On Computing the Tate-Shafarevich group order and type of some rational elliptic curves of conductor less than a million.

Gerardo E. Zelaya Eufemia

A dissertation
submitted in partial fulfillment of the
requirements for the degree of

Doctor of Philosophy

University of Washington

2019

Reading Committee:

William Stein, Chair

Ralph Greenberg

Bianca Viray

Program Authorized to Offer Degree:
Mathematics

University of Washington

Abstract

On Computing the Tate-Shafarevich group order and type of some rational elliptic curves of conductor less than a million.

Gerardo E. Zelaya Eufemia

Chair of the Supervisory Committee:
Professor William Stein
Department of Mathematics

In this dissertation, I will present the tabulation of the Tate-Shafarevich group order and type of around 4.5 million rational elliptic curves of conductor less than a million. These curves were obtained from the database of Cremona and that of Stein and Watkins, and I assumed standard conjectures including the Birch and Swinnerton-Dyer standard and p-adic conjectures and the Generalized Riemann Hypothesis.

I also predict how far we are from witnessing Delaunay's asymptotic proportions on the order valuations and ranks of their Tate-Shafarevich groups.

ACKNOWLEDGMENTS

First of all, I want to express sincere admiration and eternal gratitude to my adviser Prof. William Stein.

I also wish to express sincere gratefulness to the Math Department of the University of Washington, the professors and the staff for their invaluable teachings and support, but mostly thanks to my committee members Prof. Greenberg and Prof. Viray.

I also want to thank C. M. Canjura and my M.S. adviser Prof. Chad Sprouse for motivating him to enter into this program.

Finally, I thank C. Geiger and Dr. Kevin Lui at UW, and A. Yassine at UC Riverside for their academic support and friendship.

DEDICATION

To my beloved wife Katherine, to my dear parents Edgar and Ligia, and to the memory of my grandmother Rosa.

NOTATION

The main object of this dissertation is the order of the Tate-Shafarevich group of a rational elliptic curve, which I will denote by $\text{sha}(E) := \#Ш(E/\mathbb{Q})$. Since I am assuming the standard Birch Swinnerton-Dyer conjecture and using the p-adic Birch Swinnerton-Dyer conjecture for primes of good ordinary reduction as described in [SW13], for any elliptic curve E, I will denote the leading coefficient of its L-series by $\text{lc}(E) := \frac{L^{(r)}(E,1)}{r!}$, the torsion subgroup order by $\text{tor}(E) := \#E(\mathbb{Q})_{\text{tor}}$, the product of its Tamagawa numbers by $\text{tam}(E) = \prod_p \tau_p$, the regulator of the elliptic curve by $\text{reg}(E)$ and the p-adic regulator by $\text{reg}_p(E)$, the rank of its Mordell-Weil group by $\text{rank}(E) = \text{rank}(E(\mathbb{Q}))$, its Cremona-Prickett-Siksek height bound by $\text{cps}(E)$ and the naive point search bound used in my computations as $\text{cps}(E)$. Finally, I will denote the $\mathbb{F}_2$-rank of the 2-torsion part of the Tate-Shafarevich group by $r_2Ш(E) = \text{rank}_{\mathbb{F}_2} Ш(E/\mathbb{Q})[2]$ and the $\mathbb{F}_3$-rank of the 3-torsion part of the Tate-Shafarevich group by $r_3Ш(E) = \text{rank}_{\mathbb{F}_3} Ш(E/\mathbb{Q})[3]$. Throughout I will refer to any of these elements in general without denoting the elliptic curve E. For example, sha or $\#Ш$ or $\#Ш(E/\mathbb{Q})$ is the corresponding order of the Tate-Shafarevich group of any elliptic curve in any subset of the ones studied. Additionally, I will denote ord_p to be the p-valuation of a rational number or a p-adic number. Finally, many proportions will be presented as the number of elliptic curves per million, which I abbreviated as "npm" and should not be confused with the JavaScript tool package manager.

TABLE OF CONTENTS

Chapter 1

PRELIMINARY KNOWLEDGE

1.1 Elliptic curves over the rational numbers

Following [Sil09, Ch.III], an elliptic curve E is a smooth projective curve of genus one with a specified base point O_E. Geometrically, it is represented by the locus in the projective plane $\mathbb{P}^2$ of a non-singular Weiestrass equation of the form

$$E : Y^2 + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

where

$$O_E = (0 : 1 : 0)$$

and the coefficients a_i's are called the defining a-invariants of the curve. In this dissertation, I am mainly interested in elliptic curves with coefficients on $\mathbb{Q}$ also called rational elliptic curves, and unless otherwise specified I will assume this.

Other relevant invariants attached to an elliptic curve E are its b-invariants:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= a_1a_3 + 2a_4 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_162a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2 \end{aligned}$$

its c-invariants:

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

its discriminant, its j-invariant, and its invariant differential:

$$\begin{aligned} \Delta(E) &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ j(E) &= c_4^3/\Delta \\ \omega_E &= \frac{dx}{2y+a_1x+a_3} = \frac{dy}{3x^2+2a_2x+a_4-a_1y} \end{aligned}$$

The main interest of elliptic curves is to identify its rational points or rational solutions to its Weierstrass equation. Mordel and Weil showed that the set of rational points of an elliptic curve form a finitely generated abelian group $E(\mathbb{Q})$ called its Mordell Weil group, where three points add up to its identity 0_E if they belong to the same line. Thus $E(\mathbb{Q}) \cong \mathbb{Z}^r \times E(\mathbb{Q})_{tor}$, where r is called its algebraic rank. The **Nagell-Lutz's theorem** helps to compute the torsion points on a given elliptic curve, and in 1978 Mazur classified all possible torsion subgroups for rational elliptic curves. In particular, he showed that

$$E(\mathbb{Q})_{tor} = \begin{cases} \mathbb{Z}/n & 1 \leq n \leq 10 \text{ or } n = 12 \\ \mathbb{Z}/2 \times \mathbb{Z}/2n & 1 \leq n \leq 4 \end{cases}$$

Remarkably, in 1996 Loic Merel proved the generalization to number fields by showing the boundedness of the torsion subgroup of elliptic curves over any number field.

