ is called the *dual isogeny* to $\phi$. If $\phi = [0]$, then we set $\hat{\phi} = [0]$.

### 1.1.2 Torsion Points

The *m-torsion subgroup* of $E$, $E[m]$ is defined to be $\ker([m])$. The torsion subgroup of $E$ is the set of points of finite order, $\cup_{m=1}^{\infty} E[m]$. If $E$ is defined over $K$, then $E(K)_{tors}$ denotes the points of finite order in $E(K)$. The following fact gives us the structure of the torsion subgroup.

**Proposition 1.1.1** *Let $m \in \mathbb{Z}, m \neq 0$.*

1. *If char*$(K) = 0$ *or* $\gcd(m, \mathit{char}(K)) = 1$*, then*

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$$

2. *If char*$(K) = p$ *and* $m = p^e$*, then either*

$$\begin{aligned} E[m] &\cong \{O\} \quad \textit{for all } e = 1,2, \ldots; \textit{or} \\ E[m] &\cong \mathbb{Z}/m\mathbb{Z} \quad \textit{for all } e = 1,2, \ldots. \end{aligned}$$

### 1.1.3 Division Polynomials

Division polynomials of an elliptic curve over a field $K$ encode information about its torsion points. We will restrict our attention to the case when $K$ is a number field. Moreover what we say will also hold for $K$ being a finite field with $\mathrm{char}(K) > 3$ when the statements are viewed in the appropriate context. A general treatment of these polynomials can be found in [BSS00, §III.4].

Let $K$ be a number field and $\overline{K}$ be an algebraic closure of $K$. Let $E$ be an elliptic curve over $K$ given by a Weierstrass equation $y^2 = x^3 + ax + b$, where $a, b \in R$, where $R$ is the ring of integers of $K$.

We begin by presenting definitions and theorems concerning torsion points and polynomials which characterize them. Define *division polynomials* $\Psi_m$ recursively as follows:

$$\begin{aligned}
&\Psi_1 = 1,\ \Psi_2 = 2y,\ \Psi_3 = 3x^4 + 6ax^2 + 12bx - a^2,\\
&\Psi_4 = (2x^6 + 10ax^4 + 40bx^3 - 10a^2x^2 - 8bax - 2a^3 - 16b^2)\Psi_2,\\
&\Psi_{2k+1} = \Psi_{k+2}\Psi_k^3 - \Psi_{k-1}\Psi_{k+1}^3,\ k \geq 2\\
&\Psi_{2k} = (\Psi_{k+2}\Psi_{k-1}^2 - \Psi_{k-2}\Psi_{k+1}^2)\Psi_k/\Psi_2,\ k \geq 2.
\end{aligned}$$

Define for $m > 2$, $f_m = \Psi_m$, when $m$ is odd and $f_m = \Psi_m/\Psi_2$, when $m$ is even. Observe that $f_m$ (also referred to as division polynomials) are univariate. Let $d$ denote $\deg f_m$, which is equal to $\frac{m^2-1}{2}$, if $m$ is odd and $\frac{m^2-4}{2}$ otherwise. The leading coefficient of $f_m$ is $m$, when $m$ is odd and $\frac{m}{2}$ otherwise.

The $x$-coordinates of the $m$-torsion points of $E$ correspond to the roots of $f_m$ in the following way [BSS00, Corollary III.7]: Let $P \in E(\overline{K})$, such that $P$ is not a 2-torsion point then $P \in E(\overline{K})[m] \Leftrightarrow f_m(x(P)) = 0$.

We will now define the discriminant of a polynomial and related notions [Coh93, §3.3.2]. Let $S$ be an integral domain with quotient field $L$ and $\overline{L}$ be an algebraic closure of $L$. Let $g \in S[X]$ with $n = \deg(g)$, $lc(g)$ be its leading coefficient and $\alpha_i$ be the roots of $g$ in $\overline{L}$. Define the *discriminant* of $g$ to be

$$\Delta(g) = lc(g)^{n-1+deg(g')} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Let $f = x^3 + ax + b$ and hence $\Delta(f) = -(4a^3 + 27b^2)$. As indicated earlier, the discriminant of the elliptic curve is defined to be $\Delta(E) = -16(4a^3 + 27b^2)$ and the letter

$E$ is dropped when the curve is clear from the context. A formula for the discriminant of the $m$-division polynomial of an elliptic curve can be found in §2.2.2.

## 1.2 Elliptic curves over $\mathbb{F}_q$

Let $E$ be an elliptic curve over $\mathbb{F}_q$, the finite field with $p^n$ elements. H. Hasse proved the following conjecture of E. Artin, which provides bounds on the size of $E(\mathbb{F}_q)$.

**Theorem 1.2.1 (Hasse)** *Let $E$ be an elliptic curve over $\mathbb{F}_q$. Then*

$$\#E(\mathbb{F}_q) = q + 1 - a_q, \ \textit{with } |a_q| \leq 2\sqrt{q}$$

The Frobenius map $\mathbb{F}_q \to \mathbb{F}_q, x \mapsto x^q$, induces an isogeny on $E$, which in turn induces a map on the $l$-adic Tate module $T_l(E)$, where $l$ is a prime different from $p$. The $a_q$ appearing in the above theorem is the trace of the Frobenius map acting on $T_l(E)$ (see sections III.7, V.2 of [Sil92] for details).

## 1.3 Elliptic curves over $\mathbb{Q}$

The purpose of this section is to present some background material on elliptic curves over $\mathbb{Q}$ before we introduce the BSD conjecture.

A theorem of L.J. Mordell states that $E(\mathbb{Q})$ is finitely generated as a group. In other words:

**Theorem 1.3.1 (Mordell)**

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

*where $E(\mathbb{Q})_{tors}$, the torsion subgroup is finite and $r$ is a non-negative integer called the* rank *of $E(\mathbb{Q})$.*

Weil proved that the above theorem in the number field setting and the theorem is known as the Mordell-Weil theorem and $E(K)$ is called the Mordell-Weil group, where $K$ is a number field.

The free part of $E(\mathbb{Q})$ is a mysterious entity as compared to the torsion subgroup. Two important results about $E(\mathbb{Q})_{tors}$ are the following:

**Theorem 1.3.2 (Nagell, Lutz)** *Let $E$ be an elliptic curve over $\mathbb{Q}$ given by*

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

*Suppose $P \in E(\mathbb{Q})_{tors}$ is a nontrivial point ($P \neq O$) then*

1. *$x(P), y(P) \in \mathbb{Z}$ and*

2. *either $y(P) = 0$ or $y(P)^2 | (4a^3 + 27b^2)$.*

**Theorem 1.3.3 (Mazur)**

$$E(\mathbb{Q})_{tors} \cong \begin{cases} \mathbb{Z}/n\mathbb{Z}, & 1 \leq n \leq 10, 12, \ \textit{or} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, & 1 \leq n \leq 4. \end{cases}$$

Observe that an elliptic curve over $\mathbb{Q}$ can be transformed into the form which appears in the Nagell-Lutz theorem using a change of coordinates [Sil92, Pages 46-50].

Let us assume that $E$ is an elliptic curve over $\mathbb{Q}$ given by $y^2 = x^3+ax+b$, with $a, b \in \mathbb{Z}$. This implies that the division polynomials $f_m$ have integral coefficients and hence their discriminants $\Delta(f_m) \in \mathbb{Z}$, which is clear from the definition of the discriminant in terms of the Sylvester matrix [Coh93, Lemma 3.3.4].

A *global minimal model* for an elliptic curve over $\mathbb{Q}$ is an integral Weierstrass equation for which the absolute value of the discriminant is minimal among Weierstrass equations with coefficients in $\mathbb{Z}$ for the elliptic curve. The discriminant of such a model is called the *(global) minimal discriminant*. A closely related notion is that of a *local minimal model* of an elliptic curve over $\mathbb{Q}_p$. This is a Weierstrass equation for the elliptic curve with coefficients in $\mathbb{Z}_p$ such that $v_p$ of the discriminant is minimal among all Weierstrass equations with coefficients in $\mathbb{Z}_p$ for the elliptic curve. (The *valuation* $v$ at $p$ of a rational number r denoted by $v_p(r)$ is the largest integer power of $p$ which divides the number.)

### 1.3.1 Reduction of an elliptic curve modulo $p$

For the sake of exposition let $E$ be an elliptic curve over $\mathbb{Q}$ given by a global minimal Weierstrass equation

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

with $a_i \in \mathbb{Z}$.

We can now talk about reducing this equation modulo a prime. Recall that an elliptic curve is a smooth (or non-singular) curve, that is, there exists a unique tangent at each point of the elliptic curve. Considering the above equation modulo a prime $p$, we obtain an equation of a curve over $\mathbb{F}_p$. If this reduced curve is non-singular (singular), then $E$ is said to have good (bad) reduction at $p$. The type of bad reduction is classified based on the type of singularity (there is at most one), depending on whether the singularity is a cusp or a node. The former reduction is termed *additive* and the latter *multiplicative* reduction. If $E$ has multiplicative reduction, then the reduction is said to be split (non-split) if the slopes of the two tangents lines at the singular point are in (respectively not in) $\mathbb{F}_p$.

Let $y^2 = x^3 + ax + b$ be a minimal Weierstrass equation of $E$ an elliptic curve over $\mathbb{Q}_p$, where a prime $p > 3$ then $E$ is said to have good (bad) reduction at $p$ if $v_p(\Delta) = 0$ ($v_p(\Delta) > 0$). On the other hand, the type of bad reduction — multiplicative or additive — can be determined as follows: $E$ has multiplicative reduction if and only if $v_p(\Delta) \geq 1$ and $v_p(ab) = 0$ and it has additive reduction if and only if $v_p(a), v_p(b) \geq 1$ [Sil92, Exercise VII.7.1(b)]. Also $E$ has split multiplicative reduction if and only if the reduction of $-2ab$ modulo $p$ is a square [Milb, Page 27]. Otherwise $E$ is said to have non-split multiplicative reduction.

In general, to compute a minimal Weierstrass equation of an elliptic curve at $p$ and other local information, algorithm of J. Tate [Sil94, Chapter IV.9], [Cre97, §3.2] can be used.

### 1.3.2 L-series

When faced with an interesting subset of the natural numbers, it is natural to encode these numbers into a polynomial or power series and study its generating function. The L-series of an elliptic curve is one such example. It captures information about the reduced curve modulo each prime. An introduction to the content of this subsection can be found in [Kna92], [Milb] and [Sil92, Appendix §16].

Let $E$ be an elliptic curve over $\mathbb{Q}$, $p$ be a prime at which $E$ has good reduction and let $\overline{E}_p$ denote the elliptic curve modulo $p$. The *zeta function* of $\overline{E}_p$ over $\mathbb{F}_p$ is given by

$$Z(\overline{E}_p/\mathbb{F}_p;T) = \exp(\sum_{n=1}^{\infty} \#\overline{E}_p(\mathbb{F}_{p^n}) \cdot \frac{T^n}{n}).$$

We know that $Z(\overline{E}_p/\mathbb{F}_p;T)$ is a rational function [Sil92, Theorem V.2.4]

$$Z(\overline{E}_p/\mathbb{F}_p;T) = \frac{L_p(T)}{(1-T)(1-pT)},$$

where

$$L_p(T) = 1 - a_pT + pT^2 \in \mathbb{Z}[T] \text{ and } a_p = p + 1 - \#\overline{E}_p(\mathbb{F}_p).$$

The definition of $L_p(T)$ when $E$ has bad reduction at $p$ is as follows

$$L_p(T) = \begin{cases} 1 - T & \text{if E has split multiplicative reduction at p} \\ 1 + T & \text{if E has non-split multiplicative reduction at p} \\ 1 & \text{if E has additive reduction at p.} \end{cases}$$

Then in all cases we have the relation

$$L_p(p^{-1}) = \frac{\#\overline{E}_{ns}(\mathbb{F}_p)}{p},$$

where $\#\overline{E}_{ns}(\mathbb{F}_p)$ is the group of non-singular $\mathbb{F}_p$-points on $\overline{E}$.

**Definition 1.3.1** *The* L-series *of $E$ over $\mathbb{Q}$ is defined by the Euler product*

$$L_E(s) = \prod_p L_p(p^{-s})^{-1}.$$

The $L$-series of $E$ an elliptic curve over $\mathbb{Q}$ is a priori defined only for complex numbers $s \in \mathbb{C}$ with $Re(s) > \frac{3}{2}$.

Define $\Lambda_E(s) = (2\pi)^{-s} \cdot \Gamma(s) \cdot N(E)^{s/2} \cdot L_E(s)$, where $\Gamma(s)$ is the $\Gamma$-function.

**Theorem 1.3.4 (Hecke, Wiles et al.)** *The function $\Lambda_E(s)$ can be analytically continued to a complex analytic function on the whole of $\mathbb{C}$, and it satisfies a functional equation*

$$\Lambda_E(2 - s) = w(E) \cdot \Lambda_E(s),\ w(E) = \pm 1. \tag{1.3}$$

Wiles et al. proved the modularity conjecture (now theorem) that essentially states that $L_E(s)$ is the $L$-series associated to a modular form [BCDT01], and Hecke proved that the $L$-series of a modular form analytically continues and satisfies the above functional equation Eq. 1.3 (see [Milb, Theorem 26.5]). The import of Theorem 1.3.4 with regards to the BSD conjecture is that $L_E(s)$ has a Taylor expansion at $s = 1$.

The integer $N(E)$ is called the *conductor* of $E$, and the sign of the functional equation $w(E)$ is called the *root number* of $E$. The primes which divide $N(E)$ are the same as the primes which divide $\Delta(E)$ the minimal discriminant of $E$. For primes $p \geq 5$,

$$v_p(N(E)) = \begin{cases} 0 \quad \text{if E has good reduction at p} \\ 1 \quad \text{if E has multiplicative reduction at p} \\ 2 \quad \text{if E has additive reduction at p.} \end{cases}$$

Tate's algorithm can be used to compute $N(E)$, and there are formulae which can be used to compute $w(E)$ (see [Riz03]).

## 1.4 Selmer and Shafarevich-Tate groups

Let $\phi : E \to E'$ be an isogeny between elliptic curves $E, E'$ defined over $\mathbb{Q}$ and $\hat{\phi} : E' \to E$ be the dual isogeny of $\phi$. The following exact sequence arises from the Galois cohomology associated to $E$:

$$0 \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to S^{(\phi)}(E) \to Ш(E)[\phi] \to 0 \tag{1.4}$$

where $S^{(\phi)}(E)$ is the $\phi$-Selmer group of $E$ over $\mathbb{Q}$ and $Ш(E)$ is the (conjecturally finite) Shafarevich-Tate group of $E$ over $\mathbb{Q}$. It is known that if $\#Ш(E) < \infty$ then it is a square due to the existence of the Cassels-Tate pairing. We will proceed to give only a flavor of these groups, their definitions can be found in [Sil92, Chapter X].

The elements of $Ш(E)$ can be viewed as smooth curves called *(principal) homogeneous spaces* with the property that they have a point over $\mathbb{R}$ and $\mathbb{Q}_p$ for every prime $p$. An element of $Ш(E)$ which has a $\mathbb{Q}$-point corresponds to the trivial element of $Ш(E)$.

The group $S^{(\phi)}(E)$ is finite and computable and gives upper bounds for the size of $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$, the so-called *weak* Mordell-Weil group. It follows from the theory of height functions on elliptic curves that, once we have computed the weak Mordell-Weil group, the Mordell-Weil group $E(\mathbb{Q})$ can be recovered.

If an element $c \in S^{(\phi)}(E)$ maps to $0 \in Ш(E)$, then by the exactness of the sequence Eq. 1.4, $c$ arises from an element of $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$. Therefore, this *descent by $\phi$ isogeny* procedure reduces the computation of weak Mordell-Weil group to the question of existence of a rational point on a finite number of homogeneous spaces and the calculation of these points. The inability to decide whether a homogeneous space is a nontrivial element of $Ш(E)[\phi]$ is what makes rank computation using this procedure difficult.

In this context, the BSD conjecture comes to the rescue by providing information about the rank of the elliptic curve, via the order of zeros of the $L$-series of the curve. We give an overview of this conjecture in the next section.

## 1.5 Birch and Swinnerton-Dyer Conjecture

*This remarkable conjecture relates the behavior of a function L at a point where it is not at present known to be defined to the order of a group* Ш *which is not known to be finite!*

J. Tate

B.J. Birch and H.P.F. Swinnerton-Dyer made their famous conjecture [BSD63] inspired by the class number formula and computational evidence obtained using the EDSAC2 computer at Cambridge during the late 1950s. This interplay of Computer Science and Mathematics is what drew us to work on this conjecture. We fix some notation before we present the BSD conjecture.

1. $E$ : an elliptic curve over $\mathbb{Q}$.
2. $r_E$ : is the algebraic rank of $E$, that is $E(\mathbb{Q}) = E(\mathbb{Q})_{tors} \times \mathbb{Z}^{r_E}$.
3. $L_E(s)$: the $L$-series of $E$.
4. $L_E^{(t)}(1) := (\frac{d}{ds} L_E^{(t)}(s))|_{s=1}$.
5. $r_E^{an} := \min_t L_E^{(t)}(1) \neq 0$. That is the analytic rank of $E$ is defined as order of vanishing of $L_E(s)$ at $s = 1$.
6. $\omega := dx/(2y + a_1x + a_3)$, the invariant differential on a global minimal Weierstrass equation for $E$ over $\mathbb{Q}$, where $a_1, a_3$ are the coefficients of the Weierstrass equation (Eq. 1.1).
7. $\Omega := \int_{E(\mathbb{R})} |\omega|$ [Either the real period, or twice the real period, depending on whether or not $E(\mathbb{R})$ is connected.]

8. $Ш(E)$: the Shafarevich-Tate group of $E$ over $\mathbb{Q}$.

9. $Reg(E)$: the elliptic regulator of $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$, computed using the canonical height pairing.

10. $c_p$: $\#E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$, the Tamagawa number at prime $p$, where $E_0(\mathbb{Q}_p)$ is the subgroup of the group of $\mathbb{Q}_p$-points of $E$ that correspond to a non-singular point on the reduced curve at $p$.

11. $L_E^*(1) := \frac{L_E^{(r_E^{an})}(1)}{r_E^{an}!}$, the leading coefficient of the Taylor expansion of $L_E(s)$ at $s = 1$.

**Conjecture 1.5.1 (Birch, Swinnerton-Dyer)**

$$\begin{aligned} r_E^{an} &= r_E && (1.5) \\ L_E^*(1) &= \frac{\#Ш(E) \cdot Reg(E) \cdot \Omega \cdot \prod_p c_p}{(\#E(\mathbb{Q})_{tors})^2} && (1.6) \end{aligned}$$

Eq. 1.5 is referred to as the Weak BSD conjecture.

The quote of Tate at the beginning of this section does not reflect the current state of affairs with regards to the conjecture. The left hand side of Eq. 1.6 is well-defined (see §1.3.2), and the Shafarevich-Tate group has been proved to be finite when the rank of the elliptic curve is at most 1 by the work of B. Gross and D. Zagier, and V. Kolyvagin [Kol90]. Moreover,

$$r_E^{an} = 0 \Rightarrow r_E = 0 \quad (1.7)$$

$$r_E^{an} = 1 \Rightarrow r_E = 1. \quad (1.8)$$

There also results about the validity of the BSD formula in these cases — see [GJP$^+$05].

### 1.5.1 Congruent Number Problem

The BSD conjecture is closely related to an ancient problem: find an algorithm to determine whether or not a given integer $n$ is the area of some right angled triangle all of whose sides are rational numbers. If such a triangle exists, $n$ is called a *congruent number*. The following theorem of J.B. Tunnell states that assuming the BSD conjecture there is a verifiable criterion for the congruent number problem [Kob93].

**Theorem 1.5.1 (Tunnell)** *If $n$ is a squarefree and odd (respectively, even) positive integer and $n$ is the area of a right angled triangle with rational sides, then*

$$\#\{x, y, z \in \mathbb{Z} \mid n = 2x^2 + y^2 + 32z^2\} = \frac{1}{2}\#\{x, y, z \in \mathbb{Z} \mid n = 2x^2 + y^2 + 8z^2\}$$

*(respectively,*

$$\#\{x, y, z \in \mathbb{Z} \mid \frac{n}{2} = 4x^2 + y^2 + 32z^2\} = \frac{1}{2}\#\{x, y, z \in \mathbb{Z} \mid \frac{n}{2} = 4x^2 + y^2 + 8z^2\}).$$

*If the weak BSD conjecture is true for the elliptic curves $E_n : y^2 = x^3 - n^2x$, then, conversely, these equalities imply that $n$ is a congruent number.*

## 1.6 Outline of the dissertation

An aspect which makes computing the *mysterious* invariants of the BSD conjectural formula, namely the Shafarevich-Tate group and Regulator, interesting is that either there are no known algorithms that exist or the ones that do exist take exponential time.

In chapter 2 we introduce an $l$-adic torsion computation algorithm for an elliptic curve defined over $\mathbb{Q}$. We begin the chapter by presenting the facts which we leverage (Nagell-Lutz theorem and Mazur's classification) and the techniques we utilize (Hensel lifting) in the algorithm. The randomized version of this procedure runs in expected time which is essentially linear in number of bits required to write down the equation of the elliptic curve. We finish the chapter by analyzing the theoretical time complexity of the algorithm.

In Chapter 3 we discuss a conjecture of Hindry, who proposed a Brauer-Siegel type formula for elliptic curves over $\mathbb{Q}$. Driven by a suggestion of Hindry, we prove assuming standard conjectures that there are infinitely many elliptic curves with Shafarevich-Tate group of size about as large as the square root of the minimal discriminant of the curve.

The next chapter is devoted to study of certain quartic twists of the elliptic curve $y^2 = x^3 - x$, which raises interesting questions about integer factoring and heights of rational points. We establish a reduction between the problem of factoring integers of a certain form and the problem of computing rational points on these twists. We illustrate that the size of Shafarevich-Tate group of these curves will make it computationally expensive to factor integers by computing rational points via the Heegner point method.

Chapter 5 sketches existing algorithms that compute the invariants appearing in the BSD formula and introduces strategies to parallelize them.

In Appendix A we devise a polynomial-time algorithm (polynomial in $\log p$ and the bit length of the coefficients of the curve) that decides whether a given elliptic curve over $\mathbb{Q}_p$ has a nontrivial $p$-torsion part. The algorithm has two subroutines, the first procedure computes $\#E_0(\mathbb{Q}_p)[p]$ and the second determines $\#E(\mathbb{Q}_p)[p]$ when $E$ has split multiplicative reduction.

We present our original descent analysis for the aforementioned twists in Appendix B. The proof suggested by an anonymous referee, which is found in §4.1.1, is much shorter and perhaps more conceptual.

In Appendix C we tabulate computation driven by the questions and conjectures of Chapter 3. Specifically, we compute the Brauer-Siegel ratio of $E$, for the elliptic curves in databases [Cre], [SW02], and certain rank 0 elliptic curves.

*I wrote this book and compiled in it everything that is necessary for the computer,*
*avoiding both boring verbosity and misleading brevity.*

Ghiyath al-Din Jamshid Mas'ud al-Kashi *in* The Key to Arithmetic *(1427)*

# Chapter 2

# Chapter Two: Computing Elliptic Curve Rational Torsion

*The object of numerical computation is theoretical advance. A.O.L. Atkin [Bir98]*

The Mordell-Weil theorem says that given an elliptic curve $E$ over a number field $K$, the group of $K$-rational points $E(K)$ is finitely generated. This implies that the group of $K$-rational torsion $E(K)_{tors}$ is finite. A theorem of B. Mazur states the groups which can appear as $E(K)_{tors}$, when $K = \mathbb{Q}$.

Let $E$ be an elliptic curve over $\mathbb{Q}$ defined by $y^2 = x^3 + ax + b$, where $a, b \in \mathbb{Z}$ and let $H(E) = \max\{|a|^3, |b|^2\}$. Any elliptic curve over $\mathbb{Q}$ can be efficiently transformed to the above form. The purpose of this chapter is to introduce methods which efficiently compute elliptic curve rational torsion and to prove the following theorem.

**Theorem 2.0.1** *There is a randomized algorithm which computes $E(\mathbb{Q})_{tors}$ in $\mathcal{O}(\log H(E))$ expected time. The deterministic version of the algorithm runs in $\mathcal{O}(\log^2 H(E))$ time.*

*Notation*. The *soft-Oh* notation $\mathcal{O}$ refers to the fact that logarithmic factors in the length of input are ignored. A time step is a bit operation and the words *size* and *bit length* of an integer will used synonymously. The discriminant of an elliptic curve $E$ will be denoted by $\Delta(E)$ or simply $\Delta$.

We begin by briefly recalling the current approaches to determine $E(\mathbb{Q})_{tors}$. Firstly, one can compute torsion in a brute force fashion using the Nagell-Lutz theorem, which states that torsion points are integral and bounded in magnitude, but this technique can be computationally expensive. This naïve method was superseded by D. Doud's complex analytic cubic time algorithm [Dou98].

I. García-Selfa et al. [GSOT02] proposed a softly quadratic time algorithm ("softly" refers to the soft-Oh notation), where they compute with the Tate Normal Form of an elliptic curve. Their procedure uses R. Loos' root-finding algorithm as a blackbox routine and does not use any information about how the discriminants of $F_m$ (polynomials which arise in their algorithm) are related to the discriminant of the elliptic curve.

The roots of the so-called division polynomials correspond to the $x$-coordinates of torsion points of the elliptic curve (see §1.1.3). Our algorithm discussed in §2.3 performs root-finding on these polynomials using an $l$-adic approach. It has a worst case softly quadratic running time and the randomized avatar of this method runs expectedly in softly linear number of bit operations.

The basic idea of the algorithm is given an elliptic curve $E$ over $\mathbb{Q}$ we view it as a curve over $\mathbb{Q}_l$ and use Hensel lifting to compute $E(\mathbb{Q}_l)[m]$, the $\mathbb{Q}_l$-rational $m$-torsion points, to desired precision. The values of $m$ we investigate are dictated by Mazur's result and the sufficient precision to work with is supplied by the Nagell-Lutz theorem. We then check to see if these points are in $E(\mathbb{Q})$. We discuss time complexity analysis of the above torsion computation procedure in §2.4.

The choice of the prime $l$ rests on the fact that the prime support of the discriminant of the $m$-division polynomial equals the prime support of $m$ and the prime support of the discriminant of the elliptic curve, which we prove in §2.2.1. This relationship between the discriminants enables us to use a single "good" prime to compute the $m$-torsion for all $m$. In order to relate $\Delta(f_m)$, the discriminant of $f_m$ the $m$-division polynomial, to $\Delta$, the discriminant of the elliptic curve, we symbolically computed the discriminants of these polynomials using for small values of $m$. This led us to discover a formula for $\Delta(f_m)$. In §2.2.2 we establish the equivalence of this formula when $m$ is odd to a lemma of H.M. Stark.

We would like to thank N.D. Elkies for pointing out that the running times of the algorithms as presented in [BH05], being polynomials in $\log|\Delta(E)|$, are conditional on the weak version of the Frey-Szpiro conjecture (Conjecture 3.1.6). The mistake was due to the assumption that length of input is asymptotically upper bounded by the size of the discriminant $\log H(E) = O(\log|\Delta(E)|)$. The same inaccuracy occurs in the paper of García-Selfa et al [GSOT02].

## 2.1 $E(\mathbb{Q})_{tors}$ and Hensel's lemma

The purpose of this section is to present some background material [Sil92, Chapter VIII] before we introduce our elliptic curve rational torsion algorithm. A corollary of the Mordell-Weil Theorem states that $E(\mathbb{Q})_{tors}$ is a finite group. To determine this group the methods, which are currently in use, are guided by the theorems of Nagell-Lutz and Mazur, which were stated in §1.3.

Suppose $P \in E(\mathbb{Q})_{tors} \setminus E(\mathbb{Q})[2]$ then $x(P)$ will be a root of $x^3 + ax + b - y(P)^2$. The Nagell-Lutz theorem tells us that $y(P)^2 | (4a^3 + 27b^2)$ which implies $x(P) | (b - (4a^3 + 27b^2)/k)$ for some $k \in \mathbb{Z}$. If $P \in E(\mathbb{Q})[2]$ and nontrivial then reasoning similar to the above leads to $x(P)|b$ since $y(P) = 0$. Hence the coordinates of the torsion points are $O(H(E))$ in magnitude.

The brute-force approach to compute torsion is to try out all the possible values for $y(P)^2$ such that it divides $4a^3 + 27b^2$. In the worst case this is computationally expensive as it involves factoring and also $4a^3 + 27b^2$ might have many square divisors giving rise to many possibilities [Dou98].

Instead our algorithm performs root-finding on division polynomials using the following variant of a lemma of K. Hensel [FGH00, Lemma 2.1]:

**Lemma 2.1.1 (Hensel)** *Let $u \in \mathbb{Z}_p$ and $h \in \mathbb{Z}_p[x]$. Let $k$ be such that $p^k || h'(u)$ and assume $p^{n+k} | h(u)$ for some $n > k$. Let*

$$\delta = \frac{p^{-k} h(u)}{p^{-k} h'(u)}$$

*and $v = u - \delta$. Then $v \equiv u \bmod p^n$, $p^{2n} | h(v)$ and $p^k || h'(v)$.*

Hensel's lemma states that an approximate root of a polynomial, which is not a repated root, can be used to obtain a root which has at least twice as much precision. This leads to a softly linear time method to find a root provided the initialization procedure, where the approximate root is computed modulo $p^k$, does not take more than softly linear time.

## 2.2 Discriminant of the division polynomial

In this section we prove a few facts about the discriminant of $f_m$, in particular Lemma 2.2.3, which makes $l$-adic torsion computation efficient.

### 2.2.1 Prime support of $\Delta(f_m)$

**Lemma 2.2.1** *Let $m = 2k + 1 > 1$ be an integer.*

1. $f || f'_m$

2. $2^2 | f'_m$

3. $m | f'_m$

4. $m^{d-1} | \Delta(f_m)$

**Proof 2.2.1** 1. *We will prove this by induction on $m$. $f'_3 = 12f$ and the base case holds. Suppose $f | f'_i$ for all odd $i < m$. Let us assume $k$ is odd (in the even case a similar argument applies). We have $\Psi_{2k+1} = f_{2k+1} = f_{k+2}f_k^3 - (f_{k-1}\Psi_2)(f_{k+1}\Psi_2)^3$ $= f_{k+2}f_k^3 - f_{k-1}f_{k+1}^3\Psi_2^4 = f_{k+2}f_k^3 - 2^4 \cdot f_{k-1}f_{k+1}^3 f^2$. Now $f'_{2k+1} = f'_{k+2}f_k^3 + 3 \cdot f_{k+2}f_k^2 f'_k - 2^4 \cdot (f_{k-1}f_{k+1}^3)' f^2 - 2^5 \cdot f_{k-1}f_{k+1}^3 f f'$. $f$ divides $f'_{k+2}$ and $f'_k$ by the inductive assumption and hence $f$ divides each of the terms in $f'_{2k+1}$. In particular $f$ exactly divides $f'_{2k+1}$, otherwise $f_{2k+1}$ would have repeated roots.*

2. *The argument is similar to the one above for part* 1.

3. *By [Cas49, Theorem* 1 *and Corollary* 1*] we have* $m|(\Psi_m^2)'$ *for any* $m$ *and* $p \nmid \Psi_m^2$ *for any odd prime* $p$*. Suppose* $m = \prod_i p_i$*, where* $p_i$ *are odd primes. From the above,* $m|\Psi_m\Psi_m'$ *which implies* $p_i|\Psi_m\Psi_m'$*. Also* $p_i \nmid \Psi_m$*. Therefore* $p_i|\Psi_m'$ *and therefore* $m|\Psi_m'$*.*

4. *The statement follows from part* 3*,* $lc(f_m) = m$ *and the matrix definition of the discriminant, where the coefficients of* $f_m'$ *are repeated on* $\frac{m^2-1}{2}$ *rows.*

**Lemma 2.2.2** *Let* $m = 2k > 2$ *be an integer.*

1. $k|\Delta(f_m)$

2. $2^2|f_m'$

3. $m|\Delta(f_m)$

**Proof 2.2.2** 1. *Recall that* $lc(f_m) = k$ *and the coefficient of* $x^{d-1}$ *in* $f_m$ *is* $0$*. Consider the matrix associated to* $R(f_m, f_m')$*. The first column of this matrix has* $k$ *at entry* $(1, 1)$ *and* $k\frac{m^2-4}{2}$ *at* $(\frac{m^2-4}{2}, 1)$ *and* $0$ *elsewhere. The second column of this matrix has* $k$ *at entry* $(2, 2)$ *and* $k\frac{m^2-4}{2}$ *at entry* $(\frac{m^2-4}{2} + 1, 2)$ *and* $0$ *elsewhere. Hence* $k^2|R(f_m, f_m')$ *and* $k|\Delta(f_m)$ *by the definition of discriminant.*

2. $2^2|f_4'$ *and the base case holds. Suppose* $2^2|f_i'$ *for all even* $i < m$*. Now* $f_{2k}' = (f_{k+2}f_{k-1}^2 - f_{k-2}f_{k+1}^2)f_k' + (f_{k+2}'f_{k-1}^2 + f_{k+2} \cdot 2 \cdot f_{k-1}f_{k-1}' - f_{k-2}'f_{k+1}^2 - f_{k-2} \cdot 2 \cdot f_{k+1}f_{k+1}')f_k$*. Let us assume that* $k$ *is odd (similar analysis for the even case). From the previous lemma we know that* $2^2$ *divides* $f_k', f_{k+2}', f_{k-2}'$*. By the inductive hypothesis* $2^2$ *also divides* $f_{k-1}', f_{k+1}'$*. Hence* $2^2|f_m'$*.*

*3. Follows from part* 1 *and* 2.

**Lemma 2.2.3** *Prime support of* $\Delta(f_m)$ = *prime support of* $m$ $\cup$ *prime support of* $\Delta$, *where* $m > 2$ *is an integer.*

**Proof 2.2.3** *Lemmas 2.2.1 and 2.2.2 state that* 2 *and* $m$ *divide* $\Delta(f_m)$. *Hence it suffices to consider the primes* $p$, *which are relatively prime to* $m$, *and prove that* $p$ *is in the prime support of* $\Delta(f_m)$ *if and only if* $p$ *is in the set of primes where* $E$ *has bad reduction over* $\mathbb{Q}$.

*Consider* $E$ *to be an elliptic curve over* $\mathbb{Q}_p$. *We will take a minimal Weierstrass equation denoted again by* $E$ *and let its discriminant be* $\Delta$. *Let* $L$ *be a finite extension of* $\mathbb{Q}_p$. *Let* $\mathfrak{p} = (\pi)$ *be a prime over* $p$ *in the ring of integers of* $L$, $\mathbb{F}_\mathfrak{p}$ *the residue field and* $e$ *the ramification index.*

*Let* $x = u^2x' + r, y = u^3y' + su^2x' + t$ *be a change of coordinates giving a minimal Weierstrass equation for* $E/L$ *denoted by* $E'$. *The discriminant* $\Delta'$ *for* $E'$ *satisfies* $\Delta' = u^{-12}\Delta$ *and hence* $v_\mathfrak{p}(\Delta') = -12v_\mathfrak{p}(u) + v_\mathfrak{p}(\Delta)$.

*Let* $x_i$ *and* $x_i'$, $1 \leq i \leq d$ *be the roots of the* $m$*-division polynomial associated to* $E$ *and* $E'$ *respectively. For* $i \neq j$, *we have* $v_\mathfrak{p}(x_i' - x_j') = v_\mathfrak{p}(\frac{x_i - r}{u^2} - \frac{x_j - r}{u^2}) = v_\mathfrak{p}(\frac{x_i - x_j}{u^2})$ *and hence* $v_\mathfrak{p}(x_i - x_j) = 2v_\mathfrak{p}(u) + v_\mathfrak{p}(x_i' - x_j')$.

*Now let us consider the valuation of the discriminant of the* $m$*-division polynomial associated to* $E$ *over* $\mathbb{Q}_p$*:*

$$v_\mathfrak{p}(\Delta(f_m)) = (2d-2)v_\mathfrak{p}(lc(f_m)) + 2\sum_{1 \leq i < j \leq d}(2v_\mathfrak{p}(u) + v_\mathfrak{p}(x_i' - x_j'))$$

*Suppose* $(m,p)=1$. *Observe that* $v_{\mathfrak{p}}(\cdot)=ev_p(\cdot)$. *Since* $v_p(m)=0$, *we have* $v_{\mathfrak{p}}(lc(f_m))=v_{\mathfrak{p}}(m)=0$ *when* $m$ *is odd and when* $m$ *is even, we have* $v_{\mathfrak{p}}(lc(f_m))=v_{\mathfrak{p}}(m/2)=0$.

***Case 1***. *Let* $E$ *be an elliptic curve with potential good reduction over* $\mathbb{Q}_p$. *Let* $L=\mathbb{Q}_p(E(\overline{\mathbb{Q}}_p)[m])$ *be a finite extension of* $\mathbb{Q}_p$ *over which* $E$ *has good reduction [Sil94, Proposition IV.10.3] which means* $v_{\mathfrak{p}}(\Delta')=0$ *and therefore* $v_{\mathfrak{p}}(u)=v_{\mathfrak{p}}(\Delta)/12$.

*Moreover the reduction modulo* $\mathfrak{p}$ *map* $E(L)[m]\to\overline{E}(\mathbb{F}_{\mathfrak{p}})[m]$ *is injective [Sil92, Proposition VII.3.1 b] and hence* $v_{\mathfrak{p}}(x_i'-x_j')=0$ *for all* $i\neq j$ *and hence* $v_{\mathfrak{p}}(\Delta(f_m))=d(d-1)/6\cdot v_{\mathfrak{p}}(\Delta)$ *which implies that*

$$v_p(\Delta(f_m))=\frac{d(d-1)}{6}\cdot v_p(\Delta)$$

*Hence if* $p$ *is a prime of good reduction for* $E/\mathbb{Q}$ *then* $p\nmid\Delta(f_m)$ *and if* $p$ *is a prime of bad (additive) reduction then* $p|\Delta(f_m)$.

***Case 2***. *Let* $E$ *be an elliptic curve with potential multiplicative reduction over* $\mathbb{Q}_p$. *Let* $L\supset\mathbb{Q}_p(E(\overline{\mathbb{Q}}_p)[m])$ *be a finite extension of* $\mathbb{Q}_p$ *over which* $E$ *has (split) multiplicative reduction which means* $v_{\mathfrak{p}}(\Delta')>0$ *and* $v_{\mathfrak{p}}(c_4')=0$. *We know that* $v_{\mathfrak{p}}(c_4')=v_{\mathfrak{p}}(u^{-4}c_4)$ *therefore* $v_{\mathfrak{p}}(u)=v_{\mathfrak{p}}(c_4)/4$. *Also* $j=c_4^3/\Delta$ *and this implies* $v_{\mathfrak{p}}(c_4)=\frac{1}{3}\cdot(v_{\mathfrak{p}}(\Delta)+v_{\mathfrak{p}}(j))$.

$$v_{\mathfrak{p}}(\Delta(f_m))=\frac{d(d-1)}{6}\cdot(v_{\mathfrak{p}}(\Delta)+v_{\mathfrak{p}}(j))+\sum_{1\leq i<j\leq d}2v_{\mathfrak{p}}(x_i'-x_j')$$

*Now* $v_{\mathfrak{p}}(\Delta) + v_{\mathfrak{p}}(j) = 0$ *or* $> 0$ *depending on whether* $E$ *has multiplicative or additive reduction over* $\mathbb{Q}_p$*. Also in either case there exist* $i, j$ *such that* $v_{\mathfrak{p}}(x'_i - x'_j) > 0$ *(x-coordinates of points which reduce to the singular point). Hence* $v_{\mathfrak{p}}(\Delta(f_m)) > 0$ *which implies* $v_p(\Delta(f_m)) > 0$*.*

*Therefore if* $p$ *is a prime of bad (additive or multiplicative) reduction for* $E$ *over* $\mathbb{Q}$ *then* $p|\Delta(f_m)$*.*

### 2.2.2 Discriminant formula for $f_m$

While investigating the discriminant of the $m$-division polynomials we stumbled upon a precise formula which expresses $\Delta(f_m)$ in terms of $m$ and the discriminant of the elliptic curve $E$. Based on symbolically computing the discriminants of $m$-division polynomials for $3 \leq m \leq 12$ using MAGMA [BCP97], we arrived at the following:

$$\Delta(f_m) = \begin{cases} (-1)^{\frac{m-1}{2}} & \cdot \quad m^{d-1} \cdot \Delta^{\frac{d(d-1)}{6}} \quad m \text{ odd, or} \\ 2^4 & \cdot \quad m^{d-4} \cdot \Delta^{\frac{d(d-1)}{6}} \quad m \text{ even.} \end{cases} \tag{2.1}$$

The above formula in the odd case turns out to be equivalent to a lemma of H.M. Stark [Sta82], which he proved using a complex-analytic approach, in particular L. Kronecker's second limit formula. Stark's result deals with an elliptic curve $E$ given in Weierstrass normal form by $y^2 = 4x^3 - g_2x - g_3$, where $g_2$ and $g_3$ are rational. This equation can be parameterized by the Weierstrass $\wp$-function, $x = \wp(w), y = \wp'(w)$. Suppose $N$ is odd and let $v_1$ and $v_2$ run through a set of representatives of $N^{-1}\Omega \bmod \Omega$, where $\Omega$ is the period lattice of $E$. It is shown that

$$\prod_{v_1 \not\equiv 0, v_2 \not\equiv 0, v_1 \pm v_2 \not\equiv 0} [\wp(v_1) - \wp(v_2)] \quad = \quad \pm N^{-2(N^2-3)} \Delta(E)^{(N^2-1)(N^2-3)/6}. \qquad (2.2)$$

Note that the above equation is a product over of differences of torsion points, which are distinct and not inverses of each other.

Now we will establish the equivalence between our formula and that of Stark. Let $m$ be an odd number and let the roots of $f_m$ be denoted by $x_i$, $1 \leq i \leq d$, then by the definition of the discriminant of a polynomial as stated in §1.1.3,

$$\Delta(f_m) = lc(f_m)^{2d-2} \prod_{1 \leq i < j \leq d} (x_i - x_j)^2$$

where $lc(f_m) = m$ and $d = deg\ f_m = \frac{m^2-1}{2}$. Using our formula modulo sign, we have

$$\prod_{i \neq j} (x_i - x_j) = \prod_{1 \leq i < j \leq d} (x_i - x_j)^2 = \frac{\Delta(f_m)}{m^{2d-2}} = m^{-\frac{m^2-3}{2}} \Delta^{\frac{(m^2-1)(m^2-3)}{24}}. \qquad (2.3)$$

The above equation is a product of differences of distinct $x$-coordinates of the torsion points. Now comparing Eq. 2.2 with Eq. 2.3 and taking $m = N$ we see that they are equivalent up to fourth root, which is explained by the difference in the products.

## 2.3 The $l$-adic algorithm

*Beware of bugs in the above code; I have only proved it correct, not tried it.* D. E. Knuth

As stated in the introduction of this chapter, our algorithm works as follows: given an elliptic curve $E$ over $\mathbb{Q}$ we view it as a curve over $\mathbb{Q}_l$ and using the appropriate factor of the $m$-division polynomial we compute the $\mathbb{Q}_l$-rational $m$-torsion points to desired precision and then check to see if they are, in fact, in $E(\mathbb{Q})$. The prime $l$ is chosen such that $E$ over $\mathbb{Q}_l$ has good reduction. The integers $m$ we have to consider are dictated by Mazur's theorem.

**Algorithm 2.3.1** *Input. An elliptic curve $E$ in the form $y^2 = x^3 + ax + b$, with $a, b \in \mathbb{Z}$.*

*Output. $< T, t >_i$, where $T \in E(\mathbb{Q})[t]$ and $i = 1, 2$ and these points are the generators of $E(\mathbb{Q})_{tors}$.*

```
1. Pick a prime $l > 7$ such that $l \nmid \Delta$.
2. Compute $E(\mathbb{Q}_l)[2]$ using $f$.
3. $r \leftarrow \#E(\mathbb{Q})[2] - 1$. Let $R_1, \ldots, R_r$ be the nontrivial $2$-torsion points.
4. If $r = 0$ then
    (a) For $p = 3, 5, 7$ do the following:
        i. If $p \nmid \#\overline{E}(\mathbb{F}_l)$ then goto start of the loop and iterate with next prime.
        ii. Compute $Q \in E(\mathbb{Q}_l)[p] \setminus \{O\}$ using $f_p$.
        iii. If $Q \notin E(\mathbb{Q})$ then goto start of the loop and iterate with next prime.
        iv. If $p = 5, 7$ then Return $< Q, p >$.
        v. If $3^2 | \#\overline{E}(\mathbb{F}_l)$ then
            • Compute $S \in E(\mathbb{Q}_l)[9] \setminus E(\mathbb{Q}_l)[3]$ using $f_9$. If $S \notin E(\mathbb{Q})$ then Return
              $< Q, 3 >$ else Return $< S, 9 >$.
            • else Return $< Q, 3 >$.
    (b) Return $< O, 1 >$.
5. If $r = 1$ then
    (a) For $p = 3, 5$ do the following:
        i. If $p \nmid \#\overline{E}(\mathbb{F}_l)$ then goto start of the loop and iterate with next prime.
        ii. Compute $Q \in E(\mathbb{Q}_l)[p] \setminus \{O\}$ using $f_p$.
        iii. If $Q \notin E(\mathbb{Q})$ then goto start of the loop and iterate with next prime.
        iv. $U \leftarrow R_1 + Q$.
        v. If $p = 5$ then Return $< U, 10 >$.
        vi. If $4 \nmid \#\overline{E}(\mathbb{F}_l)$ then Return $< U, 6 >$.
        vii. Compute $V \in E(\mathbb{Q}_l)[4] \setminus E(\mathbb{Q}_l)[2]$ using $f_4$.
        viii. If $V \in E(\mathbb{Q})$ then
            • Return $< V + Q, 12 >$.
            • else Return $< U, 6 >$.
    (b) If $4 \nmid \#\overline{E}(\mathbb{F}_l)$ then Return $< R_1, 2 >$.
    (c) Compute $W \in E(\mathbb{Q}_l)[4] \setminus E(\mathbb{Q}_l)[2]$ using $f_4$.
    (d) If $W \in E(\mathbb{Q})$ then
        • If $8 \nmid \#\overline{E}(\mathbb{F}_l)$ then Return $< W, 4 >$.
        • Compute $Z \in E(\mathbb{Q}_l)[8] \setminus E(\mathbb{Q}_l)[4]$ using $f_8$.
        • If $Z \in E(\mathbb{Q})$ then
```

```
            – Return $< Z, 8 >$.
            – else Return $< W, 4 >$.
    (e) Return $< R_1, 2 >$.
6. If $r = 3$ then
    (a) Do the following:
        i. If $3 \nmid \#\overline{E}(\mathbb{F}_l)$ then exit loop.
        ii. Compute a point $Q \in E(\mathbb{Q}_l)[3] \setminus \{O\}$ using $f_3$.
        iii. If $Q \in E(\mathbb{Q})$ then
            A. $U \leftarrow R_1 + Q$.
            B. Return $< U, 6 >$ and $< R_2, 2 >$.
    (b) Do the following:
        i. If $8 \nmid \#\overline{E}(\mathbb{F}_l)$ then Return $< R_1, 2 >$ and $< R_2, 2 >$.
        ii. Compute $W \in E(\mathbb{Q}_l)[4] \setminus E(\mathbb{Q}_l)[2]$ using $f_4$.
        iii. If $W \in E(\mathbb{Q})$ then
            • If $16 \nmid \#\overline{E}(\mathbb{F}_l)$ then Return $< W, 4 >$ and $< R_2, 2 >$.
            • Compute $Z \in E(\mathbb{Q}_l)[8] \setminus E(\mathbb{Q}_l)[4]$ using $f_8$.
            • If $Z \in E(\mathbb{Q})$ then
                – Return $< Z, 8 >$ and $< R_2, 2 >$.
                – else Return $< W, 4 >$ and $< R_2, 2 >$.
    (c) Return $< R_1, 2 >$ and $< R_2, 2 >$.
```

**Theorem 2.3.1** *The elliptic curve rational torsion algorithm works as desired.*

**Proof 2.3.1** *We recall that the discriminant of a polynomial gives us an upper bound on the precision at which the roots of the polynomial separate. The discriminant of the division polynomial depends on the discriminant of the elliptic curve (Lemma 2.2.3, Eq. 2.1), in particular we know that* $v_l(\Delta(f_m)) = \frac{(m^2-3)(m^2-1)}{24} v_l(\Delta)$*, where* $l$ *is an odd prime such that* $\gcd(l, m) = 1$ *and* $m > 2$.

*Our choice of prime* $l > 7$ *and* $l \nmid \Delta$ *implies that* $E$ *has good reduction at* $l$ *and the reduction map* $E(\mathbb{Q}_l)[m] \to \overline{E}(\mathbb{F}_l)[m]$ *is injective for all values of* $m$ *that we consider (*$m = 2, 3, 4, 5, 7, 8, 9$*). If* $m | \#\overline{E}(\mathbb{F}_l)$ *then the roots of* $f_m$ *are distinct modulo* $l$ *and therefore we can lift an* $\mathbb{F}_l$*-root of* $f_m$ *to* $\mathbb{Q}_l$ *using Hensel's lemma with* $k = 0$.

*We note that* $x$*-coordinates of torsion points which are negative integers have* $l - 1$ *as a recurring digit in their* $l$*-adic expansion. Such integers can be recovered using the following identity:* $\sum_{i=0}^{O(\lceil \log_l H(E) \rceil)} a_i l^i = -(l - a_0 + \sum_{i=1}^{O(\lceil \log_l H(E) \rceil)} (l - 1 - a_i) l^i)$*, where the left hand side represents truncated* $l$*-adic expansion of the negative integer. In other words, as the final step of the algorithm we need to check whether a candidate* $x$*-coordinate or its "negation" leads to a point in* $E(\mathbb{Q})$*. This can be determined using the given integral model of the elliptic curve.*

## 2.4 Time complexity analysis

Let $M(N)$ denote the bit operations required to multiply two numbers of size $N$. We will assume that a fast integer multiplication algorithm like Schönhage-Strassen is used in which case $M(N) = O(N \log N \log \log N) = \mathcal{O}(N)$ [vzGG03, Theorem 8.24]. An integer of size $N$ can be expressed $p$-adically using a recursive procedure called radix conversion in $O(M(N \log p) \log N)$ time [vzGG03, Theorem 9.17]. Due to the quadratic convergence of Hensel lifting, if the desired precision is $N$ then we can perform lifting in $O(M(N \log p))$ bit operations (assuming the degree of the polynomial is constant) [vzGG03, Theorem 9.26].

Given an elliptic curve with integral coefficients and discriminant $\Delta$, we use Tate's algorithm [Cre97, Chapter 3.2] to compute the minimal Weierstrass equation at a prime $p$. Let $\gamma = \max\{H(E), p\}$. Then the time complexity of Tate's algorithm is $\mathcal{O}(\log \gamma)$ (plus the time to compute the number of roots of certain quadratic and cubic congruences modulo $p$). The prime we work with is very small in bit length compared to $\log |\Delta|$ (see below for details). Hence in our context the running time of Tate's procedure is $\mathcal{O}(\log H(E))$.

To find a prime $l > 7$ which does not divide $\Delta$ deterministically takes $\mathcal{O}(\log^2 |\Delta|)$ time [GSOT02], whereas resorting to a randomized algorithm takes $\mathcal{O}(\log H(E))$ expected time [vzGG03, Corollary 18.12 (ii)]. Since in both the determinstic and randomized cases the magnitude of the prime selected is small — $\mathcal{O}(\log |\Delta|)$ — the time to compute $\#\overline{E}(\mathbb{F}_l)$ or to find a $\mathbb{F}_l$-root of the division polynomial is negligible. Once we find an approximate root of a division polynomial, we use Hensel lifting to compute a $\mathbb{Q}_l$-root up to $O(\log_l H(E))$ accuracy and the time complexity of this operation is $O(M((\log_l H(E)) \log l)) = \mathcal{O}(\log H(E))$ bit operations.