Among the most relevant homomorphisms between elliptic curves, one is interested in **Isogenies**, which are surjective group homomorphisms $\phi : E \to E'$ with finite kernel. The most common algorithm to compute isogenies are **Velu's formulas** and alternatively **Kohel's algorithm**, see [Koh96]. They return the equations of these morphisms and that of the codomain elliptic curve E' from the equation of the domain elliptic curve E and the kernel.

Moreover, in this dissertation, I am interested in rational isomorphic classes of elliptic curves whose Weiestrass equations are related by a change of coordinates of the form:

$$(x, y) = (u^2x' + r, u^3y' + u^2sx' + t)$$

for some $u, r, s, t \in \mathbb{Q}$ and $u \neq 0$. The short Weierstrass equation of an elliptic curve is the class representative of the form:

$$E : Y^2Z = X^3 + AXZ^2 + BZ^3$$

For a list of equations that represent elliptic curves and hence can be transformed to this canonical form see [Cas91, Ch.VIII].

1.1.1 *Elliptic curves over the complex field.*

A classical interpretation of elliptic curves over $\mathbb{Q}$ identifies them as Tori in $\mathbb{C}$ of the form $\mathbb{C}/\Lambda$, where $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ is a lattice in $\mathbb{C}$. Here, the Weiestrass $\mathcal{P}$-function associated to a lattice in $\mathbb{C}$ provides the coordinates of the points satisfying the Weiestrass equation of the elliptic curve, see [Sil09, §VI.3].

$$[z] \in \mathbb{C}/\Lambda \mapsto (\mathcal{P}_\Lambda(z) : \mathcal{P}'_\Lambda(z) : 1) \in E(\mathbb{C})$$

For the reverse map, one finds the basis of the Lattice by integrating the invariant differential of E on a basis of $H^1(E(\mathbb{C}), \mathbb{Z})$. Two elliptic curves over $\mathbb{C}$ are isomorphic if and only if they have the same j-invariant, which is equivalent to having homothetic lattices Λ_1 and Λ_2. Hence, every isomorphism class has an elliptic curve whose associated lattice is of the form $\langle 1, \tau \rangle$ where $\tau \in \{z \in \mathbb{C} : Re(z) \in [-1/2, 1/2), |z| \geq 1\} \setminus PSL_2(\mathbb{Z})$. Moreover, Tate found a uniformization of the form $\mathbb{C}/q^{\mathbb{Z}}$ for any elliptic curve over $\mathbb{C}$ for some $|q| < 1$, see [Sil94, Ch.V], which later motivated the p-adic uniformization of a rational elliptic curve with multiplicative split reduction at a prime p.

1.1.2 *Elliptic curves over the real field*

Each $\mathbb{C}$-isomorphism classes of elliptic curves split into two $\mathbb{R}$-isomorphism classes called twists, see [Sil94, S.V.2]. Hence, two elliptic curves are isomorphic over $\mathbb{R}$ if they have the same j and γ invariants, where γ depends on the c_4 and c_6 invariants. Similar to elliptic curves over $\mathbb{C}$, an elliptic curve E over $\mathbb{R}$ has a uniformization of the form $\mathbb{R}/q^{\mathbb{Z}}$ where $q \in \mathbb{R}$ and $|q| \in (0, 1)$. Moreover, $E(\mathbb{R})$ as a real Lie group is isomorphic to either $\mathbb{R}/\mathbb{Z}$ when $\Delta < 0$, or $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ when $\Delta > 0$.

1.1.3 *Elliptic Curves over p-adic numbers*

All isomorphism classes of rational elliptic curves are also defined over $\mathbb{Q}_p$, and one can find a representative whose Weiestrass equation has coefficients in $\mathbb{Z}_p$ and whose discriminant Δ

has minimal p-valuation, see [Sil09, Cor.VIII.8.3]. This minimal equation allows one to study the reduction of an elliptic curve modulo p, which does not always lead to a non-singular equation on $\mathbb{F}_p$. Yet one obtains an exact sequence of the form:

$$0 \to E_1(\mathbb{Q}_p) \to E_0(\mathbb{Q}_p) \to \tilde{E}_{ns}(\mathbb{F}_p) \to 0$$

where $\tilde{E}_{ns}(\mathbb{F}_p)$ is the set of non-singular points in the reduction, $E_0(\mathbb{Q}_p)$ is the set of points with non-singular reduction, and $E_1(\mathbb{Q}_p)$ is the kernel of the reduction. The index $\tau_p = [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$ is called the Tamagawa number of E at p, which together with the conductor N_E of the elliptic curve is usually computed using Tate's algorithm.

One defines **Frobenius endomorphism** on the reduction $\tilde{E}(\mathbb{F}_p)$ by:

$$Frob_q : (x : y : 1) \in E \to (x^q : y^q : 1) \in E^{(q)}$$

which is characterized by $Frob_q^2 - a_q \cdot Frob_q + q = 0$ where $a_q = q + 1 - \#\tilde{E}(\mathbb{F}_q)$. Hasse showed that $|a_p| \leq 2\sqrt{q}$.

Given an elliptic curve E, one classifies the reduction at a prime p as follows:

- E has **good or stable reduction** at p if $\tilde{E}_p$ is nonsingular. This is characterized either by $v_p(\Delta) = 0$ or $p \not| N_E$. Moreover,
  - $E/\mathbb{Q}$ has good ordinary reduction at p if and only if $a_p(\tilde{E}_p) \not\equiv 0 (mod.p)$.
  - Otherwise, $E/\mathbb{Q}$ is said to have a good supersingular reduction at p. Elkies showed that CM elliptic curves have infinitely many supersingular primes.

- E has **multiplicative or semi-stable** reduction at p if $\tilde{E}_p$ is singular and has a node. For $p \geq 5$, this is characterized by $p|N_E$ but p^2 does not divide N_E. If the slopes of the tangent lines at the node are in $\mathbb{F}_p$, then it is said to be **split** and is characterized by $c_4 \neq 0$, otherwise it is **nonsplit**.

- E has **bad or unstable reduction** at p if $\tilde{E}_p$ is singular and has a cusp. This is characterized by $v(\Delta) > 0$ and $v(c_4) > 0$, and for a prime $p \geq 5$, $p^2|N_E$.

For rational elliptic curves E with split multiplicative reduction at p, one has $ord_p(j) < 0$, and Tate found an analytic uniformization $E(\mathbb{Q}_p) \cong \mathbb{Q}_p/q^{\mathbb{Z}}$ compatible with the action of $Gal(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ for some parameter $q \in \mathbb{Q}_p$ obtained by inverting the q-expansion of j, see [CY97, ch.XII, Tate], [Sil94, S.V.3]. Moreover, for an odd prime p, if $E(\mathbb{Q}_p) \cong_{/\mathbb{Q}_p} \mathbb{Q}_p^*/q^{\mathbb{Z}}$, the filtration given by $E \supseteq E_0 \supseteq E_1$ corresponds to the filtration $\mathbb{Q}_p^*/q^{\mathbb{Z}} \supseteq \mathbb{Z}_p^* \supseteq 1 + p\mathbb{Z}_p$.

1.1.4 The Formal Group of an Elliptic Curve

Given an elliptic curve E over $\mathbb{Q}_p$, let $z = -x/y$ and $w = -1/y$, and one obtains an equation of the form $w = f(z, w)$. By repeatedly substituting w in $f(z, w)$, one obtains $w(z) = z^3(1 + A_1 z + A_2 z^2 + \ldots) \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][\![z]\!]$. Moreover, see [Sil09, Ch.IV]

$$\begin{aligned} x(z) &= z^{-2} - a_1 z^{-1} - a_2 - a_3 z - (a_4 + a_1 a_3) z^2 - \ldots \\ y(z) &= -z^{-3} + a_1 z^{-2} + a_2 z^{-1} + a_3 + (a_4 + a_1 a_3 z) + \ldots \\ \omega_E(z) &= (1 + a_1 z + \ldots) dz \end{aligned}$$

Moreover, there is a series $F(x, y) = x + y + \ldots \in \mathbb{Z}[\![x, y]\!]$ called the formal sum, such that the map $\phi : \hat{E}^f(\mathbb{Q}_p) := (p\mathbb{Z}_p, \bigoplus) \to E_1(\mathbb{Q}_p)$ given by $z \mapsto (x(z) : y(z) : 1)$ is an isomorphism.

1.2 Twists, the Selmer, and the Tate-Shafarevich group

While automorphisms preserve the identity of an elliptic curve, isomorphisms do not, and thus they include translations. Any isomorphism decomposes into an automorphism and a translation. On the other hand, a twist of an elliptic curve E over $\mathbb{Q}$ is an algebraic curve C that is isomorphic over $\overline{\mathbb{Q}}$ to E. Here, one studies the classes of twists of a rational elliptic curve modulo isomorphic curves over $\mathbb{Q}$.

$$Twist_Q(E) = \frac{Isom_{\overline{Q}}(E)}{\{C \cong_{/\mathbb{Q}} C'\}}$$

These classes of twists of E are in one-to-one correspondence to the cohomology classes in $H^1(G_{\mathbb{Q}}, Isom(E))$, which is a pointed set, see [Sil09, p. 10]. An isomorphism $\phi : C \to E$ corresponds to $\xi_\sigma = \phi^\sigma \phi^{-1}$. This leads to the study of **principal homogeneous spaces** or

twists which have a simply transitive algebraic group action by E. The set of all such spaces is known as the **Weil-Chatelet group** of E and denoted by $WC(E/\mathbb{Q})$. A characterization of the class containing E is that any curve C on it has a rational point corresponding to O_E. The Weil-Chatelet group is in bijection with $H^1(G_{\mathbb{Q}}, E)$, which is an abelian group, where a curve $C \in WC(E/\mathbb{Q})$ corresponds to $\xi_\sigma \mapsto P^\sigma - P$ and P any point on C. Hence $WC(E/\mathbb{Q})$ can be given a group law.

The study of the Weil-Chatelet group played a key role in proving the Mordell-Weil theorem. Using Krummer theory on the isogeny $[n]$ or multiplication by n, one can show that $\frac{E(\mathbb{Q})}{mE(\mathbb{Q})} \hookrightarrow Sel_n(E/\mathbb{Q})$, which in turn is a subgroup of

$$\left\{ b \in \frac{\mathbb{Q}(E[n])^*}{(\mathbb{Q}(E[n])^*)^n} : \mathrm{ord}_v(b) \equiv 0 \,(\mathrm{mod}\ n) \text{ for all } v \notin S \right\}$$

which is finite.

1.2.1 Selmer and Tate-Shafarevich groups

Motivated by the Hasse-Minkowski local-to-global principle, one defines the m-Selmer group of an elliptic curve E as:

$$Sel_m(E/\mathbb{Q}) := Ker \left\{ H^1(G_{\mathbb{Q}}, E[m]) \xrightarrow{res} \prod_v H^1(G_{\mathbb{Q}_v}, E) \right\}$$

And the Tate-Shafarevich group of E, which measures the obstruction of the local-to-global principle for E, to be

$$Ш(E/\mathbb{Q}) := Ker \left\{ H^1(G_{\mathbb{Q}}, E) \xrightarrow{Res} \bigcap_v H^1(G_{\mathbb{Q}_v}, E) \right\}$$

Which satisfy:

$$0 \to \frac{E(\mathbb{Q})}{mE(\mathbb{Q})} \to Sel_m(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[m] \to 0 \tag{1.1}$$

In [Cas62a], Cassels described the elements of the m-Selmer group as m-covering elements in $WC(E/\mathbb{Q})$ which are soluble in every completion of $\mathbb{Q}$, i.e. everywhere locally soluble

twists of $(E, [m])$. In other words, there is a commutative diagram:

$$\begin{array}{ccc} E & \xrightarrow{[m]} & E \\ \updownarrow & \nearrow & \\ C & & \end{array}$$

where the vertical map is an isomorphism over $\overline{\mathbb{Q}}$, and the map from C to E is over $\mathbb{Q}$. Thus, the subgroup of elements which are globally soluble comes from the Mordell Weil subgroup, and the quotient of elements which are not globally soluble represents the Tate-Shafarevic group. By taking direct limits with respect to the multiplication by p-maps, one generalizes to

$$0 \to E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to Sel_{p^\infty}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p^\infty] \to 0$$

Moreover, although $Ш(E/\mathbb{Q})$ was known to be a torsion group, Cassels showed in [Cas62b] that the Tate-Shafarevic group modulo its divisible elements has a bilinear skew-symmetric form into $\mathbb{Q}/\mathbb{Z}$, leading to the conjecture that $Ш(E/\mathbb{Q})$ is finite and of square order. Concerned with the boundedness of $Ш(E/\mathbb{Q})$, Cassels [Cas64a] showed that the 3-primary part of Ш can have arbitrarily large $\mathbb{F}_3$-rank and thus it is unbounded. Lemmermeyer [Lem00] and Atake [Ata01] showed similar results for the 2-primary part using quartic reciprocity symbols. Fisher showed analogous results for the 5-primary part in his Ph.D. thesis and in [Fis01].