Therefore, the routine to find the good prime dictates the overall running time of the $l$-adic algorithm, which is $\mathcal{O}(\log^2 |\Delta|)$ deterministic time or an expected running time of

$\mathcal{O}(\log|\Delta|)$. Phrasing the time complexity in terms of $\mathcal{O}(\log H(E))$, the length of input of the algorithm, completes the proof of Theorem 2.0.1.

In practice to compute an upper bound for the size of the elliptic curve rational torsion subgroup, $\#E(\mathbb{F}_l)$ is computed for a few primes $l$ of good reduction and their gcd is determined. Moreover, this bound is a multiple of $E(\mathbb{Q})_{tors}$ and hence restricts the orders of the torsion points which can exist for $E$. This recipe gives rise to the following theoretical question: what is a bound for when the sequence

$$\{\gcd(\{\#E(\mathbb{F}_l) \mid l \textit{ is a odd prime of good reduction}\}_{l\leq X})\}_X$$

stabilizes?

We plan to work on the above based on an idea of F. Voloch. This question becomes quite interesting in the context of computing torsion for elliptic curves over number fields, where structural results à la Mazur exist only for extensions of degrees at most 4 [KM95,JKP06] and the uniform bounds of J. Oesterlé and P. Parent [Par99] are too big to be useful to explicitly bound elliptic curve torsion over number fields of higher degrees. In addition, we could elicit information about the existence of isogenous curves in certain cases due to the results of J.-P. Serre and N.M. Katz [Kat81, Theorem 2].

# Chapter 3

# Chapter Three: Brauer-Siegel Analogue for Elliptic Curves

*Mathematics often owes more to those who ask questions than to those who answer them. R. K. Guy [Guy04]*

M. Hindry proposed a Brauer-Siegel type conjecture for abelian varieties over number fields [Hin]. We raise questions and present results motivated by this conjecture specialized to elliptic curves over rationals. Appendix C tabulates computation inspired by the contents of this chapter.

We begin by introducing the classical Brauer-Siegel theorem, which describes the growth of the class number and regulator with respect to the discriminant of a number field (see [Bra47] and [Coh93]).

**Theorem 3.0.1 (Brauer, Siegel)** *Let $K$ vary over a family of number fields of fixed degree over $\mathbb{Q}$. Then, as $|d(K)| \to \infty$, we have*

$$\log(h(K) \cdot R(K)) \sim \log \sqrt{|d(K)|}\ , \tag{3.1}$$

*where $h(K), R(K)$ and $d(K)$ are the class number, regulator and discriminant of the number field $K$ respectively.*

R. Brauer proved the above theorem by bounding left hand side (the residue of the Dedekind zeta function of $k$ at $s = 1$) of the class number formula. It is a natural to ask whether an estimate similar to Eq. 3.1 holds in the context of elliptic curves.

## 3.1 Brauer-Siegel Analogue

We begin by defining notation, which will be used in this chapter.

**Notation**

- Let $f(x)$ and $g(x)$ be real-valued functions over $\mathbb{R}$ and let $c \in \mathbb{R}$.

  "$f(x) \sim g(x)$" denotes that $g(x) \neq 0$ for sufficiently large $x$ and $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.

  Statements of the form "for every $\epsilon > 0,\ f(x) \ll g(x)^{c+\epsilon}$" should be interpreted as "for every $\epsilon > 0$, there exists a constant $\kappa(\epsilon) > 0$ such that $|f(x)| \leq \kappa(\epsilon) \cdot g(x)^{c+\epsilon}$, where $\kappa(\epsilon)$ depends on $\epsilon$, and the inequality holds for all sufficiently large values of $x$." In the literature, "$f(x) \ll g(x)^{c+\epsilon}$," "$f(x) \ll_\epsilon g(x)^{c+\epsilon}$" and "$f(x) = O(g(x)^{c+\epsilon})$" are used synonymously.

  The notation $\gg$ has a definition analogous to $\ll$.

- Every elliptic curve $E$ is defined over $\mathbb{Q}$, $N(E)$ denotes its conductor, $\Delta(E)$ denotes the global minimal discriminant of $E$, unless otherwise specified. The naïve height of an elliptic curve $E$ is defined to be $h^*(E) = \frac{1}{12} \cdot \log \max\{|c_4(E)|^3, |c_6(E)|^2\}$, where

$c_4$ and $c_6$ are quantities associated to a global minimal Weierstrass equation for $E$. The definitions of $c_4$ and $c_6$ can be found in [Sil92, §3.1], [Cre97, §3.1].

- Statements such as "for every $\epsilon > 0$, $f(E) \ll g(E)^{c+\epsilon}$," where $f(E)$ and $g(E)$ are real-valued invariants associated to elliptic curves $E$ and $c \in \mathbb{R}$, should be interpreted as "for every $\epsilon > 0$, there exists a constant $\kappa(\epsilon) > 0$ such that $|f(E)| \leq k(\epsilon) \cdot g(E)^{c+\epsilon}$, where $\kappa(\epsilon)$ depends on $\epsilon$, and the inequality holds for all sufficiently large values of $h^*(E)$, where $E$ ranges over $\{E_i\}$, a sequence of elliptic curves." If the sequence $\{E_i\}$ is not specified it would imply that we consider all elliptic curves, otherwise the sequence will be clear from the context.

The Shafarevich-Tate group and regulator of an elliptic curve are objects analogous to the class group and regulator of a number field. Though the class number of a number field — size of the class group — is finite, the size of the Shafarevich-Tate group of an elliptic curve is only conjectured to be finite. This illustrates that analogous statements between multiplicative groups and elliptic curves do not seem to carry over immediately.

S. Lang proposed a conjectural upper bound for the product of the size of the Shafarevich-Tate group and the regulator of an elliptic curve. He arrived at this conjecture by bounding the quantities which appear in the the BSD formula [Lan83].

**Conjecture 3.1.1 (Lang)** *For all elliptic curves $E : y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$,*

$$\#Ш(E) \cdot Reg(E) \ll H(E)^{\frac{1}{12}} N(E)^{\epsilon(N(E))} c^{r_E} (\log N(E))^{r_E} \tag{3.2}$$

*where* $H(E) = \max(|a|^3, |b|^2)$*,* $r_E$ *is the Mordell-Weil rank of* $E$*,* $c$ *is some universal constant, and* $\epsilon(N(E)) \to 0$ *as* $N(E) \to \infty$*. In fact,* $\epsilon(N(E))$ *may have the explicit form*

$$\epsilon(N(E)) = d(\log N(E) \cdot \log\log N(E))^{\frac{-1}{2}},$$

*where* $d$ *is some constant.*

Hindry's Brauer-Siegel type conjecture [Hin], which follows, implies that Lang's bound is "an equality in the limit".

**Conjecture 3.1.2 (Hindry)**

$$\log(\#Ш(E) \cdot Reg(E)) \sim h^*(E) \tag{3.3}$$

In explicit terms, this conjecture asserts that

**Conjecture 3.1.3** *If* $\{E_i\}$ *is a sequence of elliptic curves such that* $\lim_{i\to\infty} h^*(E_i) = \infty$*. then*

$$\lim_{i\to\infty} \frac{\log(\#Ш(E_i) \cdot Reg(E_i))}{h^*(E_i)} = 1. \tag{3.4}$$

The rank 0 version of Conjecture 3.1.3 reads

**Conjecture 3.1.4** *If* $\{E_i\}$ *is a sequence of elliptic curves of Mordell-Weil rank* 0 *such that* $\lim_{i\to\infty} h^*(E_i) = \infty$ *then*

$$\lim_{i\to\infty} \frac{\log(\#Ш(E_i))}{h^*(E_i)} = 1. \tag{3.5}$$

We note the above conjectures and a lower bound for the regulator imply upper bounds for the size of the Shafarevich-Tate groups of elliptic curves.

**Conjecture 3.1.5** *For every $\epsilon > 0$, we have*

$$\#\text{Ш}(E) \ll H^*(E)^{1+\epsilon}, \tag{3.6}$$

*where* $H^*(E) = \exp(h^*(E)) = \max\{|c_4(E)|^{\frac{1}{4}}, |c_6(E)|^{\frac{1}{6}}\}$.

The Frey-Szpiro conjecture (equivalent to the ABC conjecture [Ste]) states

**Conjecture 3.1.6 (Frey, Szpiro)** *For every $\epsilon > 0$, there exists $c_\epsilon > 0$ such that*

$$h^*(E) < (\frac{1}{2} + \epsilon) \log N(E) + c_\epsilon. \tag{3.7}$$

Combining Conjecture 3.1.5 with Conjecture 3.1.6 leads to

**Conjecture 3.1.7 (Goldfeld, Szpiro)** *For every $\epsilon > 0$, we have*

$$\#\text{Ш}(E) = O(N(E)^{\frac{1}{2}+\epsilon}). \tag{3.8}$$

Of interest is a paper of D. Goldfeld and L. Szpiro [GS95], where they establish an equivalence between Conjecture 3.1.7 and Conjecture 3.1.8.

**Conjecture 3.1.8 (Szpiro)** *For every $\epsilon > 0$, there exists $\kappa(\epsilon) > 0$ such that*

$$|\Delta(E)| < \kappa(\epsilon) \cdot N(E)^{6+\epsilon}. \tag{3.9}$$

The Frey-Szpiro conjecture implies the Szipro conjecture due to the identity $1728 \cdot \Delta(E) = c_4(E)^3 - c_6(E)^2$.

We proceed to present a result of B.M.M. de Weger [dW98], where conjectures involving $\#Ш(E)$ are formulated, but first we state a conjecture which will be needed (see [GS95]).

**Conjecture 3.1.9** *The Riemann hypothesis holds for the Ranking-Selberg zeta function associated to the weight $\frac{3}{2}$ modular form associated to an elliptic curve by the Shintani-Shimura lift.*

**Lemma 3.1.1 (de Weger)** *For every $\epsilon > 0$, there exist infinitely many elliptic curves with*

$$\begin{aligned} \#Ш(E) &\gg |\Delta(E)|^{\frac{1}{12}-\epsilon} \textit{ and} && (3.10) \\ \#Ш(E) &\gg N(E)^{\frac{1}{2}-\epsilon}. && (3.11) \end{aligned}$$

*Eq. 3.10 requires assuming the BSD conjectural formula in the rank* 0 *case. Eq. 3.11 requires assuming Szpiro's conjecture (Conjecture 3.1.8) and Conjecture 3.1.9 in addition to the BSD conjectural formula in the rank* 0 *case.*

The proof of the lemma is constructive and produces a sequence of Frey-Hellegouarch elliptic curves whose coefficients are related via the $ABC$-conjecture and whose Shafarevich-Tate groups are lower bounded as above.

Observe that Eq. 3.11 (together with Szpiro's conjecture) would imply Eq. 3.10 but de Weger's proof requires merely assuming the BSD conjectural formula in the rank 0 case. Also Eq. 3.10 would imply Eq. 3.11 with the exponent $\frac{1}{2}-\epsilon$ replaced by $\frac{1}{6}-\epsilon$, since the Frey-Hellegouarch curves satisfy $\Delta(E) >> N(E)^2$.

In §3.4 we prove the main result of this chapter, which is a refinement of Lemma 3.1.1:

**Lemma 3.1.2** *For every $\epsilon > 0$, there are infinitely many elliptic curves $E$ such that*

$$\begin{aligned} \#Ш(E) &\gg |\Delta(E)|^{\frac{1}{2}-\epsilon} \text{ and} \qquad (3.12) \\ \#Ш(E) &\gg N(E)^{\frac{1}{2}-\epsilon} \qquad (3.13) \end{aligned}$$

*assuming that the BSD conjectural formula in the rank 0 case and Conjecture 3.1.9 are true.*

It suffices that the assumptions in these lemmas hold for the constructed sequence of elliptic curves. Given the advances which have been made with regards to the BSD conjecture in the rank 0 scenario, an interesting project would be to remove the BSD formula assumption from the above lemma.

Comparing Lemmas 3.1.1 and 3.1.2, we see that the exponent in the lower bound in terms of the discriminants is improved from $\frac{1}{12}-\epsilon$ to $\frac{1}{2}-\epsilon$, but with the additional assumption of Conjecture 3.1.9, and the lower bound in terms of the conductors is established without assuming Szpiro's Conjecture.

It is interesting to note that though the assumption of Conjecture 3.1.9 plays a crucial role in the proof of Eq. 3.12, it does not play a role in the proof of Eq. 3.10. We wonder if Eq. 3.12 could be established without this assumption.

Keeping in mind the lower bound satisfied by the Shafarevich-Tate groups of the elliptic curves in Eq. 3.12 and the conjectural upper bound for Shafarevich-Tate groups of elliptic curves (Eq. 3.8), it follows that the conductor of each of these elliptic curves is "quite close" to its discriminant. This implies that the models of the aforementioned elliptic curves are close to being global minimal models, a fact which is not apparent from their construction.

We note that these conditional results involving $\#Ш(E)$ in the above discussion are consistent with the Brauer-Siegel analogue conjectures introduced earlier.

## 3.2 Conditional proof of the Brauer-Siegel Analogue

The goal of this section is to present bounds (some of which are conjectural) for the terms appearing in the BSD formula. Hindry proved that these bounds would imply a Brauer-Siegel analogue for elliptic curves (Conjecture 3.1.2) and we sketch his proof in this section. The contents of this section will also lay the foundation for proving results in section 3.4.

Recall that the the BSD conjectural formula (Eq. 1.6) states that

$$\#Ш(E) \cdot Reg(E) = L_E^*(1) \cdot \frac{\#E(\mathbb{Q})^2}{\Omega(E) \cdot \prod_p c_p(E)}, \tag{3.14}$$

where $L_E^*(1)$ is the leading coefficient of the Taylor expansion of the $L$-series of $E$ at $s = 1$.

Mazur's torsion classification theorem lists 15 groups which occur as the elliptic curve torsion group and asserts that

$$1 \leq \#E(\mathbb{Q}) \leq 16. \tag{3.15}$$

The Tamagawa number $c_p$ of an elliptic curve at a prime $p$ lies in the following interval [Sil92, Corollary 15.2.1]

$$c_p \in [1, \max\{4, \log_p(|\Delta(E)|)\}], \tag{3.16}$$

and the product of $c_p$ over all the primes $p$ is bounded as follows [dW98]

$$1 \leq \prod_p c_p \ll |\Delta(E)|^{\left(\frac{m}{\log\log|\Delta(E)|}\right)} = O(\Delta(E)^\epsilon), \tag{3.17}$$

where $m$ is some constant [dW98, Theorem 3].

The real period of an elliptic curve $E$ is bounded [Hin] as follows:

$$H(E) \ll \Omega(E)^{-1} \ll H(E)^{1+\epsilon} \tag{3.18}$$

where $H(E)$ is the exponential of $h(E)$, the height of $E$, a quantity which will not be defined in this dissertation. For the purpose of analysis, $h(E)$ can usually be replaced by $h^*(E)$, the naïve height of $E$, due to the following fact (see the discussion after Eq. 3.13 in [Hin])

**Lemma 3.2.1** *For any $\epsilon > 0$, there exists $\kappa(\epsilon)$ such that*

$$h(E) + O(1) \leq h^*(E) \leq (1+\epsilon) \cdot h(E) + \kappa(\epsilon). \tag{3.19}$$

The leading coefficient $L^*_E(1)$ is conjecturally bounded as follows [Hin]. Hindry conjectures that a lower bound similar to the one for the residue of the Dedekind zeta function of a number field would also hold true for $L_E^*(1)$ (noting that “there is less evdidence” for such a conjecture). On the other hand, it is claimed that the upper bound is implied by assuming the generalized Riemann Hypothesis.

$$N(E)^{-\epsilon} \ll |L_E^*(1)| \ll N(E)^{\epsilon} \tag{3.20}$$

Combining the above bounds we have, for every $\epsilon > 0$

$$(1-\epsilon)\cdot h^*(E) \leq \log(\#\text{Ш}(E)\cdot \mathit{Reg}(E)) \leq (1+\epsilon)\cdot h^*(E) \tag{3.21}$$

and this finishes Hindry’s conditional proof of Conjecture 3.1.2.

## 3.3 A natural question

A natural question motivated by the above conjectures — due to W. A. Stein — reads: *Are there infinitely many elliptic curves of Mordell-Weil rank* 0 *and trivial Shafarevich-Tate group?* More formally,

**Question 3.3.1** *Does there exist a sequence $\{E_i\}$ of elliptic curves, such that*

$$\lim_{i\to\infty} h^*(E_i) = \infty,\ r_{E_i} = 0 \textit{ and } \#\text{Ш}(E_i) = 1? \tag{3.22}$$

Heuristics obtained by studying the Shafarevich-Tate group from the perspective of Cohen-Lenstra type analysis for class groups [Del01] and from random matrix theory (personal communication with M. Watkins) suggest that the set of rank 0 elliptic curves with trivial Shafarevich-Tate group is a density 0 set. If the set is finite in size, then that will be consistent with the above conjectures. On the other hand, if the set is infinite, then that will imply that the Brauer-Siegel type conjectures do not hold due to the existence of a counterexample to Conjecture 3.1.2.

In the context of multiplicative groups, the analogues of elliptic curves with rank 0 Mordell-Weil group and trivial Shafarevich-Tate group are imaginary quadratic fields (as their unit groups are rank 0) with trivial class group. The analogue of Question 3.3.1 reads: *Are there infinitely many imaginary quadratic fields with class number* 1*?* (Given $n$, the determination of the list of discriminants of imaginary quadratic fields with $n$ as their class number is called the Class Number problem.) It is a fact that there are only finitely such fields $\mathbb{Q}(\sqrt{d})$, where the discriminants $d$ are from the list $-3, -4, -7, -8, -11, -19, -43, -67, -163$ [Coh93, §5.3]. If such a phenomenon holds in the elliptic curve scenario, there would exist only finitely many rank 0 elliptic curves with trivial Shafarevich-Tate group. In other words, there would exist a bound such that elliptic curves with discriminant greater than this bound would either have positive Mordell-Weil rank or nontrivial Shafarevich-Tate group.

Suppose Question 3.3.1 is true, then this would imply that the conjectural bounds for $L_E^*(1)$ are incorrect (Eq. 3.20).

## 3.4 Big Ш's

At first glance one might expect the global minimal discriminant of an elliptic curve to play the role of the discriminant of a number field in a Brauer-Siegel type formula for elliptic curves. The following conjectural inequality, which states that the ratio of the naïve height of an elliptic curve to its minimal discriminant is not a constant but varies in a certain interval, lends support to the assertion that a Brauer-Siegel type statement for elliptic curves as conjectured by Hindry (Conjecture 3.1.2) would not hold if the naïve height is replaced by the logarithm of the discriminant or conductor of an elliptic curve.

$$\frac{1}{12} \leq \frac{h^*(E)}{\log|\Delta(E)|} \leq \frac{1}{2} + \epsilon. \tag{3.23}$$

The first inequality follows from the definitions and the second inequality is a consequence of the Frey-Szpiro conjecture. We would like to thank M. Hindry for bringing these inequalities to our attention and for illustrating to us that the upper bound in Eq. 3.23 is met using a theorem of L.V. Danilov. We use this fact to prove Lemma 3.1.2.

A crucial ingredient in the proof of the lemma is Danilov's paper [Dan82], where he constructs infinitely many integers $a_k, b_k$ such that as $k \to \infty$, $|a_k|, |b_k| \to \infty$ and which satisfy

$$\left|a_k^3 - b_k^2\right| \sim c\,|a_k|^{\frac{1}{2}}, \tag{3.24}$$

where $c = \frac{54\sqrt{5}}{125} = 0.965\ldots$. He uses these integers to prove the following theorem, thereby confirming a conjecture of M. Hall (see [Dan82] for the details).

**Theorem 3.4.1 (Danilov)** *For infinitely many integers $x, y$,*

$$0 < \left|x^3 - y^2\right| < 0.97\,|x|^{\frac{1}{2}}. \tag{3.25}$$

As the pairs $(a_k, b_k)$ satisfy Eq. 3.25, we have

$$|a_k|^3 \leq \max\{|a_k|^3, |b_k|^2\} < |a_k|^3 + 0.97\,|a_k|^{\frac{1}{2}}\,. \tag{3.26}$$

Let us consider the sequence of elliptic curves $E_k : y^2 = x^3 - 27a_k - 54b_k$. The discriminant and $c$-invariants of $E_k$ are: $\Delta(E_k) = 2^6 \cdot 3^9(a_k^3 - b_k^2)$, and $c_4(E_k) = 6^4 a_k$, $c_6(E_k) = 6^6 b_k$. We do not take $(a_k, b_k)$ as the $c$-invariants of $E_k$, since it is not clear if these pairs of integers satisfy Kraus' conditions [Cre97, Proposition 3.1.1.], in other words, whether there exist elliptic curves $E_k$ with these $c$-invariants for all $k$.

Note that $\Delta(E_k)$ denotes the discriminant for the above model of $E_k$ and not necessarily the global minimal discriminant. It is not clear to us if $(a_k, b_k)$ can be chosen such that the discriminants are minimal.

By change of the variables, Eq. 3.26 reads

$$|c_4(E_k)|^3 \leq \max\{|c_4(E_k)|^3, |c_6(E_k)|^2\} < |c_4(E_k)|^3 + 0.97 \cdot 6^{10}\,|c_4(E_k)|^{\frac{1}{2}}\,. \tag{3.27}$$

The term $|c_4(E_k)|^3$ dominates over $|c_4(E_k)|^{\frac{1}{2}}$ for sufficiently large $k$, and hence

$$\max\{|c_4(E_k)|^3, |c_6(E_k)|^2\} \sim |c_4(E_k)|^3\,, \text{ as } k \to \infty. \tag{3.28}$$

Utilizing Eq. 3.24 and the relations satisfied by $\Delta(E_k)$ and $c_4(E_k)$ in terms of $a_k, b_k$, we get

$$c \cdot 2^4 \cdot 3^7 \cdot |c_4(E_k)|^{\frac{1}{2}} \sim |\Delta(E_k)|\,, \text{ as } k \to \infty. \tag{3.29}$$

Combining Eq. 3.28 and Eq. 3.29 we have illustrated that as $k \to \infty$,

$$h^*(E_k) = \frac{1}{12} \log \max\{|c_4(E_k)|^3, |c_6(E_k)|^2\} \sim \frac{1}{2} \log |\Delta(E_k)|. \tag{3.30}$$

We record a lemma which is a consequence of this asymptotic growth of the naïve height of elliptic curves $\{E_k\}$ and the BSD conjectural formula.

**Lemma 3.4.1** *Assuming the BSD formula, the elliptic curve sequence $\{E_k\}$ constructed using Theorem 3.4.1 satisfies*

$$\log\left(\frac{\#Ш(E_k) \cdot Reg(E_k)}{L^*_{E_k}(1)}\right) \geq \left(\frac{1}{2} - \frac{m}{\log\log|\Delta(E_k)|}\right) \cdot \log|\Delta(E_k)| \tag{3.31}$$

*for sufficiently large $k$, where $m$ is the constant used in bounding the product of the Tamagawa numbers (Eq. 3.17).*

The purpose of the remainder of this section is to use the aforementioned sequence of elliptic curves $\{E_k\}$ and construct another sequence $\{E'_k\}$ to prove the following lemma, which would in turn imply Lemma 3.1.2.

**Lemma 3.4.2** *Let $m$ be the constant used in bounding the product of the Tamagawa numbers (Eq. 3.17). Assuming Conjecture 3.1.9, there exists a sequence of elliptic curves $\{E'_k\}$ such that for sufficiently large $k$*

$$h^*(E'_k) < \frac{1}{2} \log \left|\Delta(E'_k)\right| \tag{3.32}$$

$$h^*(E'_k) \geq \left(\frac{1}{2} - \frac{m}{\log\log\left|\Delta(E'_k)\right|}\right) \cdot \log\left|\Delta(E'_k)\right|. \tag{3.33}$$

*In addition, assuming the rank* 0 *case of the BSD conjectural formula, we have*

$$\log \#Ш(E'_k) \quad \geq \quad (\frac{1}{2} - \frac{m}{\log\log\left|\Delta(E'_k)\right|}) \cdot \log\left|\Delta(E'_k)\right| \tag{3.34}$$

*for sufficiently large* $k$*.*

The proof will be driven by techniques similar to the ones de Weger used in establishing Lemma 3.1.1.

In what follows the elliptic curve $E_{k,q}$ will denote the quadratic twist of $E_k$ by $q$, where $q$ will depend on $k$ and more precisely on the elliptic curve $E_k$ (we do not use subscripts to enhance readability). Twisting by $q$ introduces a factor of a power of $q$ to the discriminant and the c-invariants, namely, $\Delta(E_{k,q}) = q^6 \cdot \Delta(E_k),\ c_4(E_{k,q}) = q^2 \cdot c_4(E_k)$ and $c_6(E_{k,q}) = q^3 \cdot c_6(E_k)$.

Multiplying the inequalities in Eq. 3.27 by $q^6$ and switching to notation in terms of $E_{k,q}$ we get

$$|c_4(E_{k,q})|^3 \leq \max\{|c_4(E_{k,q})|^3, |c_6(E_{k,q})|^2\} < |c_4(E_{k,q})|^3 + 0.97 \cdot 6^{10} q^5 \, |c_4(E_{k,q})|^{\frac{1}{2}} \, . \tag{3.35}$$

Let us start with Eq. 3.24 which $(a_k, b_k)$ obey, namely for each $\delta > 0$,

$$1 - \delta < \frac{a_k^3 - b_k^2}{c\,|a_k|^{\frac{1}{2}}} < 1 + \delta \tag{3.36}$$

for sufficiently large $k$. Multiplying the numerator and denominator of the fraction by $q^6$, translating to notation in terms of $E_{k,q}$, taking sixth powers and retaining the same notation for $\delta$ we get, for each $\delta > 0$,

$$1 - \delta < \frac{|\Delta(E_{k,q})|^6}{c' \cdot q^{30} \, |c_4(E_{k,q})|^3} < 1 + \delta \tag{3.37}$$

for sufficiently large $k$ and where $c' = c^6 \cdot 2^{24} \cdot 3^{42}$.