Poonen and Stoll [PS99] showed that the skew-symmetry property of this form comes from the fact that all elliptic curves are principally polarized and self-dual. Indeed, although Tate [Tat63] generalized this to an alternating form on the principal homogeneous spaces of an abelian variety and these of its dual, Flach proved that this pairing is only antisymmetric. This also led to show that the Tate-Shafarevich group of a principally polarized abelian variety, e.g. the Jacobian of any curve, is either a square or twice a square. Stein [Ste04] constructed explicit examples for every odd prime $p \neq 37$ and less than 25000 where a twist of $E^{p-1} = E \times \ldots \times E$ has $\#Ш(A_T/\mathbb{Q}) = pn^2$ with n an integer.

Both the Selmer and Tate-Shafarevic group definitions generalize to isogenies, which is

usually refered to first descent through isogenies. Indeed, for a p-degree isogeny $\phi : E \to \tilde{E}$, one has:

$$0 \to \frac{\tilde{E}(\mathbb{Q})}{\varphi(E(\mathbb{Q}))} \xrightarrow{\delta} Sel_{\varphi}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[\varphi] \to 0$$

Lemma 1. *Let $\phi : E \to \tilde{E}$ be an isogeny whose dual is $\tilde{\phi}$. Then $Ш(E)[p]$ is contained in $Ш(E)[\varphi]$, and thus one obtains a boundary for $\operatorname{rank}_{\mathbb{F}_p} Ш(E/\mathbb{Q})(p)$.*

1.3 Descents

Descents are methods to obtain curves C in the n-Selmer group of an elliptic curve E. They are of great aid when searching for generators of the Mordell-Weil group $E(\mathbb{Q})$. In many cases, when the resulting curve C represents an element from $E(\mathbb{Q})/nE(\mathbb{Q})$, finding a rational point in C might be faster, and then one can map this point to a point in $E(\mathbb{Q})$.

In [Cre+08, §1], Cremona, Fisher, O'Neil, Simon, and Stoll present several characterizations of the crossed homomorphisms in $H^1(G_{\mathbb{Q}}, E[n])$, which contains $Sel_n(E/\mathbb{Q})$:

- A torsor or twist of the pair $(E, [n \cdot 0_E])$, where the brackets denote a divisor in E.
- An n-covering of E or twist of $(E, [n])$, where $[n]$ denotes the isogeny of multiplying by n, see also [Cas62a, S.1].
- A Brauer-Severi diagram or twist of the map $E \to \mathbb{P}^{n-1}$.
- A twist of the zero dimensional variety $(E[n], +)$.

and two others. Moreover, Cremona et al. [Cre+15] present the algorithms for Descent methods, which aim to compute equations on principal homogeneous spaces of an elliptic curve E and equations of the morphisms to E.

Most of these started in Cassel's work in the 1960's, see [Cas62b, Thm.1.3], where he showed that any principal homogeneous space $C \in Ш(E/\mathbb{Q})[n]$ admits a $\mathbb{Q}$-rational divisor of degree n, whose linear system embeds C in $\mathbb{P}^{n-1}$.

- If the minimal degree is $n = 2$, then C is a hyperelliptic curve of the form $y^2 = f(x)$, where $f(x)$ is a 4-th degree univariate polynomial, see [BSD63]. Applying two descent on an elliptic curve is performed by computing some invariants I and J from the equation of the elliptic curve, which are the classical invariants for the quartic polynomials representing its principal homogeneous spaces C in $H^1(\mathbb{Q}, E[2])$, and then finding all candidates which are everywhere locally soluble. See [Cre01a],[CFS10] for further details.

- If the minimal degree is $n = 3$, then C is a plane cubic curve, i.e. the locus of a ternary cubic equation. Similarly to the two descent, applying three descent on an elliptic curve E is performed by computing some invariants from the equation of the elliptic curve, which is the Hessian of the principal homogeneous spaces C and two more invariants. Then one finds all candidates for C and establishes conditions for which C is everywhere locally soluble, see [CFS10]. For a reduction algorithm on the results see [CFS10, §6C]. Moreover, the implementation in *Magma* used in this dissertation requires the ideal class group of a number field to be computed, and in order to speed such computations, one assumes the General Riemann Hypothesis.

- If the minimum degree is 4, then C is the intersection of two quadrics, i.e. quadratic equations on 4 variables. Alternatively, a curve C_4 obtained from 4-descent on an elliptic curve E is a 2-covering of a curve C_2 obtained from 2-descent on E. For a construction of 4-descents see [MSS96, §4]. For the minimization and reduction algorithms see [CFS10, §4.3, 6.4].

- If the minimum degree is 5, then C is the locus of the 4×4 principal Pfaffians of a 5×5 alternating matrix of linear forms on 5 variables, see [Fis13a] and [Fis13b] for algorithms on computing and reducing the models of C. Yet contrary to the previous cases, 5 descent is not implemented on *Magma*.

- In general, if the minimum degree is $n \geq 4$, then C is the locus of a vector space of quadrics on n variables of dimension $n(n-3)/2$. Further descents have been studied, see for example [Cre14], but *Magma* has implementations of only $2, 3, 4, 6, 8, 9$, and 12 descents. For a classical introduction explaining the models for 2, 3, 4 descent coverings, see also [Wei07, Ch.2, App.2]. An important theory to keep in mind is the minimization and reduction of these models, see for example [Cre01b], which is aided by Gaston Julia's reduction of binary forms.