Assuming Conjecture 3.1.9 holds for each $E_k$, it is known that for every $\epsilon > 0$, there exists $q < N(E_k)^\epsilon$ such that $L(E_{k,q}, 1) \gg 1$ for sufficiently large $k$ (consult [dW98] for details). As $L(E_{k,q}, 1)$ is bounded away from 0, $E_{k,q}$ has Mordell-Weil rank 0 by the work of V.A. Kolyvagin's work on the BSD conjecture [Kol90].

Applying the inequality $q < N(E_k)^\epsilon$ to the right of Eq. 3.35 we have, for every $\epsilon > 0$,

$$\max\{|c_4(E_{k,q})|^3, |c_6(E_{k,q})|^2\} < |c_4(E_{k,q})|^3 + 0.97 \cdot 6^{10} N(E_k)^{5\epsilon} \, |c_4(E_{k,q})|^{\frac{1}{2}} \tag{3.38}$$

for sufficiently large $k$, and noting that $1 \leq q$ for each elliptic curve, we have, for every $\delta > 0$,

$$1 - \delta < \frac{|\Delta(E_{k,q})|^6}{c' \, |c_4(E_{k,q})|^3} \tag{3.39}$$

for sufficiently large $k$.

Combining Eq.3.40 and Eq. 3.39 proves that, for every $\epsilon > 0$ and every $\delta > 0$

$$\max\{|c_4(E_{k,q})|^3, |c_6(E_{k,q})|^2\} < \frac{|\Delta(E_{k,q})|^6}{c'(1-\delta)} + 0.97 \cdot 2^6 \cdot 3^3 N(E_k)^{5\epsilon} \frac{|\Delta(E_{k,q})|}{c(1-\delta)} \tag{3.40}$$

for sufficiently large $k$.

Using the defintion of the naïve height of an elliptic curve, we have illustrated, for each $\epsilon > 0$ and every $\delta > 0$,

$$h^*(E_{k,q}) < \frac{1}{2}\log|\Delta(E_{k,q})| - \frac{1}{12}\log(c'(1-\delta)) + \frac{1}{12}\log(1 + c''\frac{N(E_k)^{5\epsilon}}{|\Delta(E_{k,q})|^5}) \tag{3.41}$$

for sufficiently large $k$, where $c'' = 0.97 \cdot 2^6 \cdot 3^3$. This proves Eq. 3.32.

On the other hand, applying the inequality $q < N(E_k)^\epsilon$ to the inequality on the right of Eq. 3.37 we have, for each $\epsilon > 0$ and for each $\delta > 0$,

$$\frac{|\Delta(E_{k,q})|^6}{c' \cdot N(E_k)^{30\epsilon}\,|c_4(E_{k,q})|^3} < 1 + \delta \tag{3.42}$$

for sufficiently large $k$.

The combination of the inequality on the left of Eq. 3.35 with Eq. 3.42 results in: for each $\epsilon > 0$ and for each $\delta > 0$,

$$\max\{|c_4(E_{k,q})|^3, |c_6(E_{k,q})|^2\} > c'^{-1} \cdot |\Delta(E_{k,q})|^6 \cdot N(E_k)^{-30\epsilon} \cdot (1+\delta)^{-1} \tag{3.43}$$

for sufficiently large $k$. By the defintion of the naïve height of an elliptic curve and the fact that $|\Delta(E_{k,q})| \geq N(E_k)$, we obtain, for each $\epsilon > 0$ and for each $\delta > 0$,

$$h^*(E_{k,q}) > (\frac{1}{2} - \frac{5\epsilon}{2})\log|\Delta(E_{k,q})| - \frac{1}{12}\log(c' \cdot (1+\delta)) \tag{3.44}$$

for sufficiently large $k$, where $c' = c^6 \cdot 2^{24} \cdot 3^{42}$. This proves Eq. 3.33.

Denote by $E_k'$ the rank 0 quadratic twist of $E_k$ by $q$ such that $L(E_{k,q}, 1) \gg 1$. Under the BSD conjectural formula (rank 0 case), we have proved that

$$\log \#\text{Ш}(E_k') > (\frac{1}{2} - \frac{5\epsilon}{2} - \frac{m}{\log\log\left|\Delta(E_k')\right|}) \cdot \log\left|\Delta(E_k')\right| \tag{3.45}$$

for sufficiently large $k$, where $m$ is the constant used in bounding the product of the Tamagawa numbers (Eq. 3.17).

This finishes the proof of Lemmas 3.4.2 and 3.1.2. A question which arises in this context is whether there exist sequences of elliptic curves which could be used, in lieu of the one constructed using Danilov's theorem, to prove the aforementioned lemmas and perhaps yield easier proofs.

A final remark we would like to make is that analysis similar to above discussion can applied to a sequence of elliptic curves $\{E_i\}$ with $c_4(E_i) = 0$ for all $i$ (or $c_6(E_i) = 0$). For instance, the elliptic curves $E_p$ in Appendix C.1 fit this description. Such elliptic curves could be used to prove

$$h^*(E_i') \sim \frac{1}{12}\log\left|\Delta(E_i')\right|, \tag{3.46}$$

where $E_i'$ are rank 0 quadratic twists of $E_i$ such that $L_{E_i'}(1) \gg 1$ for sufficiently large values of $i$. This would imply that there are infinitely many elliptic curves $E'$ with

$$\#\text{Ш}(E') \gg \left|\Delta(E')\right|^{\frac{1}{12}-\epsilon}; \tag{3.47}$$

a result on the lines of de Weger's work — see Lemma 3.1.1.

# Chapter 4

## Chapter Four: Notes on certain quartic twists of an elliptic curve

*The problem of distinguishing prime numbers from composite numbers, and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic.* C. F. Gauss *in article 329 of Disquisitiones Arithmeticae (1801).*

In this chapter we investigate certain quartic twists of the elliptic curve $y^2 = x^3 - x$ and present some of their interesting properties. Specifically, we consider the family of elliptic curves $E_D : y^2 = x^3 - Dx$, where $D = pq$ with $p$ and $q$ distinct prime numbers, $p \equiv q \equiv 3 \bmod 16$. These elliptic curves have complex multiplication by $\mathbb{Q}(i)$. The 2-torsion point $(0, 0)$ generates the torsion subgroup of the Mordell-Weil group $E_D(\mathbb{Q})$. Employing the method of two-descent, we show that under the Birch and Swinnerton-Dyer conjecture, the Mordell-Weil rank of $E_D$ is one.

Let $E'_D$ denote $y^2 = x^3 + 4Dx$ the isogenous curve of $E_D$, and $C'_d$ represent the homogeneous spaces $dW^2 = d^2 - DZ^4$ of $E'_D$.

We argue that any point $R$ of the Mordell-Weil group $E_D(\mathbb{Q})$ which is not in $\langle(0,0)\rangle + 2E_D(\mathbb{Q})$ must behave differently with respect to $p$-adic and $q$-adic valuations. This sets the stage for reductions between the problem of factoring integers of the form $D$ and the problem of computing non-torsion rational points on $E_D$.

In one direction, we prove that if there exists a rational point of the above form such that its naïve height is polynomial in the naïve height of the elliptic curve $h^*(E_D)$, then factoring $D$ is polynomial time reducible to computing a non-torsion rational point of $E_D$.

In the other direction, we show that if either of the homogeneous spaces $C'_p$ or $C'_{-q}$ of $E'_D$ has a rational point whose naïve height is bounded by a polynomial in $\log h^*(E_D)$, then computing a non-torsion rational point of $E_D$ is polynomial time reducible to factoring $D$.

The chapter ends with a discussion about Heegner point computation restricted to these elliptic curves $E_D$. We observe the dependence of the Heegner index on $\#Ш(E_D)$. Assuming that the Shafarevich-Tate groups tend to get "big" (for instance by the Brauer-Siegel Analogue — Conjecture 3.1.2), it follows that factoring numbers of the form $D$ by computing a point in $E_D(\mathbb{Q})$ via the Heegner point method would be computationally expensive.

## 4.1 Analysis of $E_D$

In this section we will study a particular class of elliptic curves parameterized by primes $p$ and $q$ and obtain the structure of their Mordell-Weil groups subject to congruence conditions. The analysis in this section closely follows §$X$.6 from J.H. Silverman's book, which in turn exploits Proposition $X$.4.9 (Descent via Two-isogeny) from the same book [Sil92]. The reader eager to learn about the reduction mentioned in the chapter's introduction can skip this section.

Let $E_D$ over $\mathbb{Q}$ be the elliptic curve

$$E_D : y^2 = x^3 - Dx.$$

where $D \in \mathbb{Z}$ (the subscript $D$ will be dropped when it is clear from the context). Then $E_D$ is isogenous to the elliptic curve

$$E'_D : Y^2 = X^3 + 4DX$$

via the isogeny $\phi : E_D \to E'_D, (x, y) \mapsto (y^2/x^2, -y(D + x^2)/x^2)$ and let $\hat{\phi} : E'_D \to E_D$ be the dual isogeny of $\phi$.

We will consider the curves $E_{pq} : y^2 = x^3 - pqx$, where $p$ and $q$ are odd and distinct primes and perform descent via $\phi$, which is an isogeny of degree 2.

Let $M_{\mathbb{Q}}$ be the set of primes of $\mathbb{Z}$ and $\infty$ (that is, a complete set of inequivalent absolute values on $\mathbb{Q}$). Let $S = \{\infty, 2, p, q\} \subset M_{\mathbb{Q}}$ and $\mathbb{Q}_\nu$ denote the completion of $\mathbb{Q}$

with respect to the absolute value associated to $\nu \in S$. In particular, $\mathbb{Q}_\infty$ denotes $\mathbb{R}$ and for $\nu \in S \setminus \{\infty\}$ and $\mathbb{Q}_\nu$ denotes the $\nu$-adic numbers. Let

$$\mathbb{Q}(S,2) := \{b \in \mathbb{Q}^*/\mathbb{Q}^{*2} \mid \nu(b) \equiv 0 \bmod 2 \ \text{ for all } \ \nu \notin S\}.$$

We take the following representatives for the cosets in $\mathbb{Q}(S,2)$:

$$\{\pm 1, \pm 2, \pm p, \pm 2p, \pm q, \pm 2q, \pm pq, \pm 2pq\}.$$

Let $WC(E)$ denote the Weil-Châtelet group of $E$, the group of equivalence classes of homogeneous spaces for $E$ over $\mathbb{Q}$. For each $d \in \mathbb{Q}(S,2)$, the corresponding homogeneous spaces $C_d \in WC(E)$ and $C'_d \in WC(E')$, also referred to as quartics, are given by the equations

$$\begin{aligned} C_d &: \ dw^2 = d^2 + 4pqz^4, \\ C'_d &: \ dW^2 = d^2 - pqZ^4. \end{aligned}$$

The $\phi$-Selmer group can be viewed as a subset of $\mathbb{Q}(S,2)$ as follows:

$$S^{(\phi)}(E) \cong \{d \in \mathbb{Q}(S,2) : C_d(\mathbb{Q}_\nu) \neq \emptyset \ \text{ for all } \ \nu \in S\}.$$

The $\hat{\phi}$-Selmer group $S^{(\hat{\phi})}(E')$ has an analogous isomorphism where $C_d$ is replaced by $C'_d$.

The images of $(0,0)$, the 2-torsion point of $E'(\mathbb{Q})$ and $E(\mathbb{Q})$ in the Selmer groups are given by

$$pq \in S^{(\phi)}(E) \text{ and } -pq \in S^{(\hat{\phi})}(E') \tag{4.1}$$

respectively.

### 4.1.1 Descent via two-isogeny

We restrict our attention to elliptic curves

$$E = E_D : y^2 = x^3 - Dx \tag{4.2}$$

where $D = pq$, $p$ and $q$ are distinct primes such that $p \equiv q \equiv 3 \bmod 16$ and $(\frac{p}{q}) = (\frac{-q}{p}) = 1$.

In this subsection we perform descent on the 2-isogenous elliptic curves $E$ and $E'$. We would like to thank an anonymous referee for providing us with the following elegant argument. Our original analysis can be found in Appendix B.

When $K = \mathbb{Q}$ or $\mathbb{Q}_\nu$, we have the exact sequence

$$0 \to E'[\hat{\phi}] \to E' \to E \xrightarrow{f} K^*/K^{*\,2}, \tag{4.3}$$

with $f$ induced by $P \mapsto x(P)$ for the models above. When $K = \mathbb{Q}_\nu$, we write $S^{(\hat{\phi})}(K)$ for the actual image of $f$. Let the group $S^{(\hat{\phi})}(\mathbb{Q})$ be obtained by globalizing the local data. It is identical to the Selmer group $S^{(\hat{\phi})}(E')$ introduced in §1.4.

Suppose $P \in E(\mathbb{Q}_\nu)$, $\nu$ being equal to 2 or a place of good reduction then $2|\nu(x(P))$ and we find that $f(P) \in \mathbb{Z}_\nu^*$.

For $\nu = p$ or $\nu = q$, $E$ has bad, type III reduction and $[E : E_0] = 2$ [Sil92, Table 15.1]. The group $E(\mathbb{Q}_\nu)$ is generated by $E_0(\mathbb{Q}_\nu)$ and the point $T = (0, 0)$. Since both $E_1(\mathbb{Q}_\nu) \cong \mathbb{Z}_\nu$ and $E_0(\mathbb{Q}_\nu)/E_1(\mathbb{Q}_\nu) \cong \overline{E}_{ns}(\mathbb{F}_\nu) \cong \mathbb{F}_v$ (the last ismorphism due to the type of reduction being additive) are divisible by 2, so is the group $E_0(\mathbb{Q}_\nu)$. It follows that $S^{(\hat{\phi})}(\mathbb{Q}_\nu) = \langle -pq \rangle$. We recall that it is assumed that $p \equiv q \equiv 3 \bmod 16$, labeled so that $(p/q) = (-q/p) = 1$. Since $p$ and $-q$ are squares modulo $q$ and modulo $p$ respectively, we have illustrated that $S^{(\hat{\phi})}(\mathbb{Q}_p) = \langle p \rangle$ and $S^{(\hat{\phi})}(\mathbb{Q}_q) = \langle -q \rangle$.

For $d \in \mathbb{Q}(S, 2)$ to be an element of $S^{(\hat{\phi})}(\mathbb{Q})$, it must necessarily correspond to a unit in $S^{(\hat{\phi})}(\mathbb{Q}_v)$ when $\nu$ is 2 and when $\nu$ is a place of good reduction, and when $\nu$ is $p$ and $q$, $d$ must map to an element of $S^{(\hat{\phi})}(\mathbb{Q}_v)$. In this fashion based on local conditions, we can eliminate the elements of $\mathbb{Q}(S, 2)$ which cannot occur as elements of $S^{(\hat{\phi})}(\mathbb{Q})$. It follows that the Selmer group is $\langle p, -q \rangle$.

Next, we consider the group $S^{(\phi)}(\mathbb{Q})$. If $P \in E'(\mathbb{R})$ then $x(P) \geq 0$. This fact coupled with reasoning similar to the preceding paragraphs show that $S^{(\phi)}(\mathbb{Q}) = \langle pq \rangle$.

When the rank of $E(\mathbb{Q})$ is 1, it follows that the points on $E(\mathbb{Q})$ map onto $S^{(\hat{\phi})}(\mathbb{Q})$. Therefore we find that for any point $R$ in $E(\mathbb{Q})$ but not in $E[\phi] + 2E(\mathbb{Q})$, $\nu_p(x(R))$ and $\nu_q(x(R))$ have opposite parity.

### 4.1.2 $E_D$ is conjecturally rank 1

The purpose of this subsection is to conditionally prove that the elliptic curves $E_D$ have Mordell-Weil rank 1. Driven by techniques used in proving Proposition X.6.2(c) [Sil92], we obtain

$$\begin{aligned} r_E + \dim_2 Ш(E'/\mathbb{Q})[\hat{\phi}] &= \dim_2 S^{(\phi)}(E) + \dim_2 S^{(\hat{\phi})}(E') - 2 \\ &= 1. \end{aligned}$$

where $\dim_2$ is the dimension as a $\mathbb{Z}/2\mathbb{Z}$-vector space. In particular, $r_E \leq 1$.

Next, we will investigate the zeros of the $L$-series of $E$ at $s = 1$. For the curves of interest the global root number $w(E)$ can be computed from the formulae in [BS66] and it equals -1. Evaluating the functional equation of $\Lambda_E(s)$ at $s = 1$ (Eq. 1.3), we have $\Lambda_E(1) = -\Lambda_E(1)$ and hence $\Lambda_E(1) = 0$. This implies that $L_E(1) = 0$, in other words, $r_E^{an} > 0$.

If $r_E^{an} = 1$, that is, $L_E^{(1)}(1) \neq 0$, then $r_E = 1$, by a result of V.A. Kolyvagin [Kol90]. The lemma below records our result.

**Lemma 4.1.1** *Let $E$ be an elliptic curve as defined in Eq. 4.2. Assuming $r_E^{an} = 1$ (or alternatively the BSD conjecture), $r_E = 1$.*

## 4.2 The reduction

**Definition 4.2.1** *Let $E$ be an elliptic curve over $\mathbb{Q}$, $P \in E(\mathbb{Q})$ and $x(P) = \frac{a}{b}$, we define the naïve height of $P$ to be $h_x(P) = \log \max\{|a|, |b|\}$.*

**Definition 4.2.2** *Let $E$ be an elliptic curve over $\mathbb{Q}$ and define the naïve height of the elliptic curve to be*

$$h^*(E) = \frac{1}{12} \log \max\{|c_4(E)|^3, |c_6(E)|^2\}$$

*where $c_4(E)$ and $c_6(E)$ are the c-invariants associated to a minimal model of $E$.*

**Definition 4.2.3** *Let $f \in \mathbb{Z}[X]$.*

$SE^f := \{E/\mathbb{Q} \mid$ *there exists a non-torsion point* $T \in E(\mathbb{Q})$ *with* $\lceil h_x(T) \rceil \leq f(h^*(E))\}$.

In other words, $SE^f$ is the set of elliptic curves which have a non-torsion rational point whose bit length is bounded by a polynomial $f$ in the bit length of the respective elliptic curve.

Let the problem of factoring integers of the form $D$ (as defined in Eq. 4.2) be denoted by $IF_D$. Let the problem of computing a non-torsion rational point of $E_D$ be denoted by $CRPSE_D$. We note that $h^*(E_D) = \log(2^4 \cdot 3 \cdot D) = O(\log D)$.

Let us recapitulate the results of the previous section: $E_D$ has conjectural rank 1 and the $x$-coordinate of a generator of $E_D(\mathbb{Q})$ has different valuations with respect to $p$ and $q$.

**Definition 4.2.4** *Let $f \in \mathbb{Z}[X]$. $SED^f := \{E_D/\mathbb{Q} \mid E_D \in SE^f\}$.*

The set $SED^f$ being infinite in size, follows from conjectural evidence which is presented toward the end of this section — Remark 4.2.1.

Fixing $f$ a polynomial with integral coefficients, let the problem of factoring integers of the form $D$ such that the associated elliptic curve $E_D \in SED^f$ be denoted by $IF_D^f$ and the problem of computing a non-torsion rational point of $E_D \in SED^f$ be denoted by $CRPSE_D^f$. We are ready to prove the following result:

**Theorem 4.2.1** *Fixing $f \in \mathbb{Z}[X]$, $IF_D^f \leq_P CRPSE_D^f$.*

**Proof 4.2.1** *Given $f, D$, a blackbox algorithm for $CRPSE_D^f$ can be used to compute $P$, a non-torsion rational point on $E_D$. A point $R \in E_D(\mathbb{Q}) \setminus (E_D[\phi] + 2E_D(\mathbb{Q}))$ can be constructed by "halving" $P$ using the duplication formula [Sil92, Algorithm 2.3 (d)]. Since $v_p(x(R)) \neq v_q(x(R))$, $p$ and $q$ can be recovered. Moreover, since $h_x(R)$ is a polynomial in $h^*(E_D)$, it follows that this is a polynomial time reduction.*

We remark that one of the procedures to compute a rational point of $E_D$ is to search for a rational point on the homogeneous spaces: $C'_p : W^2 = p - qZ^4$, $C'_{-q} : -W^2 = q - pZ^4$ (assuming $(\frac{p}{q}) = 1$) and this gives us a rational point of $E_D$ via the map $\psi : C'_d \to E$, $\psi(Z, W) = (d/Z^2, dW/Z^3)$. But to write down the equation of the homogeneous space requires knowledge of a factor of $D$.

This observation prompts us to ask whether factoring is sufficient to be able compute a non-torsion rational point on $E_D$. In order for the reduction in the reverse direction to be polynomial time, we require that the heights of rational points on the associated homogeneous spaces be appropriately bounded.

**Definition 4.2.5** *Let $g \in \mathbb{Z}[X]$. $HED^g := \{E_D/\mathbb{Q} \mid \lceil h_Z(U_D) \rceil \leq g(\log h^*(E_D))\}$, where $U_D$ denotes a rational point $(Z, W)$ on $C'_p$ or $C'_{-q}$ with the smallest naïve $Z$-height.*

Let the problem of computing a non-torsion rational point for the elliptic curves in $HED^g$ be denoted by $CRPHE^g_D$.

**Theorem 4.2.2** *Fixing $g \in \mathbb{Z}[X], CRPHE^g_D \leq_P IF_D$.*

**Proof 4.2.2** *Given a particular elliptic curve $E_D \in HED^g$, a blackbox algorithm for $IF_D$ can be used to factor $D$ and equations of the homogeneous spaces $C'_p$ and $C'_{-q}$ can be determined. Since a rational point $(Z, W)$ on one of these homogeneous spaces has height which is a polynomial in $\log h^*(E_D)$, searching naïvely and in parallel on the above quartics, the rational point can be found and using which a rational point on $E_D$ can be constructed. It follows that the reduction takes time polynomial in $h^*(E_D)$.*

**Remark 4.2.1** *Let us reconsider the quartic $C'_p : W^2 = p - qZ^4$. Suppose there are infinitely many pairs of primes $p, q$ of the type appearing in Eq. 4.2 such that $p - q$ is a square. (Observe that with these conditions $(-q, q\sqrt{p-q})$ is a rational point on $E_D$.) This would imply that there are infinitely many elliptic curves in the sets $SED^f$ and $HED^g$, for every $f$ and $g$, nonzero polynomial of degree at least 1 and nonzero polynomial respectively.*

*In the simplest case taking $q = 3$, the question boils down to* are there infinitely many primes $p$ of the form $3 + 16n^2$*? The answer is affirmative under Hardy-Littlewood's F conjecture [HL23].*

Though the above reductions are interesting, we observe that the elliptic curves $E_D$ with points of small height, which are covered by the above reductions should be viewed as the exception rather than the rule as one expects the heights of generators of the Mordell-Weil group to get "big" (for instance under the Brauer-Siegel type conjectures).

Given that $E_D$ are conjecturally rank 1 elliptic curves, can the Heegner point method be used to compute points on curves which have points of “small” height? We will seek answers to this question in the next section.

## 4.3 Heegner points computation

Suppose $E$ is an elliptic curve over $\mathbb{Q}$ with conductor $N$ and analytic rank one, then the Heegner point procedure computes a rational point on elliptic curve using the theory of complex multiplication.

An imaginary quadratic field $K$ (or its discriminant $d_K$) wherein the primes dividing $N$ split is said to satisfy the *Heegner hypothesis.* The Heegner point method constructs a point $y_K$ in $E(K)$, which turns out to be in $E(\mathbb{Q})$. The Gross-Zagier formula states that $y_K$ is a non-torsion point if and only if $r^{an}(E) = 1$ and $r^{an}(E^{d_K}) = 0$, where $E^{d_K}$ is the quadratic twist of $E$ by $d_K$. More precisely, the formula states

**Theorem 4.3.1 (Gross, Zagier)** *If* $\gcd(d_K, N) = 1$ *and* $d_K \neq -3$*, then* $y_K$ *the Heegner point computed satisfies*

$$\hat{h}(y_K) = \frac{\sqrt{|d_K|}}{4 \cdot \mathit{Vol}(E)} \cdot L'(E,1) \cdot L(E^{d_K},1), \tag{4.4}$$

*where* $\hat{h}(y_K)$ *denotes the canonical height of* $y_K$*,* $\mathit{Vol}(E)$ *is volume of the lattice* $\Lambda$ *such that* $E(\mathbb{Q}) = \mathbb{C}/\Lambda$*,* $L'(E,1)$ *and* $L(E^{d_K},1)$ *are the leading coefficients of the Taylor expansion of the L-series of* $E$ *and* $E^{d_K}$ *at* $s = 1$ *respectively.*

Table 4.1: Invariants associated to the elliptic curves $E_D$ and $E_D^{d_K}$

| $E$ | $E_D$ | $E_D^{d_K}$ |
|---|---|---|
| $\#E(\mathbb{Q})_{tors}$ | $2$ | $2$ |
| $\#\text{Ш}(E)$ | $\#\text{Ш}(E_D)$ | $\#\text{Ш}(E_D^{d_K})$ |
| $Reg(E)$ | $m^{-2}\hat{h}(y_K)$ | $1$ |
| $\Omega(E)$ | $\frac{\pi}{D^{1/4}\cdot \text{agm}(\sqrt{2},1)}$ | $\frac{\pi}{\sqrt{\lvert d_K\rvert}D^{1/4}\cdot \text{agm}(\sqrt{2},1)}$ |
| $\prod_l c_l(E)$ | $\prod_{l\mid 2\cdot D} c_l(E_D) = 2\cdot 2\cdot 2$ | $\prod_{l\mid 2\cdot D\cdot d_K} c_l(E_D^{d_K})$ |

### 4.3.1 Indexes of Heegner points on $E_D$

Let us reconsider the conjecturally Mordell-Weil rank 1 family of quartic twists of $y^2 = x^3 - x$, which were introduced in the previous sections, $E_D : y^2 = x^3 - Dx$, where $D = pq$ is a product of two distinct primes such that $p \equiv q \equiv 3 \bmod 16$.

We apply the Gross-Zagier formula (Eq. 4.4) taking $E = E_D$ and $E^{d_K} = E_D^{d_K} : y^2 = x^3 - d_K^2 Dx$. The elliptic curve $E_D^{d_K}$ denotes the quadratic twist of $E_D$ by $d_K$, which we assume to be a discriminant satisfying the Heegner hypothesis. Moreover, let us suppose that $E_D^{d_K}$ is a Mordell-Weil rank 0 elliptic curve.