1.3.1 Models and Distributions

R. Heath-Brown [HB93], [HB94] discovered a remarkable distribution for the 2-Selmer groups of the quadratic twists of the elliptic curve $y^2 = x^3 - x$ over $\mathbb{Q}$ while studying the congruent number problem. P. Swinnerton-Dyer [SD08] and D. Kane [Kan13] generalized this result to the family of quadratic twists of any rational elliptic curve. In [PR12], B. Poonen and E. Rains formulated a generalized conjecture of this by modeling the p-Selmer group as the intersection of two random maximal isotropic modules:

Conjecture 1. *[PR12, Conj-1.1, Thm-5.2] The distribution of the $\mathbb{F}_p$-rank of the p-Selmer group of elliptic curves over $\mathbb{Q}$ ordered by height is given by*

$$Prob\left(\dim_{\mathbb{F}_p} Sel_p E = d\right) = \left(\prod_{j\geq 0}(1+p^{-j})\right)\left(\prod_{j=1}^{d}\frac{p}{p^j-1}\right)$$

Moreover, this agrees with C. Delaunay's conjectured distribution of the $\mathbb{F}_p$-rank of the Tate-Shafarevich group, see proposition 3. It also agrees with D. Goldfeld's conjecture that asymptotically 50% of elliptic curves have rank 0 and 50% have rank 1, see [Gol79, Conj.B].

Delaunay's conjecture followed Cohen-Lenstra heuristics on the ideal class group. It modeled the Tate-Shafarevich group of rational elliptic curves as a random simplectic group, i.e. with a bilinear alternating form representing the Tate-Cassels pairing. Similarly, M. Bhargava, Kane, Lenstra, Poonen and Rains modeled the p-primary part of the Tate-Shafarevich

group as the cokernel of a random alternating matrix with coefficients in $\mathbb{Z}_p$ based on Friedman and Washington's conjectures of the ideal class group, see [Bha+15, Thm.1.10].

1.4 The BSD Conjecture

In the 60's, Birch and Swinnerton-Dyer showed strong computational evidence of an explicit relation between several arithmetic and analytic invariants of an elliptic curve. The case for rational elliptic curves can be summarized as follows:

Conjecture 2. *Given an elliptic curve E over $\mathbb{Q}$, then:*

1. *The algebraic rank* $\operatorname{rank}(E)$ *is equal to the analytic rank* $ord_{s=1}L(E,s)$. *This is known as their weak conjecture.*

2. *Let $E(\mathbb{Q})_{tor}$ be the torsion subgroup of the Mordell-Weil group of the curve E, $\tau_p = [E(\mathbb{Q}) : E_0(\mathbb{Q})]$ be the Tamagawa-number at p,* $\operatorname{reg}(E)$ *be the regulator of E, Ω_E be the minimal real period of E, and $L(E,s)$ be the L-series of E. Then*
$$\frac{L^{(r)}(E,1)}{r!} = \frac{\operatorname{reg}(E)\cdot\Omega_E\cdot\prod_{p|N_E}\tau_p\cdot\#Ш(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{tor})^2}$$
This is known as the strong conjecture.

Here, the regulator of an elliptic curve E, in particular the height, measures the complexity of the generators of the Mordell-Weil group of E. One initially defines a logarithmic naive height and then through the Weil height machine, see for example [HS00, §B], one finds the Neron-Tate canonical height of the generators. Then given an elliptic curve E of rank r, and a set of generator points of the quotient $E(\mathbb{Q})/E(\mathbb{Q})_{tor}$, one has:

$$\operatorname{reg}(E) := \det(\langle P_i, P_j\rangle)$$

where $\langle P,Q\rangle = \frac{1}{2}\left(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)\right)$ is the nondegenerate bilinear height pairing associated to the canonical height $\hat{h}$. A standing lower bound conjecture [Sil09, Conj.9.9] on the canonical height for points in a rational elliptic curve is given by

$$\hat{h}(P) > C\max\{h(j(E)), \log\Delta(E), 1\}$$

where Δ is the minimal discriminant of E and C is independent of both the elliptic curve E and the point P. However, the constant C derived from the data in this dissertation is too small to be of use in deriving the Tate-Shafarevich group order of any given curve. Moreover, Cremona, Pricket and Siksek decomposed the canonical height into local terms in order to find an upper bound for the difference between the naive height h and the canonical height $\hat{h}$ on a point of an elliptic curve, see [CPS06, Thm.1]

$$h(P) - \hat{h}(P) \leq \frac{1}{3}\log \epsilon_\infty + \sum_p \alpha_p \log(p)$$

where α_p depends on the reduction type of E at a given prime p. This upper bound has been implemented in *SageMath* and is used in the results presented here.

1.4.1 Modularity and the Gross-Zagier formula

Another element in the BSD conjecture is the L-series of the elliptic curve E. There is much more to say about this L-series due to the Modularity conjectured, proved by Breuil, Conrad, Taylor, Diamond and others, see [DI95] and [DS05] for introduction to these theories.

From modularity theory, one knows that for every rational elliptic curve, there is a new cusp form $f_E \in S_2(N)$ with integer Fourier coefficients $a_n(f)$, after normalizing it to have $a_1(f_E) = 1$ such that $a_n(f) = a_n(E) = p + 1 - \#\tilde{E}(\mathbb{F}_p)$. Moreover, the L-functions of f and that of E agree:

$$\begin{aligned} L(f,s) &:= \tfrac{(2\pi)^s}{\Gamma(s)} \textstyle\int_0^{i\infty} (-iz)^s f(z) \frac{dz}{z} \\ &= \textstyle\sum_{n\geq 1} \frac{a_n}{n^s} = \prod_{p|N} (1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p\not|N} (1 - a_p p^{-s})^{-1} \\ &=: L(E,s) \end{aligned}$$

Moreover, there is a surjective holomorphic homomorphism $\phi : X_0(N) \to E$, see [DS05, Thm.2.5.1], whose degree is called the Modular degree of E. This degree plays a role in visualizing the elements of the Tate-Shafarevich group in the embedding of E into the Jacobian Curve $J_0(M)$, see [JS07].

In the attempts to prove how the order of a point in an analytic function relates to the existence of independent generators of an algebraic group, Gross and Zagier developed the

theory of Heegner points. These are points $y_K \in E(K)$ where K is some quadratic field over $\mathbb{Q}$. The Gross-Zagier formula states that:

$$h(y_K) = \frac{\sqrt{D}}{c^2 \int_{E(\mathbb{C})} \omega_E \wedge \overline{i\omega_E}} L'(E/K, 1)$$

or alternatively, as stated in [Wat12, Thm.3.1], let $E/\mathbb{Q}$ be an elliptic curve of analytic rank 1 and conductor N. Suppose $D < -4$ a fundamental discriminant with D a square modulo $4N$ and $gcd(D, 2N) = 1$. Then

$$h(y_K) = \frac{\sqrt{|D|}}{4\Omega_{vol}} L'(E, 1) L(E_D, 1)$$

See [GZ86], [GKZ87], [BS12, Thm.2].

Moreover, Watkins [Wat12, Alg.3.3] found an algorithm to approximate the coordinates of a Heegner point of an elliptic curve of rank 1, with the hope that one can retrieve the rational coordinates. Although I tried to run naively his code on *Magma* for some of the elliptic curves where I could not find a generator, *Magma* simply threw a warning message that it cannot be computed. This may be because the precision required to find the denominator of the x-coordinate is too big and thus it would require too much memory for the sum involving the Hasse coefficients a_n of E. However, I expect that this is due only to a parameter in the coding, because his examples reflect that this could work with most, if not all, of the curves where I am missing the generator.

Kolyvagin used the Gross-Zagier formula to show that this rank conjecture holds whenever the analytic rank is less than or equal to one, see [Kol91c]. Bhargava, Skinner, and Zhang showed that at least 66.48% of rational elliptic curves ordered by height satisfy this. Moreover, for these curves, #Ш is finite, see [BSZ, Thm.2, Cor.22,24,26].

Among several contributions, Grigorov, Jorza, Patrikis, Stein, and Corinain [Gri+09] verified that the p-valuation of #Ш agrees with the conjectural value for several non-CM rational elliptic curves of rank ≤ 1 with conductor ≤ 1000, an odd prime p coprime with their Tamgawa product, and an irreducible representation $\overline{\rho}_{p,E}$. Jetchev, Skinner, and Wan [JSW17] and Castella [Cas18] showed that for a semistable elliptic curve $E/\mathbb{Q}$ with analytic

rank 1 and a prime $p \geq 5$ where $E[p]$ is irreducible, one has:

$$ord_p\left(\frac{L'(E,1)}{Reg(E/\mathbb{Q})\Omega_E}\right) = ord_p\left(\#Ш(E/\mathbb{Q})\prod_{l|\infty}\tau_l(E/\mathbb{Q})\right)$$

Chapter 2

ELABORATION OF THE TABLES

2.1 Introduction

In this chapter I describe the construction of my tables showing the Tate-Shafarevich group order and type of nearly 4.5 million rational elliptic curves up to conductor one million from Cremona's and Stein-Watkins' databases. Assuming several standard conjectures, which include the Birch and Swinnerton-Dyer conjecture and the Generalized Riemann Hypothesis, I describe how to compute these elements using both *SageMath* and *Magma*. I also make predictions on how far we are from having data showing any evidence of Delaunay's asymptotic proportions on the p-primary parts of the Tate-Shafarevich group.

2.2 On the preparation of the tables and graphs.

For the elliptic curves in Cremonas database, I copied the conductor N_E, the a-invariants, the rank r, the torsion subgroup order, the product of the Tamagawa numbers, the regulator, the leading coefficients, and Tate-Shafarevich group order of all elliptic curves. I later added the non-torsion generators. However, t find the generators for ranks 3 and 4 curves, I performed a point search in *SageMath* (which uses Michael Stoll's ratpoints module in PARI/GP), so they may differ from the generators listed in Cremonas tables. I computed in *Magma* the $\mathbb{F}_2$-rank of the 2 primary part and the $\mathbb{F}_3$-rank of the 3 primary part of their Tate-Shafarevich group, i.e.

$$r_2Ш := \text{rank}_{\mathbb{F}_2} Ш(E/\mathbb{Q})(2) = \text{rank}_{\mathbb{F}_2} Ш(E/\mathbb{Q})[2]$$

$$r_3Ш := \text{rank}_{\mathbb{F}_3} Ш(E/\mathbb{Q})(3) = \text{rank}_{\mathbb{F}_3} Ш(E/\mathbb{Q})[3]$$

and printed them into a text file, and then read this file and inserted these values into my *Postgresql* database from *SageMath*.

For the elliptic curves in Stein-Watkins database, I copied the rank r, the leading coefficient, and the Tate-Shafarevich group order for elliptic curves of rank $r = 0$. For positive rank curves, I searched for their non-torsion generators and wrote the results in the *Postgresql* database in *SageMath*. Notice that point search in *SageMath* includes the saturation routine (using Cremona's "mwrank" package) of the subgroup found. I also searched for rational points in the curves obtained from descent methods in *Magma*. I copied these results to *SageMath* and saturated the results. Regrettably, I was manually copying and pasting the results, so I decided to run a check to verify that the coordinates of these points were actually on the curves. I also tried saturating the generators of curves whenever they showed a non-trivial Tate-Shafarevich group which was not predicted by r_2Ш and r_3Ш. In many cases, where I was not able to obtain the generators, I computed the leading coefficient (using *SageMath*'s interface to Tim Dokchitser's program for computing with the L-series of the elliptic curve) to a greater precision than the one on Stein-Watkins original tables. Then I estimated a lower bound for their regulators $\mathrm{reg}(E)$ using the Cremona-Prickett-Siksek cps of each curve. In some cases where 2^8 divided the Tate-Shafarevich group order, I computed the number of 4-coverings of the 2-coverings of each curve obtained from 2-descent in *Magma*, which again I saved into a text file as a string. Then I read this file from *Sagemath* and translated into a list of pairs (a, b), which means there are b curves with a coverings each. The rest of the elements in this table were computed and wrote into *Postgresql* from *SageMath*.