Next, using the BSD formula (Eq. 1.6) for the elliptic curves $E_D$ and $E_D^{d_K}$, we replace the terms $L'(E_D, 1)$ and $L(E_D^{d_K}, 1)$ appearing in the Gross-Zagier formula. Aided by the entries of Table 4.1 we arrive at the following formula:

$$m^2 = \#\text{Ш}(E_D) \cdot \#\text{Ш}(E_D^{d_K}) \cdot \frac{1}{2} \cdot \prod_{l\mid 2\cdot D\cdot d_K} c_l(E_D^{d_K}) \tag{4.5}$$

where $m = [E_D(\mathbb{Q}) : \mathbb{Z}y_K]$ is the index of the Heegner point $y_K$ in the Mordell-Weil group. In Table 4.1 the periods of the elliptic curves $E_D, E_D^{d_K}$ were computed using the formulae listed in [Cre97, §3.7], and the Tamagawa numbers were calculated using Tate's algorithm [Cre97, §3.2]. (We also know that $Ш(E_D)[2] = 0$.)

If we assume $\gcd(d_K, 2 \cdot D) = 1$, then $c_l = 2$ for primes $l \mid 2 \cdot D$, and $c_l = 3 + (\frac{D}{l})$ for primes $l \mid d_K$. Let us consider the special case where $\gcd(d_K, 2 \cdot D) = 1$ and $|d_K|$ is a prime number. If we substitute the Tamagawa numbers into Eq. 4.5, we obtain

$$m^2 = 2^2 \cdot (3 + (\frac{D}{|d_K|})) \cdot \#Ш(E_D) \cdot \#Ш(E_D^{d_K}). \tag{4.6}$$

Both $\#Ш(E_D)$ and $\#Ш(E_D^{d_K})$ are square integers, which implies that $(\frac{D}{|d_K|}) = 1$. This constraint on the discriminant $d_K$ is interesting as it would normally be drawn out using descent analysis, but instead it is elicited by calculating the Tamagawa numbers appearing in the Gross-Zagier formula via the BSD formula.

### 4.3.2 A sketch of the time complexity analysis

Given that we are interested in factoring integers of the form $D$ by computing a rational point on $E_D$ an elliptic curve of rank 1, the Heegner point method is a candidate technique to accomplish this computation. In the discussion which follows we will examine the computational viability of this approach.

This procedure turning into a reasonable algorithm is contingent on the fact that there exists a suitable discriminant satisfying the Heegner hypothesis and the time complexity of finding one such discriminant. The former holds due to Bump, Friedberg and Hoffstein [BFH90], and Murty and Murty [MM91], who independently proved that there are infinitely many such discriminants [GJP$^+$05]. The latter would follow by performing some analysis with the aid of a result of M. Krir [Kri94, Proposition 2], which established that there exists a suitable discriminant whose absolute value is bounded by a function (essentially cubic) in the conductor of the elliptic curve. We note that this bound is much larger than what actually happens in practice since in reality such a discriminant is found in a few tries.

For an elliptic curve $E$ of rank 1 and conductor $N$, the naïve height $h$ of the computed Heegner point is $m^2 \cdot Reg(E)$ (plus a term to compensate for the difference between the naïve and canonical heights), where $m$ is the index of the Heegner point and this index depends on $E$ and the discriminant $d_K$.

Recall that the Brauer-Siegel analogue (Conjecture 3.1.2) states that for elliptic curves $E$, $\log(Reg(E) \cdot \#Ш(E))$ gets arbitrarily close to $h^*(E)$, for sufficiently large values of $h^*(E)$. This conjecture sheds light on the (worst-case) time complexity of the Heegner point method because $h$ the height of the computed point involves $Reg \cdot \#Ш$ terms for both the elliptic curve of rank 1 and its quadratic twist of rank 0.

An algorithm that computes an elliptic curve rational point in time which is polynomial in the naïve height of the point would be considered a computationally efficient algorithm. When describing the time complexity of computing elliptic curve rational points, the length of output is an alternative metric compared to the length of input because one expects the naïve height of the computed point, which measures the length of output, to be much larger than $h^*(E)$, which measures the length of input.

Shifting focus from worst-case scenarios of elliptic curves with points of "large" heights to special ones with points of "small" height (for instance $E_D : y^2 = x^3 - Dx$, where $D = pq$ and $p, q$ are distinct primes $p \equiv q \equiv 3 \bmod 16$ and $p - q$ is a square integer), it appears that the Heegner point method would not be an efficient way to compute a rational point due to the sizes of the Shafarevich-Tate groups involved — for sufficiently large values of $D$, the Brauer-Siegel analogue would predict that the $\#Ш$'s would be big. Therefore factoring integers of the form $D$ by computing a rational point via the Heegner point method would be computationally inefficient.

Investigating the internals of the Heegner point algorithm leads to another reason why factoring integers in this fashion is not a good idea. We will closely follow Cohen's presentation of the algorithm [Coh07].

A crucial step in the Heegner point method is computing the modular parameterization $\varphi : X_0(N) \to E$ of certain points on complex upper-half plane to appropriate precision and this involves calculating coefficients $a_n$ of the Fourier expansion of $f_E$ the modular form of weight 2 on $\Gamma_0(N)$ associated to the elliptic curve — $f_E(\tau) = \sum_{n\geq 1} a_n \cdot (e^{2\pi i\tau})^n$.

The height $h$, which was introduced at the beginning of this subection, dictates that all computations in this algorithm are to be performed with an accuracy of $h' = \lceil \frac{h}{\log(10)} \rceil$ decimal digits. The decimal digit accuracy $h'$ mandates that the number of terms to be considered in computing the modular parameterization $\varphi$ is at least $\frac{N \cdot h'}{\pi\sqrt{|d_K|}}$, which implies that as many Fourier coefficients are to be determined. If the number field $K$ is choosen such that the fraction $\frac{N \cdot h'}{\pi\sqrt{|d_K|}}$ is made as small as possible then the class number of $K$ might become significant (classical Brauer-Siegel theorem, Theorem 3.0.1) and play a role in the running time of this method. On the other hand, if $|d_K|$ is choosen to be small, then computing $\varphi$ might require knowledge of the first $\Omega(N)$ many Fourier coefficients of the elliptic curve. If these Fourier coefficients were computed sequentially on a prime-by-prime basis then the prime factors of the conductor of the elliptic curve ($p$

and $q$ when the elliptic curve is $E_D$) are obtained without actually performing the bulk of the Heegner point computation.

These arguments lead to the conclusion that factoring integers by computing rational points on elliptic curves of rank 1 via the Heegner point method is overkill.

A “program” born in this setting (suggested by W.A. Stein) is to investigate higher rank elliptic curves, in particular, finding an analogue of Heegner points for elliptic curves of rank greater than 1 might be relevant to integer factorization.

The question of whether it is possible to compute elliptic curve rational points of “small” height in time polynomial or subexponential in the height of the point (without explicitly factoring) is open.

# Chapter 5

# Chapter Five: Some thoughts on Parallel Computation

*By examining parallelism, we may in this way gain deeper insights into specific computational problems than is offered by sequential analyses alone.*

*L. G. Valiant [Val75]*

The recent arrival of multicore/multiprocessor CPUs on desktops warrants rethinking the design of software to leverage the presence of more than one processor even in the domain of personal computing.

I was one of the co-organizers of a workshop titled *Interactive Parallel Computation in Support of Research in Algebra, Geometry and Number Theory*, which was held at Mathematical Sciences Research Institute in Berkeley, CA from January 29 to February 2, 2007. The goal of the workshop was "to study and formulate practical parallel algorithms that support interactive mathematical research in algebra, geometry, and number theory, and to formulate strategies to encourage implementation and testing of these ideas" [BDG$^+$07].

Discussions during the workshop made it apparent that computer hardware manufacturers have turned away from single processor to multicore architecture as a means of enabling faster computers. The primary reason for this switch is that faster processors would consume more power and generate more heat, and heat buildup raises concerns about the reliable functioning of devices such as hard drives. Resorting to multiple core/processor architecture is a way to avoid this problem.

These turn of events raise two interesting questions:

1. How do we turn serial code which has been written into "parallel" code?

2. How do we design an environment so that code could be written with ease to harness parallelism?

The first question is related to both theoretical computer science and compiler construction. The concern is that code which has been developed might have to be rewritten to leverage parallelism.

The second question is one of software design and engineering. This design will have to provide a layer of abstraction so that the developer could focus on logical tasks instead of actual threading mechanisms and the code developed would require no maintenance as more cores become available.

Currently general purpose number theory software — MAGMA [BCP97], PARI/GP [ABC$^+$], SAGE [Gro], etc. — do not harness parallelism. In fact, there is hardly any research literature to look toward for ideas on how to implement specific number theory computation in parallel. The exceptions being certain areas of research related to symbolic computation such as polynomial arithmetic, and cryptography such as modular/finite field arithmetic, integer factoring and computing discrete logarithms.

In this chapter we will enumerate important algorithms associated to elliptic curves from the perspective of the BSD conjecture, which will benefit from parallelization. We will briefly comment on *embarassingly parallel* versions of these algorithms. In other words, each logical thread of execution is independent from the other and hence these threads could be made on run in parallel.

A quantity related to an elliptic curve over the rationals can often be expressed as a function — usually a sum or product — of local versions of that quantity, which are associated to the elliptic curve defined over the real numbers and the $p$-adic numbers. The $p$-padic places which contribute to the function are usually the primes of bad reduction for the elliptic curve. (There are also instances where a finite list of primes of good reduction contribute to the function.) The computation of the local quantities can be performed in parallel and this is our main strategy to incorporate parallelism. The problem of determining the primes of bad reduction (which is polynomial time equivalent to the problem of factoring) or a finite number of primes of good reduction for an elliptic curve can be considered to be part of the precomputation phase of the parallel algorithm.

We will proceed to consider each of the terms appearing in the BSD conjectural formula (Eq. 1.6) and make observations about leveraging parallelism from existing algorithms which compute these invariants. It is interesting to note that computation of $\Omega$ the real period of an elliptic curve, which is one of the quantities appearing in the BSD formula, does not seem to benefit much from parallelism due to the sequential nature of the Arithmetic-Geometric Mean (AGM), which is involved in the computation.

For a background on the theory of elliptic curve consult [Sil92], and for an introduction to the elliptic curve algorithms see [Cre97, Coh93].

## 5.1 Torsion subgroup

In chapter 2 we presented an algorithm that computes $E(\mathbb{Q})_{tors}$ leveraging the fact that torsion points have integral coordinates of bounded magnitude (by the Nagell-Lutz theorem). The algorithm proceeds by computing integer roots of $m$-division polynomials (which are the $x$-coordinates of $m$-torsion points) by determining the roots modulo $l$ and lifting the roots to approriate precision using Hensel's lemma. The prime $l$ is choosen such that $l > 7$, an odd prime of good reduction and "small" in magnitude. The values of $m$ of interest are guided by Mazur's theorem, which lists the groups that can occur as the elliptic curve rational torsion subgroup. The time complexity of the algorithm is as follows:

**Theorem 5.1.1** *[BH05] Let $E$ be an elliptic curve defined by $y^2 = x^3 + ax + b$, where $a, b \in \mathbb{Z}$. There is a randomized algorithm which computes $E(\mathbb{Q})_{tors}$ in $\mathcal{O}(\log H(E))$ expected time. The deterministic version of the algorithm runs in $\mathcal{O}(\log^2 H(E))$ time, where $H(E) = \max\{|a|^3, |b|^2\}$.*

In practice, a standard trick to reduce the list of of values of $m$ that are investigated is to pick $m$ such that $m \mid \#E(\mathbb{F}_l)$, since $\#E(\mathbb{F}_l)$ is a multiple of $\#E(\mathbb{Q})_{tors}$.

**Parallel Note 5.1.1** *Compute in parallel a few odd primes of good reduction $l$ for $E$, determine $\#E(\mathbb{F}_l)$ and calculate their* gcd *to obtain a bound for $\#E(\mathbb{Q})_{tors}$.*

### 5.1.1 A parallel algorithm

An alternative approach to computing elliptic curve rational torsion points is to search for integer roots of division polynomials in a parallel fashion.

**Parallel Note 5.1.2** *Using the $m$-division polynomial compute the $x$-coordinate of a $m$-torsion point modulo sufficiently many — $O(\log |\Delta(E)|)$ — odd primes of good reduction and recover the coordinate using the Chinese Remainder Theorem.*

**Parallel Note 5.1.3** *If the goal is to compute torsion for a sequence of elliptic curves, then we observe that primes used in computing torsion for one curve might also be useful for others.*

## 5.2 Tamagawa numbers

The product of the Tamagawa numbers $\prod_p c_p$ is one of the terms appearing in the BSD conjectural formula. We recall that the Tamagawa number for an elliptic curve $E$ over $\mathbb{Q}$ at $p$ is defined to be $c_p = [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$, where $E_0(\mathbb{Q}_p)$ is the subgroup of $E(\mathbb{Q}_p)$, consisting of points with non-singular reduction modulo $p$. It follows from the definition of $c_p$, that the contributions to the Tamagawa number product are from the primes of bad reduction.

**Parallel Note 5.2.1** *Compute the product of the Tamagawa numbers by determining $c_p$ for each prime of bad reduction in parallel.*

### 5.2.1 Tate's algorithm

Given an elliptic curve $E$ with integer coefficients and a prime $p$, the output of Tate's algorithm is as follows [Cre §3.2]:

- the Tamagawa number $c_p$ of $E$ at $p$,
- the exponent $f_p$ of $p$ in the conductor $N$ of $E$,
- the Kodaira symbol of $E$ at $p$, which classifies the type of reduction of $E$ at $p$,
- The algorithm also detects whether the given model of $E$ is non-minimal at $p$, and if so, returns a model which is miniml at $p$.

**Parallel Note 5.2.2** *The internals of this algorithm boil down to root finding modulo p on certain polynomials of degree at most* 3*. Parts of the algorithm could be parallelized, in particular, the root finding phase.*

The conductor of the elliptic curve is determined using the $f_p$ obtained by running Tate's algorithm in succession for each of the primes dividing the discriminant [Cre97, §3.2]. Moreover, all the coordinate transformations $T(r, s, t, u)$ which occur during the various iterations can be applied to the original model of $E$ to obtain its global minimal model.

## 5.3 Periods

The *periods* $\lambda_1$ and $\lambda_2$ of an elliptic curve $E$ form a $\mathbb{Z}$-basis for the period lattice of $E$. As the curve is defined over $\mathbb{Q}$, it can be arranged such that $\lambda_1 \in \mathbb{R}$.

The period $\Omega$ which appears in the Birch and Swinnerton-Dyer conjectural forumla 1.6 is $\lambda_1$ or $2 \cdot \lambda_1$ depending on whether or not $E(\mathbb{R})$ is connected.

We describe a recipe to compute the periods using C.F. Gauss's Arithmetic-Geometric Mean (AGM) algorithm taken from [Cre97, §3.7]. Write the equation for $E$ in the form

$$(y + \frac{a_1 x + a_3}{2})^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4} = (x - e_1)(x - e_2)(x - e_3),$$

where the roots $e_i$ are found as complex floating point approximations (using Cardano's formula, say). Then the periods are given by

$$\lambda_1 = \frac{\pi}{\mathrm{AGM}(\sqrt{e_3 - e_1}, \sqrt{e_3 - e_2})} \tag{5.1}$$

$$\lambda_2 = \frac{\pi}{\mathrm{AGM}(\sqrt{e_3 - e_1}, \sqrt{e_2 - e_1})} \tag{5.2}$$

The complex area of an elliptic curve $E$ denoted by $\mathrm{Vol}(E)$ is defined to be equal to $\lambda_1 \cdot im(\lambda_2)$. It is a quantity appearing in the Gross-Zagier formula (Eq. 4.4).

The Arithmetic-Geometric Mean of two non-negative real numbers $\alpha$ and $\beta$ denoted by $AGM(\alpha, \beta)$ is defined iteratively as follows

$$\alpha_0 = \alpha, \beta_0 = \beta, \alpha_{n+1} = \frac{1}{2}(\alpha_n + \beta_n), \beta_{n+1} = \sqrt{\alpha_n \beta_n} \tag{5.3}$$

until $\alpha_n = \beta_n$ to the desired precision.

**Parallel Note 5.3.1** *The computation of the square roots in Eq. 5.1 and Eq. 5.2 could be performed in parallel. Also, the computation of an AGM could be parallelized by computing*

*$a_n$ and $b_n$ (Eq. 5.3) in tandem. However, we observe that nature of the recursive definition of AGM inhibits parallelization.*

## 5.4 Leading coefficient of $L_E(s)$ at $s = 1$

Given an elliptic curve $E$ defined over $\mathbb{Q}$ with conductor $N$, as input, computing $L^{(r)}(E, 1)$, $r = 0, 1$ (for higher derivatives see [Coh93, §8.5.3]) using $k$ terms of the associated series involves computing the root number $w(E)$, the Fourier coefficients $a_n$ and the sum

$$2 \cdot \sum_{n=1}^{k} \frac{a_n(E)}{n} E_r(\frac{2\pi n}{\sqrt{N}}). \tag{5.4}$$

The functions $E_0(x)$ and $E_1(x)$ denote $\exp(x)$ and $\int_x^\infty \frac{e^{-t}}{t} dt$, the exponential integral function, respectively. A bound on the tail of the series is given by [GJP$^+$05]

$$2 \cdot e^{-2\pi(k+1)N^{-1/2}} \cdot (1 - e^{-2\pi N^{-1/2}})^{-1}.$$

**Parallel Note 5.4.1** *The computation of $\{E_0(i \cdot x)\}_{i \leq k}$ could be parallelized since the function $E_0$ satisfies the relation $E_0(a + b) = E_0(a) \cdot E_0(b)$ for $a, b \in \mathbb{R}$. On the other hand, the definition of $E_1(x)$ seems to inhibit such parallelism.*

### 5.4.1 Root number

The (global) root number $w(E)$ of an elliptic curve $E$ is 1 if the order of vanishing of the L-series $L(E, s)$ at 1 is even, and $-1$ if it is odd. The root number can be computed from the local root numbers: $w(E) = \prod_{p \leq \infty} w_p(E)$, where $w_p(E) = \pm 1$ and equal to 1 for the primes of good reduction, and $-1$ for $p = \infty$. Hence $w(E) = -\prod_{p|\Delta} w_p(E)$. There are explicit formulae [Riz03] to compute the local root numbers of the elliptic curve, which boil down to solving modular equations.

**Parallel Note 5.4.2** *Compute local root numbers at primes of bad reduction in parallel to determine the global root number of an elliptic curve.*

### 5.4.2 Fourier coefficients

Let $a_n$ denote the $n^{\text{th}}$ Fourier coefficient of the modular form corresponding to the elliptic curve $E$, where n is a positive integer.

Let $N$ be the conductor of $E$. The first coefficient $a_1 = 1$. When $p$ is a prime of good reduction for $E$, that is when $p \nmid N$, $a_p = p + 1 - \#E(\mathbb{F}_p)$, where $\#E(\mathbb{F}_p)$ denotes the number of $\mathbb{F}_p$-points of the curve $E$. When $p \mid N$, in other words, $p$ is a prime of additive, split multiplicative or non-split multiplicative reduction for $E$, $a_p = 0, 1, -1$ respectively.

The Fourier coefficients at composite indexes are determined by the following formulae: $a_{m \cdot n} = a_m \cdot a_n$ when $m$ and $n$ are relatively prime, $a_{p^r} = a_{p^{r-1}} \cdot a_p - p \cdot a_{p^{r-2}}$ when $p$ is prime and $p \nmid N$, and $a_{p^r} = a_p^r$ when $p$ is prime and $p \mid N$,.

**Parallel Note 5.4.3** *Computing a single $a_n$ can be performed in parallel utilizing the above recurrence relations.*

*Computing $\{a_n\}_{n \leq k}$ can be broken down into two tasks: determining $a_p$, for prime $p \leq k$ and calculating $a_n$, for $n$ composite using the above recurrence relations. The $a_p$'s can be computed in parallel and algorithms to determine them are discussed in the next subsection when $p$ is a prime of good reduction.*

### 5.4.3 Order of the group $E(\mathbb{F}_p)$

The order of the group $E(\mathbb{F}_p)$ can be computed using one of the following methods:

*Legendre symbol*: Let $E$ be an elliptic curve defined by $y^2 = f(x)$, where $f(x)$ is a cubic polynomial in $\mathbb{F}_p$. Then $\#E(\mathbb{F}_p) = p + 1 + \sum_{x_0 \in \mathbb{F}_p} (\frac{f(x_0)}{p})$ where $(\frac{\cdot}{p})$ is the Legendre symbol at $p$.

**Parallel Note 5.4.4** *The determination of* $\{(\frac{f(x_0)}{p})\}_{x_0 \leq p}$ *can be parallelized and computed values could be stored to speed up the calculations.*

*Generic algorithms.* Algorithms such as Baby-Step Giant-Step and the Pollard Rho work on any finite group [BSS00, §VI.3, §V.5]. These are exponential time algorithms and moreover, the Baby-Step Giant-Step is also an exponential space algorithm.

**Parallel Note 5.4.5** *The lambda method which is a variant of the rho method can be parallelized to achieve a linear speedup as discovered by van Oorschot and Wiener (consult [BSS00] for references).*

*R. Schoof's algorithm*: This algorithm was the first polynomial time algorithm for elliptic curve point counting. The overview of this method is that $a_p \bmod l$ is determined for all primes $l = O(\log p)$ and $a_p$ can be recovered using the Chinese Remainder Theorem. The algorithm involves symbolic computation using the $f_l$ division polynomials. The interested reader should consult [BSS00, §VII] for details.

**Parallel Note 5.4.6** *The computation of* $a_p \bmod l$ *for various primes* $l$ *could be proceed in parallel.*

## 5.5 Regulator

The elliptic regulator of an elliptic curve $E$ denoted by $Reg(E)$ is the volume of a fundamental domain for $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$ computed using the Néron-Tate pairing $\hat{h}$. Explicitly, if $P_1, \ldots, P_r$ generate $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$ then

$$Reg(E) = det(\langle P_i, P_j \rangle)_{1 \leq i,j \leq r}, \tag{5.5}$$

where $\langle P_i, P_j \rangle = \hat{h}(P_i + P_j) - \hat{h}(P_i) - \hat{h}(P_j)$. If $r = 0$, $Reg(E)$ is set to 1 by convention.

Computing the regulator can be broken down into the following tasks: computing the determinant of a (symmetric) matrix, computing the canonical height of a point, and determining a set of generators for $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$. Strategies to harness parallelism in these three tasks will occupy the remainder of this section and the next one.

### 5.5.1 Determinant of a matrix

Parallel computation of the determinant of matrix is a problem which has received the attention of the research community, see [GP89].

### 5.5.2 Canonical height of a point

The canonical height $\hat{h}(P)$ of a point $P \in E(\mathbb{Q})$ is defined as a sum of *local heights*:

$$\hat{h}(P) = \sum_{p \leq \infty} \hat{h}_p(P) \tag{5.6}$$

where the sum is over all finite primes $p$ and the 'infinite prime' $\infty$ coming from the real embedding of $\mathbb{Q}$. The local height of $P$ at $p$, $\hat{h}_p(P)$ can be determined using formulae listed in [Cre97, Proposition 3.4.1], and $\hat{h}_\infty(P)$ can be calculated using an infinite series. Explicitly the canonical height of a point can be determined as follows:

$$\hat{h}(P) = \hat{h}_\infty(P) + 2\log(c) + \sum_{p|\Delta, p\nmid c} \hat{h}_p(P), \tag{5.7}$$

where $c^2$ is the denominator of the $x$-coordinate of the point $P$. An alternative method of computation was described by J.H. Silverman which utilizes little or no factorization.

**Parallel Note 5.5.1** *The local heights in Eq. 5.7 can be computed in parallel. Moreover, calculation of a specific local height also has potential for parallelization, in particular, the calculation of* $\hat{h}_\infty(P)$.

## 5.6 Mordell-Weil group

The procedure of descent is a method to determine the rank and the generators of the Mordell-Weil group of an elliptic curve. It is not an algorithm as it is not guaranteed to terminate (in fact, there are no known unconditional algorithms to compute the rank). In this section, we sketch the main tasks of performing descent via 2-isogeny and provide techniques to incorporate parallelism. The reader should consult J.E. Cremona's book [Cre97, §3.6] for a description of the general two-descent procedure.

Performing descent via 2-isogeny and returning generators for the Mordell-Weil group $E(\mathbb{Q})$ modulo torsion involves:

- computing the set $S$ (which equals $\mathbb{R}$ and the set of places of bad reduction) involves factoring the discriminant and

$$\mathbb{Q}(S,2) = \{\mathbb{Q}^*/\mathbb{Q}^{*2} \mid ord_\nu(b) \equiv 0 \bmod 2 \text{ for } \text{ all } \nu \notin S\}. \tag{5.8}$$

- determining which elements of $\mathbb{Q}(S,2)$ are elements of the Selmer group. This corresponds to checking whether the associated quartics have points over $\mathbb{R}$ and over every $\mathbb{Q}_p$ (suffices to check for $p \in S$). These computations are local in nature (and involve Hensel lifting). This step determines the homogeneous spaces on which to search for rational points.

- searching for rational points on each homogeneous space.

**Parallel Note 5.6.1** *Parallelize descent by: computing $S$ and $\mathbb{Q}(S,2)$ in parallel, parallelize selmer group computation, searching for rational points on homogeneous spaces in parallel, and searching in parallel for rational points on a specific homogenous space on distinct height intervals.*

## 5.7 Size of the Shafarevich-Tate group

The standard method to compute $\#Ш(E)$ is via the BSD conjectural formula. The formula can be used to obtain $\#Ш(E) \cdot Reg(E)$ and $\#Ш(E)$ is determined provided the regulator of the elliptic curve is known. The size of $Ш(E)$ calculated using the BSD formula is termed the *analytic order* of $Ш(E)$, denoted by $\#Ш_{an}(E)$, and computing it would involve the methods listed in the previous sections.