I was not able to find the Tate-Shafarevich group order of around 200 curves of rank 1 where these techniques would take too long or too much memory. I expect most of them could be solved using Heegner points as described in Watkins' [Wat12]. Yet, $\mathrm{reg} \cdot \#Ш + \mathrm{cps}$ and $\mathrm{reg} \cdot \#Ш/25 + \mathrm{cps}$ are good indicators of the complexity of the curves, where reg is the regulator of the curve and $\#Ш$ is the Tate-Shafarevich group order of the curve.

For the curves where I used Mazur-Tate-Teitelbaums p-adic BSD conjecture, I computed all quantities in *SageMath*. Although Wuthrichs algorithm for numerical modular symbols is still in testing stages, the reason why I was not able to compute some of the leading

coefficients of the p-adic L-series was that the algorithm requires a sum of too many terms for some curves. Hence, I ran out of memory or I simply canceled the computation because it was taking too long.

Using basic statistical models for proportions, I predict a bound on the conductor of rational elliptic curves, so data would show some resemblance to Delaunay's conjectures on the Tate-Shafarevich group type of rational elliptic curves. Although, at a glance, the data suggests a logarithmic model, such model does not resemble proportion distributions because logarithmic functions diverge. Hence, I opted to simplify our model function to measure only the growth of this proportions. I chose $D - ae^{bx}$ as such a statistical function, where D is the asymptotic Delaunay's proportion of a particular phenomena.

In addition, due to the difference in nature of the original databases, I split the data and did independent statistical models for both Cremona's and Stein-Watkins' curves. Their graphs were created using Time Series in *SageMath,* which does not take all points but only a bounded number of sample points. However, I tested some of them and these graphs indeed resemble data patterns.

2.3 Elliptic curves of rank 0

2.3.1 Origin of the Tables

I took all rank 0 elliptic curves obtained by combining Cremona's database, which contains all curves up to conductor 4×10^5, and Stein-Watkins' database up to conductor 10^6, which only contains curves whose discriminant satisfies $|\Delta| \leq 10^{12}$ and it does not list in general all the curves of a particular conductor. For the 1553579 elliptic curves of rank 0, I took the torsion order tor, the Tamagawa product tam, the leading coefficient lc of the associated L-series, and the Tate-Shafarevich analytic group order. The origins of the curves are summarized in table 2.1.

$\lfloor \frac{n}{10^5} \rfloor$	CRE	SW	%
0	267565	207860	15.85
1	238781	165335	14.14
2	228539	149992	13.53
3	221201	140726	13.1
4	0	132886	7.87
5	0	127350	7.54
6	0	122021	7.23
7	0	120274	7.12
8	0	116742	6.91
9	0	113267	6.71
Total	956086	1396453	1688626

Table 2.1: Origin of rank 0 elliptic curves

2.3.2 The first part of the strategy

Given a rank 0 rational elliptic curve, known through the a-invariants of its minimal equation, I wanted to compute its Tate-Shafarevich group type given that I already knew its Tate-Shafarevich group order as predicted by the Birch and Swinnerton-Dyer strong conjecture on rational elliptic curves.

If the square root of $\#Ш(E/\mathbb{Q})$ is square free, then one can deduce the Tate-Shafarevich group type from its order:

$$\#Ш(E/\mathbb{Q}) = \prod_{i=1}^{j} p_i^2 \Rightarrow Ш(E/\mathbb{Q}) \cong \prod_{i=1}^{j} \left(\frac{\mathbb{Z}}{p_i \mathbb{Z}} \right)^2$$

I found 1259266 examples where $\#Ш(E/\mathbb{Q}) = 1$, and I found curves where p divides $\#Ш(E/\mathbb{Q})$ for most primes below 50. See table 2.2.

p	CRE - npm	SW - npm
2	76116.91	114042
3	24440	32718
5	4119	3920
7	1015	807
11	139	66
13	68	29
17	13	2
19	11	1
23	6	0
29	1	0
31	1	1
37	0	0
41	0	0
43	0	0
47	0	0

Table 2.2: No. of rank 0 elliptic curves per million whose #Ш is divisible by a prime.

2.3.3 Asymptotic proportions

In [Del01], motivated by Cohen-Lenstra heuristics, Delaunay's proposed a series on conjectures on the distribution of the Tate-Shafarevich rank and group types for elliptic curves over $\mathbb{Q}$. There, Delaunay's models the Tate-Shafarevich group as a random group with an alternating bilinear pairing representing the Cassels-Tate pairing, and weighted by the group order divided by its automorphism group order. These conjectures depend on the rank of the Mordell-Weil groups. See also [Del07, §3.1],[PR12, §5].

Conjecture 3. *[Del01] When ordering all rank r rational elliptic curves by conductor, they*

satisfy the following:

$$Prob(\text{rank}_{\mathbb{F}_p} Ш(p) = 2n) = p^{-n(2r+2n-1)} \frac{\prod_{i=n+1}^{\infty}(1-p^{-(2r+2i-1)}}{\prod_{i=1}^{n}(1-p^{-2i})})$$

In particular,

$$Prob(p|\#Ш(E/\mathbb{Q})) = 1 - \prod_{i=1}^{\infty}(1-p^{1-2i-2r})$$

$$Prob\left(Ш(p) \cong \left(\frac{\mathbb{Z}}{p^k\mathbb{Z}}\right)^2\right) = \frac{p^{(-1-2r)k}}{1-p^{-2}} \prod_{i=1}^{\infty} 1 - p^{1-2i-2r}$$

And,

$$Prob\left(Ш(p) \cong \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^4\right) = \frac{p^{4(1-r)}}{p^{10}(1-p^{-2})(1-p^{-4})} \prod_{i=1}^{\infty} 1 - p^{1-2r-2i}$$