# Bibliography

[ABC$^+$] Bill Allombert, Karim Belabas, Henri Cohen, Xavier Roblot, and Ilya Zakharevitch. `PARI/GP`. `http://pari.math.u-bordeaux.fr/`.

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939 (electronic), 2001.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BDG$^+$07] Iftikhar A. Burhanuddin, James Demmel, Edray Goins, Eric Kaltofen, Fernando Perez, William A. Stein, Helena Verrill, and Joe Weening. Workshop: Interactive parallel computation in support of research in algebra, geometry and number theory. 2007. `http://sage.math.washington.edu/msri07`.

[BFH90] Daniel Bump, Solomon Friedberg, and Jeffrey Hoffstein. Nonvanishing theorems for $L$-functions of modular forms and their derivatives. *Invent. Math.*, 102(3):543–618, 1990.

[BH05] Iftikhar A. Burhanuddin and Ming-Deh A. Huang. Elliptic curve torsion points and division polynomials. In *Computational aspects of algebraic curves*, volume 13 of *Lecture Notes Ser. Comput.*, pages 13–37. World Sci. Publ., Hackensack, NJ, 2005.

[Bir98] Bryan J. Birch. Atkin and the Atlas Lab. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *AMS/IP Stud. Adv. Math.*, pages 13–20. Amer. Math. Soc., Providence, RI, 1998.

[Bra47] Richard Brauer. On the zeta-functions of algebraic number fields. *Amer. J. Math.*, 69:243–250, 1947.

[BS66] Bryan J. Birch and Nelson M. Stephens. The parity of the rank of the Mordell-Weil group. *Topology*, 5:295–299, 1966.

[BS98] László Babai and Joel Spencer. Paul Erdős (1913–1996). *Notices Amer. Math. Soc.*, 45(1):64–73, 1998.

[BSD63] Bryan J. Birch and H. Peter F. Swinnerton-Dyer. Notes on elliptic curves. I. *J. Reine Angew. Math.*, 212:7–25, 1963.

[BSS00] Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart. *Elliptic curves in cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2000. Reprint of the 1999 original.

[Cas49] John W. S. Cassels. A note on the division values of $\wp(u)$. *Proc. Cambridge Philos. Soc.*, 45:167–172, 1949.

[Coh93] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[Coh07] Henri Cohen. *Number Theory*, volume 239-240 of *Graduate Texts in Mathematics*. Springer-Verlag, 2007.

[Cre] John E. Cremona. Elliptic curve data up to conductor $120,000$. `http://www.maths.nott.ac.uk/personal/jec/ftp/data/`.

[Cre97] John E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997. `http://www.maths.nott.ac.uk/personal/jec/book`.

[Dan82] L. V. Danilov. The Diophantine equation $x^3 - y^2 = k$ and a conjecture of M. Hall. *Mat. Zametki*, 32(3):273–275, 425, 1982. English translation: Math. Notes 32 (1982), no. 3, and Letter to the editor Math. Notes 36 (1984), no. 3.

[Del01] Christophe Delaunay. Heuristics on Tate-Shafarevitch groups of elliptic curves defined over $\mathbb{Q}$. *Experiment. Math.*, 10(2):191–196, 2001.

[Dou98] Darrin Doud. A procedure to calculate torsion of elliptic curves over $\mathbf{Q}$. *Manuscripta Math.*, 95(4):463–469, 1998.

[dW98] Benjamin M. M. de Weger. $A + B = C$ and big Ш's. *Quart. J. Math. Oxford Ser. (2)*, 49(193):105–128, 1998.

[FGH00] Mireille Fouquet, Pierrick Gaudry, and Robert Harley. An extension of Satoh's algorithm and its implementation. *J. Ramanujan Math. Soc.*, 15(4):281–318, 2000.

[GJP$^+$05] Grigor Grigorov, Andrei Jorza, Stephan Patrikis, William A. Stein, and Corina E. Tarniţă-Pătraşcu. Verification of the Birch and Swinnerton-Dyer Conjecture for Specific Elliptic Curves. 2005. (Preprint) `http://sage.math.washington.edu/papers/bsdalg/`.

[GP89] Zvi Galil and Victor Pan. Parallel evaluation of the determinant and of the inverse of a matrix. *Inform. Process. Lett.*, 30(1):41–45, 1989.

[Gro] The SAGE Group. SAGE Mathematics Software (Version 2.6). `http://www.sagemath.org/`.

[GS95] Dorian Goldfeld and Lucien Szpiro. Bounds for the order of the Tate-Shafarevich group. *Compositio Math.*, 97(1-2):71–87, 1995. Special issue in honour of Frans Oort.

[GSOT02] Irene García-Selfa, Miguel A. Olalla, and José M. Tornero. Computing the rational torsion of an elliptic curve using Tate normal form. *J. Number Theory*, 96(1):76–88, 2002.

[Guy04] Richard K. Guy. *Unsolved problems in number theory*. Problem Books in Mathematics. Springer-Verlag, New York, third edition, 2004.

[Har92] Godfrey H. Hardy. *A mathematician's apology*. Canto. Cambridge University Press, Cambridge, 1992. With a foreword by C. P. Snow, Reprint of the 1967 edition.

[Hin] Marc Hindry. Why is it difficult to compute the Mordell-Weil group? (Preprint) `http://www.math.jussieu.fr/∼hindry/MW-size.pdf`.

[HL23] Godfrey H. Hardy and John E. Littlewood. Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes. *Acta Math.*, 44(1):1–70, 1923.

[JKP06] Daeyeol Jeon, Chang Heon Kim, and Euisung Park. On the torsion of elliptic curves over quartic number fields. *J. London Math. Soc. (2)*, 74(1):1–12, 2006.

[Kat81] Nicholas M. Katz. Galois properties of torsion points on abelian varieties. *Invent. Math.*, 62(3):481–502, 1981.

[KM95] Sheldon Kamienny and Barry Mazur. Rational torsion of prime order in elliptic curves over number fields. *Astérisque*, (228):3, 81–100, 1995. With an appendix by A. Granville, Columbia University Number Theory Seminar (New York, 1992).

[Kna92] Anthony W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992.

[Kob93] Neal Koblitz. *Introduction to elliptic curves and modular forms*, volume 97 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1993.

[Kob94] Neal Koblitz. *A course in number theory and cryptography*, volume 114 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[Kol90] Victor A. Kolyvagin. Euler systems. In *The Grothendieck Festschrift, Vol. II*, volume 87 of *Progr. Math.*, pages 435–483. Birkhäuser Boston, Boston, MA, 1990.

[Kri94] Mohamed Krir. Minorant de la dérivée au point 1 de la fonction $L$ attachée à une courbe elliptique de Weil. *J. Théor. Nombres Bordeaux*, 6(2):281–299, 1994.

[Lan78] Serge Lang. *Elliptic curves: Diophantine analysis*, volume 231 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1978.

[Lan83] Serge Lang. Conjectured Diophantine estimates on elliptic curves. In *Arithmetic and geometry, Vol. I*, volume 35 of *Progr. Math.*, pages 155–171. Birkhäuser Boston, Boston, MA, 1983.

[Mila] James S. Milne. Course Notes: Class Field Theory. `http://www.jmilne.org/math/CourseNotes/math776.html`.

[Milb] James S. Milne. Course Notes: Elliptic Curves. `http://www.jmilne.org/math/CourseNotes/math679.html`.

[MM91] M. Ram Murty and V. Kumar Murty. Mean values of derivatives of modular $L$-series. *Ann. of Math. (2)*, 133(3):447–475, 1991.

[Par99] Pierre Parent. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *J. Reine Angew. Math.*, 506:85–116, 1999.

[Pau01] Sebastian Pauli. Factoring polynomials over local fields. *J. Symbolic Comput.*, 32(5):533–547, 2001.

[Riz03] Ottavio G. Rizzo. Average root numbers for a nonconstant family of elliptic curves. *Compositio Math.*, 136(1):1–23, 2003.

[Ros00] Harvey E. Rose. On some elliptic curves with large sha. *Experiment. Math.*, 9(1):85–89, 2000.

[Sem98] Igor A. Semaev. Evaluation of discrete logarithms in a group of $p$-torsion points of an elliptic curve in characteristic $p$. *Math. Comp.*, 67(221):353–356, 1998.

[Sil92] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[ST92] Joseph H. Silverman and John Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[Sta82] Harold M. Stark. The Coates-Wiles theorem revisited. In *Number theory related to Fermat's last theorem (Cambridge, Mass., 1981)*, volume 26 of *Progr. Math.*, pages 349–362. Birkhäuser Boston, Mass., 1982.

[Ste] William A. Stein. Elliptic Curves, the ABC conjecture, and points of small canonical height (notes from a seminar talk by Matt Baker). `http://modular.fas.harvard.edu/mcs/archive/Fall2001`.

[SW02] William A. Stein and Mark J. Watkins. A database of elliptic curves—first report. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 267–275. Springer, Berlin, 2002.

[SW04] William A. Stein and Mark J. Watkins. Modular parametrizations of Neumann-Setzer elliptic curves. *Int. Math. Res. Not.*, (27):1395–1405, 2004.

[Val75] Leslie G. Valiant. Parallelism in comparison problems. *SIAM J. Comput.*, 4(3):348–355, 1975.

[vzGG03] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, second edition, 2003.

# Appendix A

## Deciding whether $\#E(\mathbb{Q}_p)[p]$ is nontrivial

*The mathematician's patterns, like the painter's or the poet's must be beautiful; the ideas, like the colors or the words must fit together in a harmonious way. Beauty is the first test: there is no permanent place in this world for ugly mathematics.*

G. H. Hardy *[Har92].*

The reader should consult Chapter 1 for definitions and theorems of relevance to elliptic curve torsion, types of reduction, etc.

We know that $E(\overline{\mathbb{Q}}_l)[p] = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Suppose $p > 2$ and $\#E(\mathbb{Q}_l)[p] = p^2$ then the Weil Pairing [Sil92, Corollary III.8.1.1] would imply $\mu_p \subset \mathbb{Q}_l^*$, which would hold if $p|l-1$, a contradiction. Therefore in particular $\#E(\mathbb{Q}_p)[p] = 1, p$.

The question of efficiently determining whether $\#E(\mathbb{Q}_p)[p] = p$ is one of independent interest. Our motivation to look at this problem is by viewing an elliptic curve $E$ over $\mathbb{Q}$ as an elliptic curve over $\mathbb{Q}_p$, $E(\mathbb{Q}_p)[p]$ being trivial would imply $E(\mathbb{Q})[p]$ is trivial (since the latter injects into the former). And this is useful information in $E(\mathbb{Q})_{tors}$ computing procedures.

The algorithms presented in this section work with an elliptic curve over $\mathbb{Q}_p$. We will assume that we are presented with an elliptic curve $E$ over $\mathbb{Q}$ and a prime $p > 2$. We make this choice to simplify the time complexity and $p$-adic precision analysis of the algorithms (otherwise in the worst case — split multiplicative reduction and $p|v_p(\Delta)$ — we will require as input the coefficients of the curve over $\mathbb{Q}_p$ to $p$ digits of $p$-adic accuracy, where $v_p$ is the $p$-adic valuation of $\mathbb{Q}_p$). Given an elliptic curve over the rationals we will use Tate's algorithm [Sil94, Chapter IV.9] to compute the minimal Weierstrass equation of $E$ at $p$. And by abuse of notation we will denote by $E$ both the original elliptic curve and its minimal Weierstrass equation at $p$. Also we will refer to the associated discriminants of the former and latter as $\Delta$ and hopefully what we mean will be clear from the context.

The proof of following theorem will keep us occupied for the remainder of this section:

**Theorem A.0.1** *There exists an algorithm which takes as input an elliptic curve over $\mathbb{Q}$ and a prime $p > 2$ and decides whether $\#E(\mathbb{Q}_p)[p] = p$. It has a worst case time complexity which is polynomial in $\log p$ and the bit length of the coefficients of the elliptic curve.*

## A.1 Computing $\#E_0(\mathbb{Q}_p)[p]$

This following algorithm determines $\#E_0(\mathbb{Q}_p)[p]$, in other words computes $\#E(\mathbb{Q}_p)[p]$ when there are no $p$-torsion points which reduce to a singular point.

**Algorithm A.1.1** *Let $E$ be an elliptic curve over $\mathbb{Q}_p$ given by a minimal Weierstrass equation, where $p > 2$.*

*Input. We are given the coefficients of $E$, modulo $p^2$ and the type of reduction.*

*Output. TRUE if $\#E_0(\mathbb{Q}_p)[p] = p$ and FALSE if $\#E_0(\mathbb{Q}_p)[p] = 1$.*

1. *$n \leftarrow \#\overline{E}_{ns}(\mathbb{F}_p)$.*

2. *If $p \nmid n$ return FALSE.*

3. *Pick a nontrivial point $\overline{P} \in \overline{E}_{ns}(\mathbb{F}_p)[p]$.*

4. *Lift $\overline{P}$ to $P \in E_0(\mathbb{Q}_p) \setminus E_1(\mathbb{Q}_p)$ using Hensel's lemma such that $P \equiv \overline{P} \bmod p$. We only need to determine $x(P)$ modulo $p^2$.*

5. *Compute $x([p-1]P) \bmod p^2$ using the repeated squaring trick [Kob94, Page 23] and the elliptic curve group law formulae [Sil92, Algorithm 2.3].*

6. *If $x([p-1]P) \equiv x(P) \bmod p^2$ return TRUE. Otherwise return FALSE.*

**Lemma A.1.1** *The above algorithm works as desired.*

**Proof A.1.1** *First we recall a fact about the structure of $\overline{E}_{ns}(\mathbb{F}_p)$ in the case of bad reduction [Sil92, Exercise III.3.5]: $\overline{E}_{ns}(\mathbb{F}_p) \cong \mathbb{F}_p^+$, $\mathbb{F}_p^*$ or $\{t \in L^* \mid N_{L/\mathbb{F}_p}(t) = 1\}$ where $L = \mathbb{F}_p(\alpha_1, \alpha_2)$ and $\alpha_1, \alpha_2$ are the slopes of tangent lines in the non-split multiplicative reduction case.*

*Note that $E_1(\mathbb{Q}_p) \cong \hat{E}(p\mathbb{Z}_p) \cong \hat{G}_a(p\mathbb{Z}_p)$ is torsion-free. Now the short exact sequence $0 \to E_1(\mathbb{Q}_p) \to E_0(\mathbb{Q}_p) \to \overline{E}_{ns}(\mathbb{F}_p) \to 0$ [Sil92, Proposition VII.2.1] gives rise to the following long exact sequence via the extended snake lemma [Mila, Lemma II.4.1]:*

$$0 \to E_0(\mathbb{Q}_p)[p] \to \overline{E}_{ns}(\mathbb{F}_p)[p] \xrightarrow{\phi} \hat{G}_a(p\mathbb{Z}_p)/p\hat{G}_a(p\mathbb{Z}_p) \to E_0(\mathbb{Q}_p)/pE_0(\mathbb{Q}_p)$$
$$\to \overline{E}_{ns}(\mathbb{F}_p)/p\overline{E}_{ns}(\mathbb{F}_p) \to 0$$

*If* $\gcd(n,p) = 1$ *then* $\overline{E}_{ns}(\mathbb{F}_p)[p] = 0$ *which implies that* $E_0(\mathbb{Q}_p)[p] = 0$*. This case takes care of split multiplicative reduction as we have* $\#\overline{E}_{ns}(\mathbb{F}_p) = \#\mathbb{F}_p^* = p-1$ *and of the non-split case as we have* $\#\overline{E}_{ns}(\mathbb{F}_p) = 1, p-1, p+1, p^2-1$*.*

*If* $\gcd(n,p) \neq 1$ *(due to good reduction or additive reduction) and we pick a point* $P \neq O$ *in* $\overline{E}_{ns}(\mathbb{F}_p)[p]$*, then appealing to the lemma below tells us that* $E_0(\mathbb{Q}_p)[p]$ *being nontrivial is equivalent to* $x([p-1]P) \equiv x(P) \bmod p^2$*. Now we observe that when we compute* $x([p-1]P)$ *by the squaring trick, the denominators are p-adic units (part (2) of the lemma) and the group law formulae hold modulo* $p^2$*. This suggests that only the coefficients of elliptic curve* $E$ *and of the coordinates of the point* $P$ *modulo* $p^2$ *contribute towards the computation. This completes the proof of the theorem.*

**Lemma A.1.2** *Let* $E$ *be an elliptic curve over* $\mathbb{Q}_p$ *given by a minimal Weierstrass equation. If* $Q \in E_0(\mathbb{Q}_p) \setminus E_1(\mathbb{Q}_p)$ *and* $\overline{Q} \in \overline{E}_{ns}(\mathbb{F}_p)[p]$ *then*

1. $[i]Q \in E_0(\mathbb{Q}_p) \setminus E_1(\mathbb{Q}_p)$*,* $i = 1, \ldots, p-1$*,*

2. $x([i]Q) \not\equiv x([j]Q) \bmod p$*,* $0 < j < i < p$ *and* $i + j < p$*,*

3. $x([p-k]Q) \equiv x([k]Q) \bmod p$ *and* $y([p-k]Q) \equiv -y([k]Q) \bmod p$ *(in particular* $y([p-k]Q) \not\equiv y([k]Q) \bmod p$*),* $0 < k < p$*,*

4. $[p]Q \in E_i(\mathbb{Q}_p) \setminus E_{i+1}(\mathbb{Q}_p) \Leftrightarrow v_p(x([p]Q)) = -2i \Leftrightarrow v_p(x([p-1]Q) - x(Q)) = i$*,* $i \geq 1$*,*

5. $x([p-1]Q) - x(Q) \equiv 0 \bmod p^2 \Leftrightarrow \phi = 0$*, where* $\phi : \overline{E}_{ns}(\mathbb{F}_p)[p] \to \hat{G}_a(p\mathbb{Z}_p)/p\hat{G}_a(p\mathbb{Z}_p)$*.*

**Proof A.1.2** 1. *Suppose* $[i]Q \in E_1(\mathbb{Q}_p)$ *then* $[i]\overline{Q} = O$ *which is a contradiction since* $\gcd(i,p) = 1$*.*

2. *Suppose* $x([i]Q) \equiv x([j]Q) \bmod p$. *This assumption combined with the fact that* $[i]\overline{Q}, [j]\overline{Q} \neq O$ *implies that* $[i]\overline{Q} = \pm([j]\overline{Q})$ *and hence* $[i \pm j]\overline{Q} = O$. *This is a contradiction as* $\gcd(i \pm j, p) = 1$.

3. *Let* $R := [p-k]Q$. *Therefore* $\overline{R} = [p-k]\overline{Q} = -[k]\overline{Q}$. *Hence* $x(\overline{R}) = x([k]\overline{Q})$ *and* $y(\overline{R}) = -y([k]\overline{Q})$.

4. *From part (3) we know that* $x([p-k]Q) \equiv x([k]Q) \bmod p$. *Say* $v_p(x([p-k]Q) - x([k]Q)) = i$. *We also know that* $y([p-k]Q) \not\equiv y([k]Q) \bmod p$. *From the group law formulae to calculate* $[p]Q$ *(say using* $[k]Q$ *and* $[p-k]Q$*), it follows that* $v_p(x([p]Q)) = -2i$ *which is equivalent to* $v_p(y([p]Q)) = -3i$ *[Milb, Proof of Theorem 7.1(c)]. And therefore* $[p]Q \in E_i(\mathbb{Q}_p) \setminus E_{i+1}(\mathbb{Q}_p)$.

5. $x([p-1]Q) - x(Q) \equiv 0 \bmod p^2$ *implies* $[p]Q \in E_2(\mathbb{Q}_p)$ *by part (4). This implies that* $\phi(\overline{Q}) = (\log_E \circ \lambda \circ [p])(Q) = 0 \in \hat{G}_a(p\mathbb{Z}_p)/p\hat{G}_a(p\mathbb{Z}_p)$. *Here* $\lambda(R) = -x(R)/y(R)$, *where* $R \in E_1(\mathbb{Q})$ *and* $\log_E(z) = z + O(z^2)$, *where* $z \in \hat{E}(p\mathbb{Z}_p)$.

   *(On the other hand* $x([p-1]Q) - x(Q) \not\equiv 0 \bmod p^2$ *implies* $[p]Q \in E_1(\mathbb{Q}_p) \setminus E_2(\mathbb{Q}_p)$ *by part (4). This implies that* $\phi(\overline{Q}) = (\log_E \circ \lambda \circ [p])(Q) \neq 0$*).*

In step 3 of the algorithm A.1.1, it is sufficient to pick $x_0 \in \mathbb{F}_p$ such that $(\frac{x_0^3+ax_0+b}{p}) = 1$. Computing the Legendre symbol can be done in $O(\log^2 p)$ [Coh93, Algorithm 1.4.12] and Hensel lifting can be performed in almost linear time. Step 5 would consume $\mathcal{O}(\log^2 p)$ bit operations. Therefore in the good reduction case the overall time complexity of the algorithm is dominated by the point counting routine which takes time $\mathcal{O}(\log^{5+\epsilon} p)$ [BSS00, Chapter 7].

In the case of good reduction if $p > 5$ we have two cases $\gcd(n, p) = 1$ and $n = p$. If $p = 3, 5$ we have a third case — $\gcd(n, p) = p$ and $n \neq p$ — the only instances of which are $n = 2p$ by the Hasse bound. And this is the reason we pick $\overline{P} \in \overline{E}(\mathbb{F}_p)[p]$ in the algorithm.

We will now use the output of the above algorithm to decide whether $E(\mathbb{Q}_p)[p]$ is nontrivial with the help of the following fact [Sil94, Corollary $IV$.9.2]: Let $E$ be an elliptic curve over $\mathbb{Q}_p$. Then we have the following exact sequence:

$$0 \to E_0(\mathbb{Q}_p) \to E(\mathbb{Q}_p) \to G \to 0$$

where if $E$ has split multiplicative reduction over $\mathbb{Q}_p$, then $G$ is a cyclic group of order $v(\Delta) = -v(j)$, in the additive scenario the group order is at most 4 and in the non-split multiplicative instance it is either 1 or 2.

In order to weed out the spurious cases we impose some conditions.

**Lemma A.1.3** *Algorithm A.1.1 correctly computes $\#E(\mathbb{Q}_p)[p]$ provided either*

- *$E$ has good reduction or*

- *$E$ has additive reduction and $p > 3$, or*

- *$E$ has additive reduction, $p = 3$ and $\gcd(\#G, 3) = 1$, or*

- *$E$ has non-split multiplicative reduction or*

- *$\#E_0(\mathbb{Q}_p)[p] = p$.*

**Proof A.1.3** *In the case of good reduction $E_0 = E$ and $\overline{E}_{ns} = \overline{E}$ and the lemma follows. If $E$ has bad reduction we have the following long exact sequence:*

$$0 \to E_0(\mathbb{Q}_p)[p] \to E(\mathbb{Q}_p)[p] \to G[p] \to E_0(\mathbb{Q}_p)/pE_0(\mathbb{Q}_p) \to E(\mathbb{Q}_p)/pE(\mathbb{Q}_p) \to G/pG \to 0$$

*Under the first 4 assumptions of the lemma we have $G[p] = 0$ and assuming the fifth case holds then $\#E(\mathbb{Q}_p)[p] = p$, and hence in all the scenarios $E_0(\mathbb{Q}_p)[p] \cong E(\mathbb{Q}_p)[p]$.*

## A.2 Algorithm when $E$ has split multiplicative reduction at $p$

To deal with the split multiplicative case we use the theory of the Tate curve [Sil94, Sections 3-5].

**Algorithm A.2.1** *An elliptic curve $E$ over $\mathbb{Q}_p$ with split multiplicative reduction given by a minimal Weierstrass equation, where $p > 2$.*

*Input. $j(E)$, the $j$-invariant of $E$ up to two significant $p$-adic digits and $v_p(j(E))$.*

*Output. TRUE if $\#E(\mathbb{Q}_p)[p] = p$ and FALSE if $\#E(\mathbb{Q}_p)[p] = 1$.*

```
1. $g \leftarrow -v_p(j(E))$.
2. If $p \nmid g$ then return FALSE.
3. $s_0 + s_1 p \leftarrow p^g \cdot j(E) \bmod p^2$.
4. $u_1 \leftarrow -(\frac{1}{p} \cdot \frac{s_0^{p-1}-1}{(p-1)s_0^{p-2}}) \bmod p$.
5. $t_1 \leftarrow \frac{s_1-u_1}{s_0} \bmod p$.
```

*6. If $t_1 = 0$ return TRUE else return FALSE.*

**Lemma A.2.1** *The algorithm works as claimed.*

**Proof A.2.1** *Now let us view $E$ as the Tate curve $E_q$, with $q \in \mathbb{Q}_p^*$ (by abuse of notation we will refer to both of them as $E$). $G = E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ which is a cyclic group of order $\#G = v_p(\Delta) = v_p(q) = -v_p(j(E))$. Furthermore $0 < v_p(\Delta) < \infty$ and hence step (1) is well-defined.*

*Recall that $E(\mathbb{Q}_p) = \mathbb{Q}_p^*/q^{\mathbb{Z}}$ [Sil94, Theorem V.3.1(d)], $E_0(\mathbb{Q}_p) \cong \mathbb{Z}_p^*$ [Sil94, Page 432]. We have $\mathbb{Z}_p^*[p] = 1$ (since $x^p - 1$ has only the trivial root of unity in $\mathbb{Q}_p$) and hence $\#E_0(\mathbb{Q}_p)[p] = 1$.*

*Now by the snake lemma, the short exact sequence*

$$0 \to \mathbb{Z}_p^* \to \mathbb{Q}_p^*/q^{\mathbb{Z}} \xrightarrow{v_p} G \to 0$$

*gives us the following long exact sequence*

$$0 \to \mathbb{Q}_p^*/q^{\mathbb{Z}}[p] \xrightarrow{v_p} G[p] \xrightarrow{\delta} \mathbb{Z}_p^*/\mathbb{Z}_p^{*p} \to (\mathbb{Q}_p^*/q^{\mathbb{Z}})/(\mathbb{Q}_p^*/q^{\mathbb{Z}})^p \to G/pG \to 0$$

*$G = \mathbb{Z}/v_p(q)\mathbb{Z}$ and $G[p]$ is generated by $\frac{v_p(q)}{p}$. Now $\mathbb{Z}_p^* = \mu_{p-1} \cdot (1 + p\mathbb{Z}_p)$, where $\mu_{p-1}$ are the $p-1^{st}$ roots of unity in $\mathbb{Z}_p^*$. This tells us that $\mathbb{Z}_p^*/\mathbb{Z}_p^{*p} \cong (1+p\mathbb{Z}_p)/(1+p^2\mathbb{Z}_p) \cong \mathbb{Z}/p\mathbb{Z}$.*

*Observe that $\delta = 0 \Leftrightarrow \mathbb{Q}_p^*/q^{\mathbb{Z}}[p] \cong G[p]$, therefore the question is how do we determine whether $\delta = 0$. In the case that $G[p] = 0$, that is, when $p \nmid v_p(q)$ then $\#E(\mathbb{Q}_p)[p] = 1$ and the correctness of step (2) of the algorithm follows. Now let us consider the case when $p | v_p(q)$. By the definition of the connecting homomorphism $\delta$, we have $\delta(\frac{v_p(q)}{p}) =$*

*$p^{\frac{v_p(q)}{p}p}/q^{\mathbb{Z}} + \mathbb{Z}_p^{*p}$, where $p^{v_p(q)}/q^{\mathbb{Z}} \in \mathbb{Z}_p^*$. If $p^{v_p(q)}/q \in \mathbb{Z}_p^{*p}$ then $\delta = 0$ which would imply $\#\mathbb{Q}_p^*/q^{\mathbb{Z}}[p] = p$, otherwise $G[p] \cong \mathbb{Z}_p^*/\mathbb{Z}_p^{*p}$ and $\#\mathbb{Q}_p^*/q^{\mathbb{Z}}[p] = 1$.*

*To check whether $p^{v_p(q)}/q \in \mathbb{Z}_p^{*p}$, firstly we will need $v_p(q)$ which is equal to $v_p(\Delta)$. The $q$ parameter is obtained by working with the $j(E)$, the $j$-invariant of $E$ [Sil94, Lemma V.5.1]. Specifically $q \equiv j(E)^{-1} \bmod p^{2 \cdot v_p(\Delta)}$ and hence $p^{v_p(q)}/q \equiv j(E) \bmod p^{2 \cdot v_p(\Delta)}$. We want to ascertain whether the unit $p^{v_p(q)}/q \in \mathbb{Z}_p^*$ is actually in $\mathbb{Z}_p^{*p} \cong (1 + p^2\mathbb{Z}_p)$ and therefore it follows that we need to compute the unit to 2 digits of $p$-adic precision since $v_p(q) > p > 2$.*

*To decide if $s \in \mathbb{Z}_p^*$ is in fact an element of $\mathbb{Z}_p^{*p}$ we do the following: Suppose $s = s_0 + s_1 p + \ldots$, then we can express it as a product of a $p - 1^{st}$-root of unity (say $u = u_0 + u_1 p + \ldots$, which is obtained by Hensel lifting $s_0$ to a root of $x^{p-1} - 1$ in $\mathbb{Z}_p^*$) and a 1-unit ($t = t_0 + t_1 p + \ldots$). Now working modulo $p^2$, we can decide whether an element of $\mathbb{Z}_p^*$ is in $\mathbb{Z}_p^{*p} = 1 + p^2\mathbb{Z}_p$ ($\Leftrightarrow t_1 = 0$).*

Given $\Delta$, the time to compute $v_p(\Delta)$ is $\mathcal{O}(\log|\Delta| \log p)$ [vzGG03, Theorem 9.17]. Step (4) of the algorithm where we compute the $p - 1^{\text{st}}$-root of unity using Hensel lifting to 2 $p$-adic digits will cost $\mathcal{O}(\log^2 p)$ (where we work modulo $p^2$ to compute $s_0^{p-1} - 1$ since $p$ divides it).

## A.3 The complete algorithm

**Algorithm A.3.1** *An elliptic curve $E$ over $\mathbb{Q}$ given by a Weierstrass equation $y^2 = x^3 + ax + b$, with $a, b \in \mathbb{Z}$.*

*Input. We are given the coefficients of $E$ and a prime $p > 2$.*

*Output. TRUE if $\#E(\mathbb{Q}_p)[p] = p$ and FALSE if $\#E(\mathbb{Q}_p)[p] = 1$.*

1. *Compute the minimal Weierstrass equation of $E$ at $p$ using Tate's algorithm.*

2. *If $E$ has additive reduction, $p = 3$ and $\#G[3] = 3$ then using $f_3$ and either some initialization and Hensel lifting of the singular point or $p$-adic polynomial factorization algorithm determine whether $\#E(\mathbb{Q}_3)[3] = 1$ or $3$ and return FALSE, TRUE respectively.*

3. *If $E$ has split multiplicative reduction then return output of algorithm A.2.1.*

4. *Return output of algorithm A.1.1.*

The time complexity of Step 1, Tate's algorithm, is analyzed in §9. The choices for $p$-adic factorization algorithm are A. L. Chistov's deterministic algorithm or S. Pauli's randomized algorithm [Pau01]. The time complexity of the complete algorithm is a polynomial in $\log p$ and $\log H(E)$ and this completes the proof of theorem A.0.1.

# Appendix B

## Descent via 2-isogeny

*I do hope that one cornerstone of Paul's theology, if you will, will long survive. I refer to 'The Book'. 'The Book' consists of all the theorems of mathematics. For each theorem there is in 'The Book' just one proof. It is the most aesthetic proof, the most insightful proof, what Paul called 'The Book' proof.* L. Babai and J. Spencer on P. Erdős *[BS98]*

In this appendix we present our original descent analysis on the 2-isogenous elliptic curves $E$ and $E'$. We will adhere to notation introduced in §4.1.

## B.1 Structure of $S^{(\phi)}(E)$

If $-d < 0$, then $-dw^2$ is negative and $d^2 + 4pqz^4$ is not and this implies that

$$-d \notin S^{(\phi)}(E). \tag{B.1}$$

**Remark B.1.1** *Suppose $\gamma = \alpha + \beta$, where $\alpha, \beta \in \mathbb{Q}_t$ for some prime $t$. Let $v = v_t$ be the normalized valuation associated to prime $t$, that is, $v_t(t) = 1$. If $v(\alpha) \neq v(\beta)$ then*

*$v(\gamma) = \min(v(\alpha), v(\beta))$ and if $v(\alpha) = v(\beta)$ then $v(\gamma) \geq v(\alpha)$. We will repeatedly use this property of valuations in this section.*

Let $t$ denote $p$ or $q$. Suppose $(z, w) \in C_2(\mathbb{Q}_t) : w^2 = 2 + 2pqz^4$ then $2v(w) = \min(0, 1 + 4v(z))$. The scenario $v(z) < 0$ is not possible. Let us suppose $v(z) \geq 0$ then $v(w) = 0$. The congruence $w^2 \equiv 2 \bmod t$ has a solution iff $(\frac{2}{t}) = 1$ and this solution lifts to a point on $C_2$. Hence for $t = p, q$, $C_2(\mathbb{Q}_t) \neq \emptyset \Leftrightarrow t \equiv \pm 1 \bmod 8$ but this contradicts our choice of $p$ and $q$. Therefore

$$2 \notin S^{(\phi)}(E). \tag{B.2}$$

If $(z, w) \in C_p(\mathbb{Q}_q) : w^2 = p + 4qz^4$ then $2v(w) = \min(0, 1 + 4v(z))$. Assuming $v(z) < 0$ leads us to a contradiction. If $v(z) \geq 0$ then $v(w) = 0$ and hence $w^2 \equiv p \bmod q$. Therefore $C_p(\mathbb{Q}_q) \neq \emptyset \Leftrightarrow (\frac{p}{q}) = 1$.

Suppose $(z, w) \in C_p(\mathbb{Q}_p)$, then $2v(w) = \min(1, 4v(z))$. It follows that necessarily $v(z) = -i \leq 0$ which in turn implies $v(w) = 2v(z)$. Substituting $w$ and $z$ by $w'/p^{2i}$ and $z'/p^i$ respectively, we have $C''_p : w'^2 = p^{1+4i} + 4qz'^4$ with $w'$ and $z'$ units. Taking $z' = 1$ and $w'$ equal to a solution to the congruence $w'^2 \equiv 4q \bmod p$, we realize that $(z', w')$ lifts to a point in $C''_p(\mathbb{Q}_p) \Leftrightarrow (\frac{4q}{p}) = 1$. This proves that $C_p(\mathbb{Q}_p) \neq \emptyset \Leftrightarrow (\frac{q}{p}) = 1$.

Due to our choice of $p$ and $q$, $(\frac{p}{q}) = -(\frac{q}{p})$ and hence

$$p \notin S^{(\phi)}(E). \tag{B.3}$$

Similar analysis illustrates that

$$q \notin S^{(\phi)}(E). \tag{B.4}$$

It follows from the above discussion that $S^{(\phi)}(E) = \langle pq \rangle$ and Eq. 1.4 enables us to demonstrate that $Ш(E/\mathbb{Q})[\phi] = 0$.

## B.2 Structure of $S^{(\hat{\phi})}(E')$

We will proceed to compute the structure of the $S^{(\hat{\phi})}(E')$ group, working with the quartics $C'_d : dW^2 = d^2 - pqZ^4$.

Employing reasoning similar to the previous section, we obtain $C'_p(\mathbb{Q}_q)$ is non-empty $\Leftrightarrow (\frac{p}{q}) = 1$ and moreover if $(Z, W) \in C'_p(\mathbb{Q}_q)$ then $v_q(Z) \geq 0$. By analogy, $C'_p(\mathbb{Q}_p) \neq \emptyset$ is equivalent to $(\frac{-q}{p}) = 1$ and $(Z, W) \in C'_p(\mathbb{Q}_p)$ implies that $v_p(Z) \leq 0$.

Let $(Z, W) \in C'_p(\mathbb{Q}_2) : W^2 = p - qZ^4$. Suppose $v(Z) = 0$ and $v(W) = i > 0$. Substituting $W$ and $Z$ by $2^i W'$ and $Z'$ respectively, we have $2^{2i} W'^2 = p - qZ'^4$ with $W'$ and $Z'$ units. If the conditions $p - q \equiv 16, p - 17q \equiv 16, p - q \equiv 0, p - 17q \equiv 0 \bmod 32$ hold, then the congruence $2^{2i} W'^2 \equiv p - qZ'^4 \bmod 32$ has solutions $(i, Z', W')$: $(2, 1, 1)$, $(2, 3, 1)$, $(3, 1, 1)$, $(3, 3, 1)$ respectively such that $(Z', W')$ lifts to a $\mathbb{Q}_2$-point.

This leads to

$$(\frac{p}{q}) = (\frac{-q}{p}) = 1 \text{ and } p \equiv q \bmod 16 \Rightarrow p \in S^{(\hat{\phi})}(E') \tag{B.5}$$

By symmetry, $q \in S^{(\hat{\phi})}(E')$ under conditions identical to above statement with the roles of $p$ and $q$ being reversed.

Also for $t = p, q$, $C'_{-1}(\mathbb{Q}_t) \neq \emptyset \Leftrightarrow t \equiv 1 \bmod 4$, which contradicts our selection of $p$ and $q$. Therefore

$$-1 \notin S^{(\hat{\phi})}(E'). \tag{B.6}$$

Next if $(Z, W) \in C'_{-2}(\mathbb{Q}_2) : -2W^2 = 4 - pqZ^4$ then $1 + 2v(W) = \min(2, 4v(Z))$, which is a contradiction and we have illustrated that

$$-2 \notin S^{(\hat{\phi})}(E'). \tag{B.7}$$

Similarly,

$$2 \notin S^{(\hat{\phi})}(E'). \tag{B.8}$$

It is a fact that $(\frac{p}{q}) = -(\frac{q}{p})$, since $p \equiv q \equiv 3 \bmod 4$. Let us assume *without loss of generality* that $(\frac{p}{q}) = 1$. This implies $(\frac{-q}{p}) = (\frac{-1}{p})(\frac{q}{p}) = 1$, since $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$.

By Eq. B.5, $p \in S^{(\hat{\phi})}(E')$ and as $-pq \in S^{(\hat{\phi})}(E')$ (Eq. 4.1), $-q \in S^{(\hat{\phi})}(E')$ and we have proved that $S^{(\hat{\phi})}(E') = \langle p, -q \rangle$.

## B.3 An elliptic curve of conjectural rank 1

The purpose of this section is to prove that the elliptic curve of interest has rank 1 under certain assumptions. Utilizing techniques inspired by the ones used in proving Proposition X.6.2(c) [Sil92], we obtain

$$\begin{aligned} r_E + \dim_2 Ш(E'/\mathbb{Q})[\hat{\phi}] &= \dim_2 S^{(\phi)}(E) + \dim_2 S^{(\hat{\phi})}(E') - 2 \\ &= 1. \end{aligned}$$

where $\dim_2$ is the dimension as a $\mathbb{Z}/2\mathbb{Z}$-vector space. In particular,

$$r_E \leq 1. \tag{B.9}$$

Next, we will investigate the zeros of the $L$-function of $E$ at $s = 1$. The global root number $w(E)$ can be computed from the local root numbers: $w(E) = \prod_{p\leq\infty} w_p(E)$, where $w_p(E) = \pm 1$ and equal to 1 for the primes of good reduction, $-1$ for $p = \infty$. Hence $w(E) = -\prod_{p|\Delta} w_p(E)$.

We will use the formulae presented in [Riz03] to compute the local root numbers of the elliptic curve.

**Lemma B.3.1** *Let $E : y^2 = x^3 - pqx$ be an elliptic curve over $\mathbb{Q}$ with $p, q$ distinct primes such that $p \equiv q \equiv 3 \bmod 16$. Then $w(E) = -1$.*

**Proof B.3.1** *We begin by listing some properties and invariants of $E$, which will play a role in the root number computation. The discriminant of $E$, $\Delta(E) = 2^6p^3q^3$, $c_4 = 48pq$,*

$c_6 = 0$, *additive type III reduction at* $2; p; q$. $E$ *has potential good reduction everywhere as* $j(E) = 1728$.

*Let* $t$ *be either* $p$ *or* $q$. *Suppose* $t > 3$ *then* $e_t = \frac{12}{\gcd(v_t(\Delta),12)} = 4$ *and from the formulae [Riz03, Fact 3],* $w_t(E) = (\frac{-2}{t}) = (\frac{-1}{t})(\frac{2}{t}) = -1 \cdot -1 = 1$. *If* $t = 3$, *then [Riz03, Table II] states that* $w_3(E) = 1$.

*To calculate* $w_2(E)$ *we need the following data:* $c_4' = 3pq$, $c_4' \equiv 3 \bmod 4$, $c_4' \equiv 11 \bmod 16$ *and* $c_{6,7} = 0$. *Referring to [Riz03, Table III], since* $c_4' - 4c_{6,7} \equiv 11 \bmod 16$, *we have demonstrated that* $w_2(E) = 1$.

*Therefore* $w(E) = -1 \cdot w_2(E) \cdot w_p(E) \cdot w_q(E) = -1$.

**Lemma B.3.2** *Let* $E$ *be the same as in lemma B.3.1. Assuming* $r_E^{an} = 1$ *(or alternatively the BSD conjecture),* $r_E = 1$.

**Proof B.3.2** *Plugging in the value of the root number into Eq. 1.3, the functional equation of* $\Lambda_E(s)$ *and taking* $s = 1$ *we have* $\Lambda_E(1) = -\Lambda_E(1)$ *and hence* $\Lambda_E(1) = 0$. *This implies that* $L_E(1) = 0$. *In other words,*

$$r_E^{an} > 0. \tag{B.10}$$

*Recall that* $r_E \leq 1$ *(Eq. B.9). Now assuming* $r_E^{an} = 1$ *[Kol90], (or assuming the BSD conjecture) we can conclude that*

$$r_E = 1. \tag{B.11}$$

## B.4 Generator of $E_D(\mathbb{Q})$

We have shown that $S^{\hat{\phi}}(E') = \{1, p, -q, -pq\}$ (assuming $(\frac{p}{q}) = 1$), that is, for each $d \in S^{\hat{\phi}}(E')$ the homogeneous space $C'_d$ has a point in every completion of $\mathbb{Q}$. Also there is a map from $C'_d$ to $E$, given by $(Z, W) \mapsto (\frac{d}{Z^2}, \frac{dW}{Z^3})$. As $r_E = 1$, we have $\dim_2 Ш(E'/\mathbb{Q})[\hat{\phi}] = 0$, that is, these quartics have $\mathbb{Q}$-points. In particular, on $E$ we have the rational points $R_1 := (\frac{p}{Z_1^2}, \frac{pW_1}{Z_1^3})$, where $v_p(Z_1) \leq 0, v_q(Z_1) \geq 0$ and $R_2 := (\frac{-q}{Z_2^2}, \frac{-qW_2}{Z_2^3})$, where $v_p(Z_2) \geq 0, v_q(Z_2) \leq 0$. The other elements of the Selmer group give rise to $O$ and $(0,0)$ respectively.

Let $E(\mathbb{Q}) = \langle T \rangle + \mathbb{Z}P$, where $T = (0,0)$. Though it is not clear whether $P$ is in the image of the map $C'_d \to E$, we will proceed to show that the integers $v_p(x(P))$, $v_q(x(P))$ are not the same and this will help us to factor $pq$.

We remark that if $R$ is a rational point on $E$, $R \neq O, T$ then using the group law formulae we arrive at the identity $x(R) \cdot x(R+T) = -pq$. This observation will be useful as we know that for $i = 1, 2$, $R_i = k_iP + l_iT$, for some $k_i \in \mathbb{Z}$, where $l_i = 0$ or $1$.

1. Let $v_p(x(P)), v_q(x(P)) \leq 0$, that is, $P$ reduces to a non-singular point on the reduced curve modulo $p$ and $q$. Then for all $k \in \mathbb{Z}$, $v_p(x(kP))$, $v_q(x(kP)) \leq 0$, which is not possible, since $R_1, R_2$ are not of the form $kP$ or $kP + T$.

2. Let $v_p(x(P)) = m, v_q(x(P)) = n$ $m, n \geq 1$. Recall that the component group at $p$ and $q$ is $\mathbb{Z}/2\mathbb{Z}$. First, let us suppose that $k \in \mathbb{Z}$ is even. Then $kP$ reduces to a non-singular point modulo $p$ and $q$ and we head towards a contradiction due to reasons similar to the previous case. If $k$ is odd, $kP$ reduces to the singular point

$(0,0)$ on the reduced curve modulo $p$ and $q$. This implies $kP \neq R_1$ or $R_2$. If $m = n$, then $x(kP+T) \neq x(R_1), x(R_2)$. And hence the case we are left with is $m \neq n$.

3. In the last scenario, $v_p(x(P)) \geq 1, v_q(x(P)) \leq 0$ and these numbers are different.

The above discussion proves that the x-coordinate of a generator of $E$ behaves differently with respect to $v_p$ and $v_q$.

# Appendix C

## Brauer-Siegel Ratio Graphs

*Much of the information in these notes is the result of machine computation; however the theoretical basis of these computations is not always trivial.*

B. J. Birch and H. P. F. Swinnerton-Dyer *[BSD63]*

In this appendix we tabulate computation driven by the questions and conjectures of Chapter 3. Specifically, we computed the Brauer-Siegel ratio of $E$,

$$BSR(E) := \frac{\log(\#\text{Ш}(E) \cdot Reg(E))}{12 \cdot h^*(E)} \tag{C.1}$$

and graphed the data on the basis of the ranks of the elliptic curves. The curves considered were those in existing databases [Cre], [SW02], and certain rank 0 elliptic curves.

Note that explicit computation can be misleading when an attempt is made to predict the growth of the functions using the generated data. The following graphs neither refute nor confirm the conjectures of Chapter 3, in particular the Brauer-Siegel analogue for elliptic curves (Conjecture 3.1.2), which in the new notation succinctly reads:

$$BSR(E) \sim \frac{1}{12} = 0.08333\ldots \tag{C.2}$$

**Notation** The histograms which follow were generated using the Matplotlib/pylab library via SAGE [Gro] with number of bins set to 1000 for the ones in §C.1, §C.2 and 10000 for the others. SAGE invokes the PARI/GP library [ABC$^+$] to compute elliptic curve information like Fourier coefficients, etc. Computations were performed on the `sage.math.washington.edu` and `meccah.math.harvard.edu` computers. The $x$ and $y$ axes denote the BSR values and the number of elliptic curves respectively. The way to interpret axes, which are labeled by $\times 1ec$, where $c$ is an integer, is a follows: each entry on an axis should be multiplied by $10^c$. For example, $\times 1e - 1$ denotes that entries should be divided by 10.

In the limited data we consider, the number of rank 0 elliptic curves with $Ш_{an} = O$ dominates the number of rank 0 curves with nontrivial Shafarevich-Tate group. As a result a histogram plotting BSR values for Mordell-Weil rank 0 elliptic curves barely illustrates the distribution of BSR's for curves with nontrivial Shafarevich-Tate group. And for this reason we resort to a second histogram, which "zooms in" on the curves with $\#Ш_{an} > 1$. The subscript *an* refers to the quantity being computed "analytically" via the BSD conjectural formula and $\#Ш_{an}(E)$ is called the *analytic order* of the Shafarevich-Tate group.

Assuming the Brauer-Siegel analogue one would expect that among the rank 0 elliptic curves the proportion of ones with $Ш_{an} = O$ would decrease as elliptic curves of larger naïve height are computed and eventually the proportion would drop to 0. Moreover, there would be no elliptic curves with trivial Shafarevich-Tate group above a certain elliptic curve naïve height bound (see §3.3). An interesting future project could be to graph this phenomena using existing databases and families of rank 0 elliptic curves.

A related project would be to produce explicit examples of elliptic curves with big Ш's. Consider a family of rank 0 elliptic curves $E$ parameterized by certain primes $p$, such that conjecturally $\#Ш(E)$ is essentially about $p^{\kappa}$, for some positive constant $\kappa$. Sections C.1 and C.2 introduce elliptic curves $E_p : y^2 = x^3 + px$ and Neumann-Setzer curves which have $\kappa = \frac{1}{4}$ assuming the BSD formula and conjectural bounds for $L_E(1)$. In the same vein, the elliptic curves $C(p^3) : y^2 = x^3 + p^3x$, and $y^2 = x^3 + p^5$ have $\kappa$ equal to $\frac{3}{4}$ and $\frac{5}{6}$ respectively. (See [Ros00] for examples of elliptic curves $C(p^3)$ with large Ш's.) The strategy for the project would be to choose families of rank 0 elliptic curves with large values of $\kappa$ and compute the analytic orders of their Shafarevich-Tate groups.

## C.1 $E_p : y^2 = x^3 + px$

Let us consider the elliptic curves $E_p : y^2 = x^3 + px$, where $p \equiv 7, 11 \bmod 16$. These are elliptic curves with $\Delta(E_p) = -2^6 \cdot p^3$, $N(E_p) = 2^5 \cdot p^2$, $E_p(\mathbb{Q})_{tors} = \{O, (0,0)\}$, $\prod_l c_l(E_p) = c_2(E_p) \cdot c_p(E_p) = 2^2$, and $\Omega(E_p) = \frac{\pi \cdot p^{\frac{-1}{4}}}{AGM(\sqrt{i}, \sqrt{-i})}$ [Cre97, §3.7]. Moreover, the Mordell-Weil rank is 0 and $Ш(E_p)[2] = 0$ [Sil92, Corollary 6.2.1].

Table C.1: Distribution of $\#\text{Ш}_{an}(E_p)$

| $\#\text{Ш}_{an}(E_p)$ | $1^2$ | $3^2$ | $5^2$ | $7^2$ | $9^2$ | $11^2$ | $13^2$ | $15^2$ | $17^2$ |
|---|---|---|---|---|---|---|---|---|---|
| $\#E_p$ | 11004 | 5314 | 2022 | 762 | 351 | 131 | 48 | 10 | 5 |

Table C.2: Smallest prime $p$ such that $\#\text{Ш}_{an}(E_p)$ has a prescribed value

| $p$ | $\#\text{Ш}_{an}(E_p)$ | $BSR(E_p)$ |
|---|---|---|
| 727 | $3^2$ | 0.0700190502702 |
| 3767 | $5^2$ | 0.0886359156938 |
| 10007 | $7^2$ | 0.0991629353885 |
| 27767 | $9^2$ | 0.10386702724 |
| 63127 | $11^2$ | 0.107115090889 |
| 145547 | $13^2$ | 0.108504145639 |
| 583127 | $15^2$ | 0.10528540048 |
| 590267 | $17^2$ | 0.110073455194 |

Substituting the above values into the BSD formula (Eq. 1.6) gives us

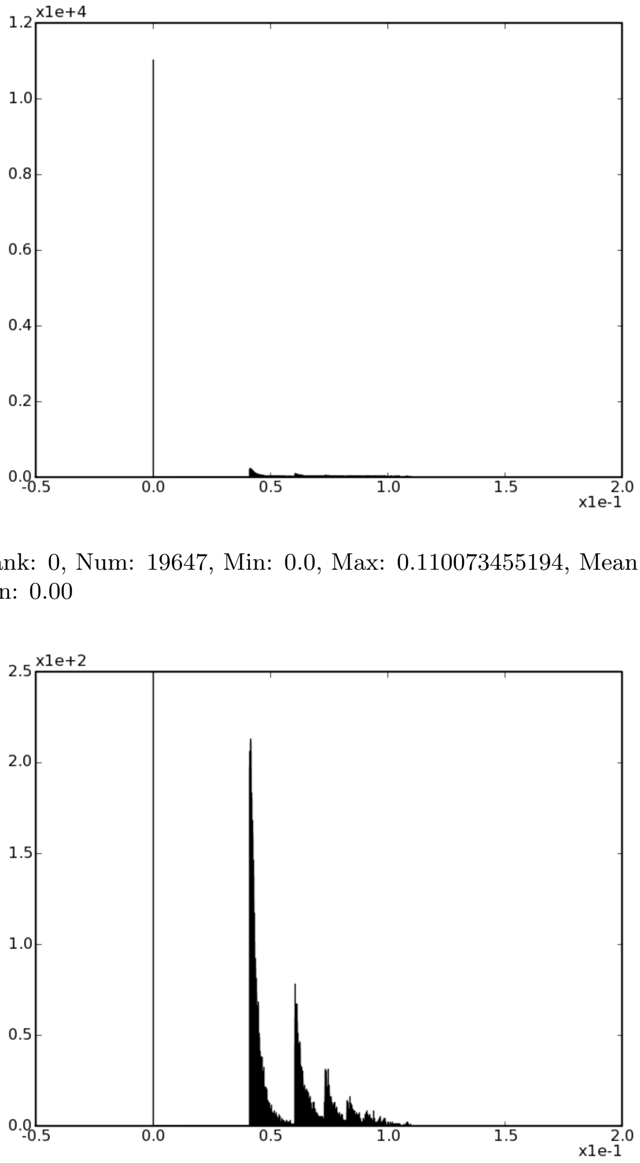
$$\#\text{Ш}(E_p) = \frac{L_{E_p}(1)}{\Omega(E_p)} = L_{E_p}(1) \cdot p^{\frac{1}{4}} \cdot \frac{AGM(\sqrt{2},1)}{\pi \cdot \sqrt{2}} \tag{C.3}$$

Applying the conjectural bounds of Hindry for $L_{E_p}(1)$ (Eq. 3.20), we arrive at

$$p^{\frac{1}{4}-\epsilon} \ll \#\text{Ш}(E_p) \ll p^{\frac{1}{4}+\epsilon}. \tag{C.4}$$

The above discussion illustrates the conjectural role played by the period in giving shape to the size of the Shafarevich-Tate group in this family of elliptic curves.

We graph BSR data for the 19647 curves $E_p$ with $p < 10^6$ in Figures C.1(a) and C.1(b). The size of the Shafarevich-Tate group $\#\text{Ш}_{an}(E_p)$ was computed using Eq. C.3. Tables C.1 and C.2 present some statistics related to $\#\text{Ш}_{an}(E_p)$.



(a) Rank: 0, Num: 19647, Min: 0.0, Max: 0.110073455194, Mean: 0.02, Median: 0.00

(b) Rank: 0, Num: 19647, Min: 0.0, Max: 0.110073455194, Mean: 0.02, Median: 0.00

Figure C.1: BSR distribution for rank 0 elliptic curves $E_p$

## C.2 Neumann-Setzer curves

Let us consider the elliptic curves $E_0 : y^2+xy = x^3-\frac{u+1}{4}x^2+4x-u$, where $p = u^2+64$ is a prime for some integer $u$, which we take to be 3 modulo 4. They are infinitely many such primes assuming Hardy-Littlewood's F conjecture [HL23]. These are elliptic curves with $\Delta(E_0) = -p^2$, $N(E_0) = p$, $E_0(\mathbb{Q})_{tors} = \mathbb{Z}/2\mathbb{Z}$, $c_4(E_0) = p - 256$, $c_6(E_0) = u \cdot (p + 512)$, the Mordell-Weil rank is 0 and $\text{Ш}(E_0)[2] = 0$ [SW04]. Moreover, the Tamagawa number $c_p(E_0) = \nu_p(\Delta(E_0)) = 2$ and the naïve height $h^*(E_0) \sim \log p^{\frac{1}{4}}$ as $p \to \infty$.

There is a 2-isogenous elliptic curve of $E_0$ given by $E_1 : y^2 + xy = x^3 - \frac{u+1}{4}x^2 - x$, where $u$ and $p$ are as defined above. They satisfy the following properties: $\Delta(E_1) = N(E_1) = p$, $E_1(\mathbb{Q})_{tors} = \mathbb{Z}/2\mathbb{Z}$, $c_4(E_1) = p - 16$, $c_6(E_1) = u \cdot (p + 8)$, the Mordell-Weil rank is 0 and $\text{Ш}(E_1)[2] = 0$. Note that $L_{E_0}(1) = L_{E_1}(1)$, since Fourier coefficients are identical for isogenous curves and $\Omega(E_0) = \Omega(E_1)$ keeping in mind that $E_0(\mathbb{R})$ is connected, whereas $E_1(\mathbb{R})$ is not. However, since $\#\text{Ш}_{an}(E_1) = \#\text{Ш}_{an}(E_0)$ under the BSD conjectural formula (rank 0), we restrict our attention to the elliptic curves $E_0$.

Substituting the values for the terms in the BSD formula (Eq. 1.6) results in

$$\#\text{Ш}(E_0) = \frac{L_{E_0}(1) \cdot 2}{\Omega(E_0)} \tag{C.5}$$

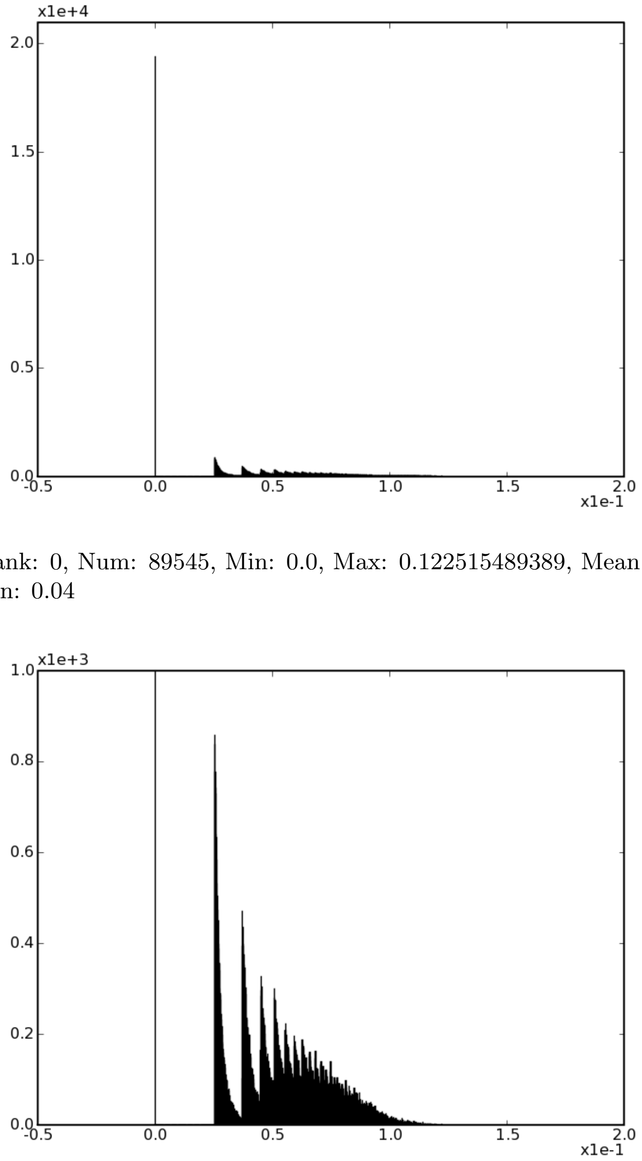
Replacing $\Omega(E_0)$ using Eq. 3.18 and utilizing the conjectural bounds of Hindry for $L_{E_0}(1)$ (Eq. 3.20), we arrive at

$$p^{\frac{1}{4}-\epsilon} \ll \#\text{Ш}(E_0) \ll p^{\frac{1}{4}+\epsilon}. \tag{C.6}$$

Table C.3: Distribution of $\#Ш_{an}(E_0)$

| $\#Ш_{an}$ | # | $\#Ш_{an}$ | # | $\#Ш_{an}$ | # | $\#Ш_{an}$ | # | $\#Ш_{an}$ | # |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 19417 | 961 | 667 | 3721 | 81 | 8281 | 18 | 14641 | 1 |
| 9 | 16605 | 1089 | 697 | 3969 | 85 | 8649 | 5 | 15129 | 3 |
| 25 | 11263 | 1225 | 500 | 4225 | 64 | 9025 | 8 | 15625 | 1 |
| 49 | 8216 | 1369 | 385 | 4489 | 46 | 9409 | 2 | 16129 | 1 |
| 81 | 6890 | 1521 | 461 | 4761 | 44 | 9801 | 2 | 16641 | 2 |
| 121 | 4587 | 1681 | 287 | 5041 | 26 | 10201 | 5 | 17161 | 1 |
| 169 | 3623 | 1849 | 223 | 5329 | 18 | 10609 | 5 | 17689 | 1 |
| 225 | 3440 | 2025 | 323 | 5625 | 30 | 11025 | 11 | 18225 | 2 |
| 289 | 2306 | 2209 | 205 | 5929 | 26 | 11449 | 4 | 19881 | 3 |
| 361 | 1892 | 2401 | 154 | 6241 | 23 | 11881 | 2 | 21609 | 1 |
| 441 | 1900 | 2601 | 184 | 6561 | 28 | 12321 | 3 | 22801 | 1 |
| 529 | 1224 | 2809 | 120 | 6889 | 24 | 12769 | 4 | 24649 | 1 |
| 625 | 1152 | 3025 | 109 | 7225 | 15 | 13225 | 1 | | |
| 729 | 1115 | 3249 | 104 | 7569 | 15 | 13689 | 1 | | |
| 841 | 787 | 3481 | 82 | 7921 | 10 | 14161 | 3 | | |

We graph BSR data for the 89545 curves $E_0$ with $p < 3 \cdot 10^{12}$ in Figures C.2(a) and C.2(b). The size of the Shafarevich-Tate group $\#Ш_{an}(E_0)$ is computed using Eq. C.5 and Table C.3 presents the distribution of $\#Ш_{an}(E_0)$.



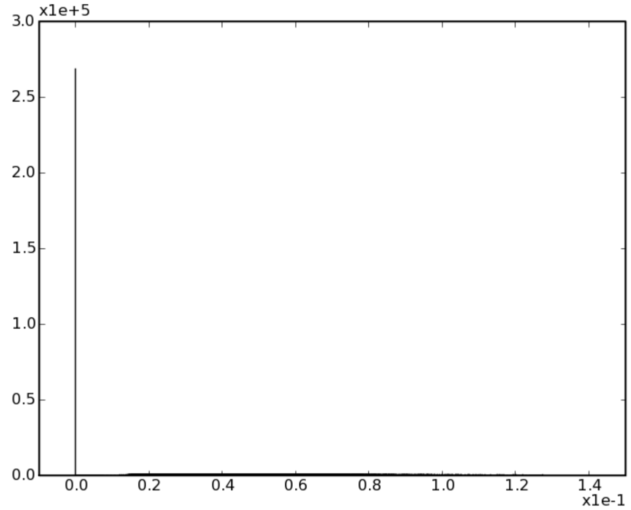
(a) Rank: 0, Num: 89545, Min: 0.0, Max: 0.122515489389, Mean: 0.04, Median: 0.04

(b) Rank: 0, Num: 89545, Min: 0.0, Max: 0.122515489389, Mean: 0.04, Median: 0.04

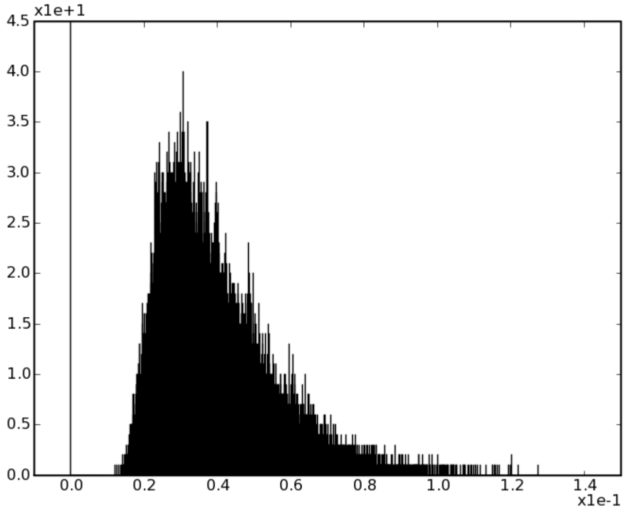
Figure C.2: BSR distribution for rank 0 Neumann-Setzer elliptic curves $E_0$

## C.3 Cremona database

The `allbsd` database [Cre] of J.E. Cremona lists elliptic curves of conductor upto $120,000$ along with terms appearing in the BSD conjecture. We used the regulator and the size of the Shafarevich-Tate group of each of these curves and plotted their BSR values.

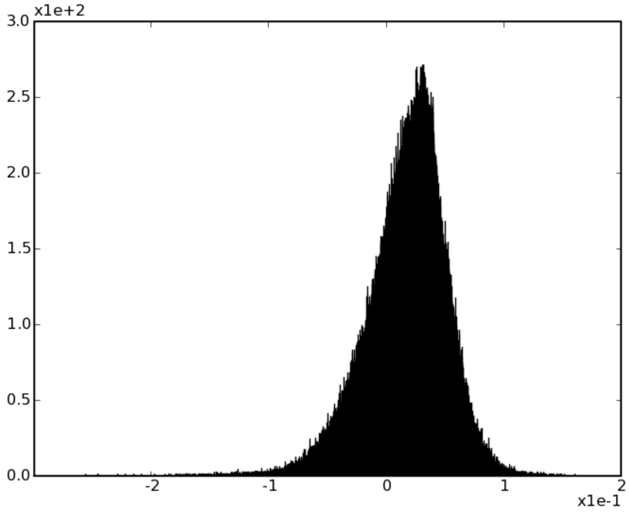


(a) Rank: 0, Num: 316414, Min: 0, Max: 0.127420362791, Mean: 0.01, Median: 0.0



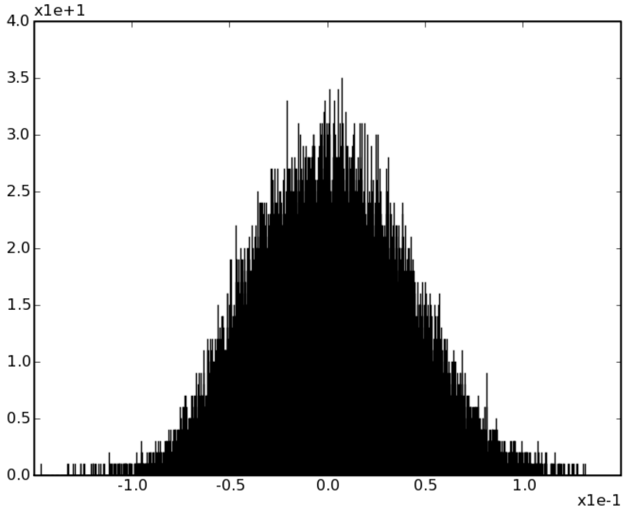
(b) Rank: 0, Num: 316414, Min: 0, Max: 0.127420362791, Mean: 0.01, Median: 0.0

Figure C.3: BSR distribution for rank 0 elliptic curves in the Cremona database



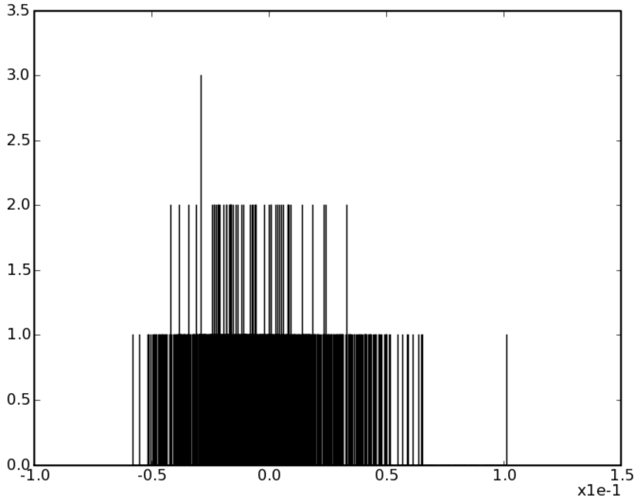
(a) Rank: 1, Num: 394879, Min: $-0.256057275686$, Max: 0.160553198649, Mean: 0.02, Median: 0.02

Figure C.4: BSR distribution for rank 1 elliptic curves in the Cremona database



(a) Rank: 2, Num: 70364, Min: $-0.146418977933$, Max: 0.131757300745, Mean: 0.0, Median: 0.0

Figure C.5: BSR distribution for rank 2 elliptic curves in the Cremona database



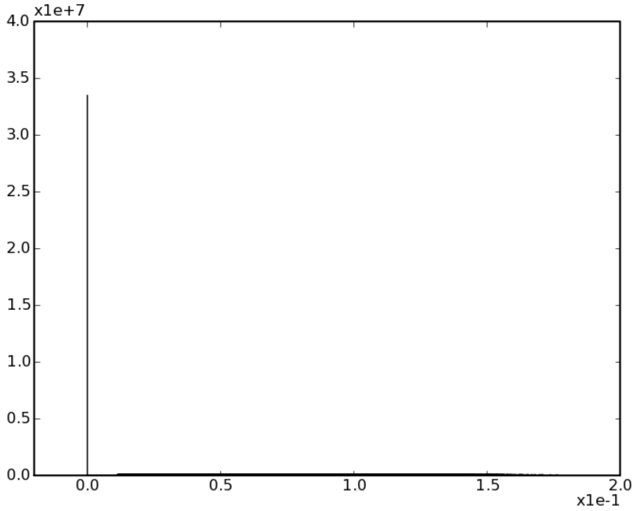
(a) Rank: 3, Num: 836, Min: $-0.0579331293169$, Max: 0.101373726334, Mean: 0.0, Median: $-0.01$

Figure C.6: BSR distribution for rank 3 elliptic curves in the Cremona database

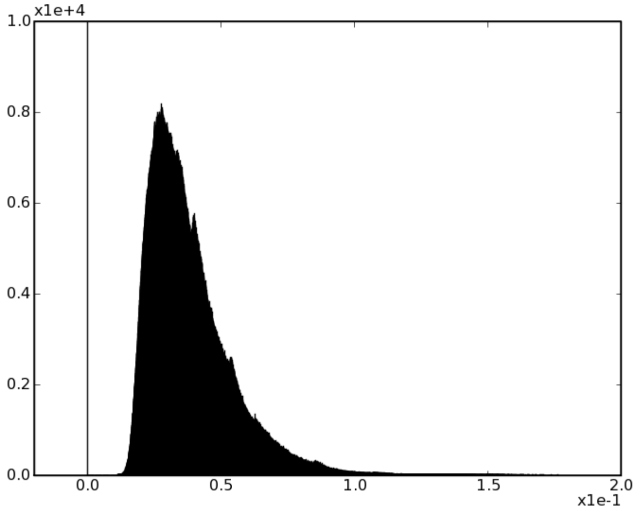
## C.4 Stein-Watkins database

The database of W.A. Stein and M.J. Watkins [SW02] lists $136,924,520$ elliptic curves of conductor at most $10^8$ along with $L_E^*(1)$ the leading coefficient of the Taylor expansion of $L_E(s)$ at $s = 1$. For each conductor and each isogeny class the database lists the rank and $L_E^*(1)$ and the curves in that isogeny class. (Recall that BSD conjecture is isogeny invariant, that is, each curve in an isogeny class have the same rank and $L_E^*(1)$.)

Our SAGE script iterates through each elliptic curve $E$ in an isogeny class and computes $BSR(E)$ by determining $Reg(E) \cdot \#Ш(E)$ via the BSD formula using the $L_E^*(1)$ value supplied by the database. The SAGE documentation notes that the Stein-Watkins database unlike the Cremona database need not list all curves of a given conductor and that it lists the curves whose coefficients are not *too large* [SW02].

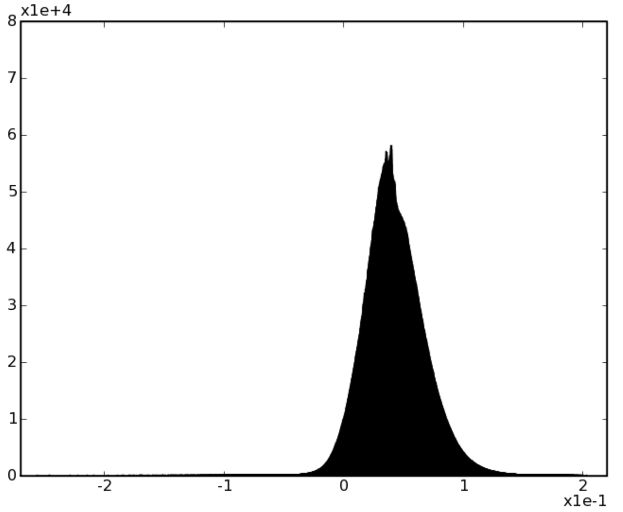


(a) Rank: 0, Num: 45976073, Min: $-4.76990360214e - 06$, Max: 0.176325563645, Mean: 0.01, Median: 0.0



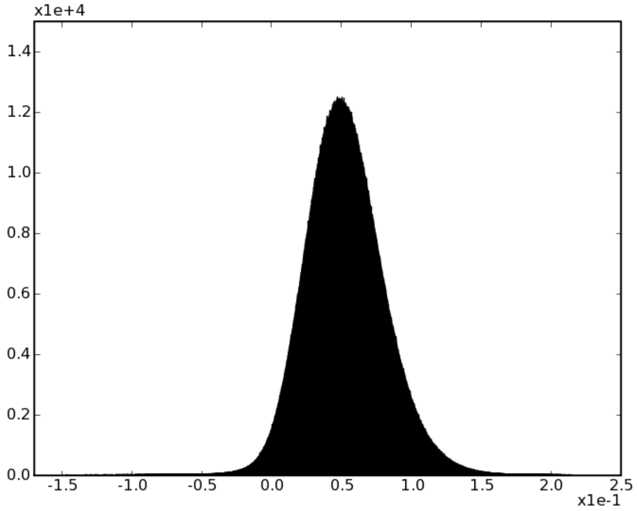
(b) Rank: 0, Num: 45976073, Min: $-4.76990360214e-06$, Max: 0.176325563645, Mean: 0.01, Median: 0.0

Figure C.7: BSR distribution for rank 0 elliptic curves in the Stein-Watkins database



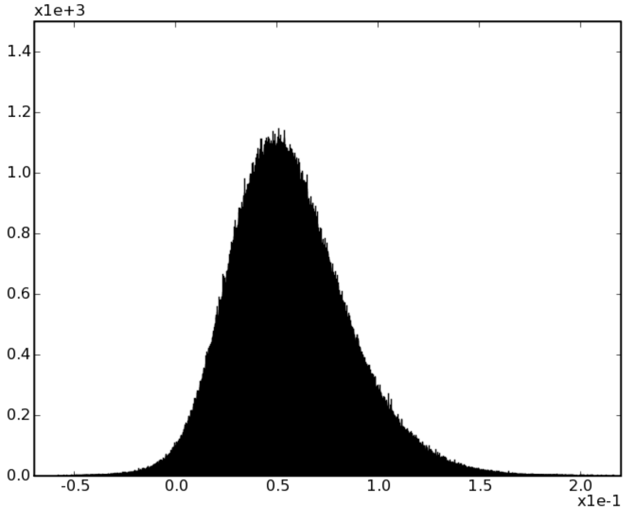
(a) Rank: 1, Num: 65944408, Min: $-0.256057212045$, Max: 0.203168866846, Mean: 0.04, Median: 0.04

Figure C.8: BSR distribution for rank 1 elliptic curves in the Stein-Watkins database



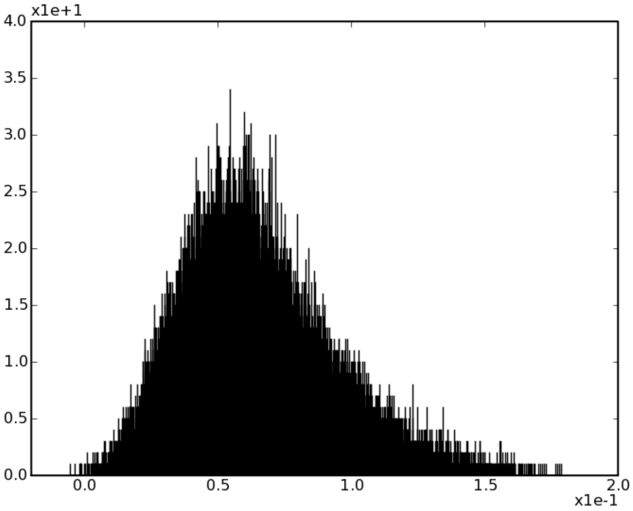
(a) Rank: 2, Num: 22372931, Min: −0.146418951508, Max: 0.214677375035, Mean: 0.05, Median: 0.05

Figure C.9: BSR distribution for rank 2 elliptic curves in the Stein-Watkins database



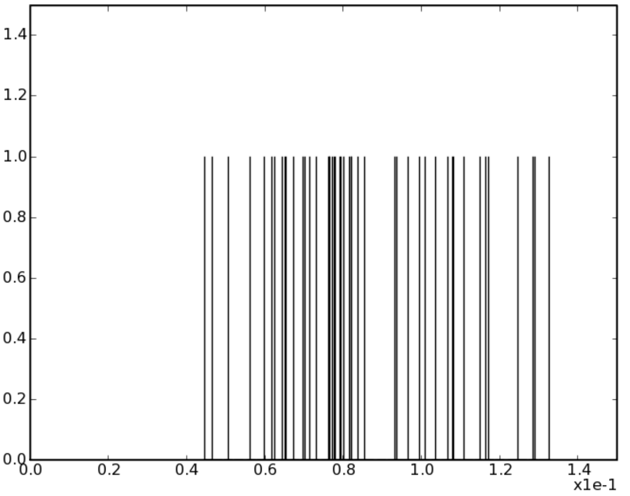
(a) Rank: 3, Num: 2571123, Min: −0.057933129036, Max: 0.216282436936, Mean: 0.06, Median: 0.05

Figure C.10: BSR distribution for rank 3 elliptic curves in the Stein-Watkins database



(a) Rank: 4, Num: 59940, Min: −0.00529790776879, Max: 0.179020653443, Mean: 0.06, Median: 0.06

Figure C.11: BSR distribution for rank 4 elliptic curves in the Stein-Watkins database



(a) Rank: 5, Num: 45, Min: 0.044667548058, Max: 0.132783309048, Mean: 0.09, Median: 0.08

Figure C.12: BSR distribution for rank 5 elliptic curves in the Stein-Watkins database

*I don't know what I may seem to the world. But as to myself I seem to have been only like a boy playing on the seashore and diverting myself now and then finding a smoother pebble or a prettier shell than the ordinary, whilst the great ocean of truth lay all undiscovered before me.* I. Newton

# Index