For the case of $r = 0$*, see table 2.3*

Remark 1. *However, for any elliptic curve here where* $p|\#Ш(E/\mathbb{Q})$ *with* $p > 5$*, the valuation of* $\text{ord}_p(\#Ш(E/\mathbb{Q})) = 2$*. Hence,*

$$Ш(E/\mathbb{Q})(p) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

Remark 2. *Interesting enough, in the rest of Stein-Watkins database, one may only find four elliptic curves of rank* 0 *whose Tate-Shafarevich group order is divisible by a prime bigger than* 50*:*

n	*a-invariants*	$\#Ш$
8402675	$[0, 0, 1, -5597749375, -161201206817969]$	53^2
49866995	$[0, 0, 1, -3759310933, -88718435978351]$	59^2
65726403	$[0, -1, 1, -1969227335320, -1063632573703622025]$	53^2
87410011	$[0, 1, 1, -230182099723060, -1344173903267584699813]$	127^2

In [Wat08, §2,4], M. Watkins reconstructed Brumer-McGuiness conjecture on the number $N_{\pm}(X)$ of rational elliptic curves of positive (or negative respectively) discriminant with absolute value bounded by X ordered by discriminant up to a given discriminant:

$$N_{\pm}(X) \sim \frac{\alpha_{\pm}}{\zeta(10)} X^{5/6}$$

p	$p\|\#Ш$	$\mathrm{r}_{\mathbb{F}_p}Ш(p)=2$	$(\mathbb{Z}/p\mathbb{Z})^2$	$(\mathbb{Z}/p^2\mathbb{Z})^2$	$(\mathbb{Z}/p\mathbb{Z})^4$
2	58.0578	55.9230	27.9615	13.9807	0.9320
3	36.0995	35.9440	23.9627	7.9876	0.0998
5	20.6665	20.6598	16.5278	3.3056	0.0053
7	14.5408	14.5399	12.4628	1.7804	0.0007
11	9.1598	9.1597	8.3270	0.7570	0.0001
13	7.7346	7.7346	7.1396	0.5492	0.0000
17	5.9016	5.9016	5.5544	0.3267	0.0000
19	5.2770	5.2770	4.9993	0.2631	0.0000
23	4.3557	4.3557	4.1663	0.1811	0.0000
29	3.4522	3.4522	3.3332	0.1149	0.0000
31	3.2291	3.2291	3.1249	0.1008	0.0000
37	2.7046	2.7046	2.6315	0.0711	0.0000
41	2.4404	2.4404	2.3809	0.0581	0.0000
43	2.3268	2.3268	2.2727	0.0529	0.0000
47	2.1286	2.1286	2.0833	0.0443	0.0000

Table 2.3: Rank 0 case for Delaunay's predictions as percentages.

where $\alpha = \frac{\sqrt{3}}{10}\int_{\pm 1}^{\infty}\frac{dx}{\sqrt{x^3\mp 1}}$. Thus, he derived a similar conjectured on the number $N(X)$ of rational elliptic curves whose conductor is less than X of the form $N(X) \sim cX^{5/6}$. I took this Heuristic to predict the number of rank 0 rational elliptic curves up to conductor X. See proposition 1

Proposition 1. *The best-fit log-log approximations for the numbers $N_{cre}(X,0)$ of rank 0 rational elliptic curves and the number $N_{sw}(X,0)$ of rank 0 rational elliptic curves of discriminant $|\Delta| \leq 10^{12}$ up to conductor X based on Cremona's and Stein-Watkins' databases*

respectively are given by:

$$N_{cre}(X,0) \approx 5.3\, X^{0.939}$$

$$N_{sw}(X,0) \approx 11.6\, X^{0.849}$$

2.3.4 Distribution when the order is divisible by 2

Proposition 2. *I found 217909 elliptic curves of rank* 0 *where* $\#Ш(E/\mathbb{Q})$ *is divisible by* 2. *Assuming the BSD conjecture, the distribution of these curves by* $\mathrm{ord}_2(\#Ш)$ *and* $\mathrm{rank}_{\mathbb{F}_2} Ш[2]$ *is given in tables 2.4 and 2.5.*

Remark 3. *In here, npm means number of curves per million and not the JavaScript tool.*

$\mathrm{rank}_{\mathbb{F}_2} Ш[2]$ / $\mathrm{ord}_2(\#Ш)$	2	npm	4	npm	Total	npm
2	113489	882956	–	––	113489	882956
4	13356	103911	654	5088	14010	108999
6	837	6511	163	1268	1000	7780
8	21	163	13	101	34	264
Total	127703	993542	830	6457	128533	1000000

Table 2.4: Cremona's rank 0 elliptic curves with $\#Ш$ divisible by 2.

The strategy to determine the 2 primary part

I needed to compute $r_2Ш := \mathrm{rank}_{\mathbb{F}_2} Ш(E/\mathbb{Q})[2]$. I first computed the torsion subgroup type of E, which by By Mazur's theorem, I know $E(\mathbb{Q})_{\mathrm{tor}}$ is exactly one of the following groups:

$$\{\mathbb{Z}/n\mathbb{Z} : 1 \leq n \leq 10, \text{ or } n = 12\} \cup \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} : 1 \leq n \leq 4\}$$

$\text{rank}_{\mathbb{F}_2}$ Ш[2]	2	npm	4	npm	6	Total	npm
$\text{ord}_2(\#Ш)$							
2	173072	898725.17	–	––	–	173072	898725.17
4	17449	90608.85	918	4766.97	–	18367	95375.83
6	828	4299.62	257	1334.54	1	1086	5639.36
8	22	114.24	26	135.01	0	48	249.25
10	0	0.0	2	10.39	0	2	10.39
Total	191371	993747.89	1203	6246.92	1	192575	1000000.0

Table 2.5: Stein-Watkins's rank 0 elliptic curves with #Ш divisible by 2.

Then I computed the order of the 2-Selmer group of E, i.e. $\#\,\text{Sel}_2(E/\mathbb{Q})$, in *Magma* by performing two descent. Recall that *Magma* returns all elements but the trivial one, and the $\#\,\text{Sel}_2(E/\mathbb{Q})$ is predicted to be:

$$\#\,\text{Sel}_2(E/\mathbb{Q}) = 2^t \cdot 2^{r_2Ш}$$

where

$$t = \begin{cases} 0 & \Leftarrow \quad E(\mathbb{Q})_{tor} \in \{\mathbb{Z}/n\mathbb{Z} : n \text{ is odd}\} \\ 1 & \Leftarrow \quad E(\mathbb{Q})_{\text{tor}} \in \{\mathbb{Z}/n\mathbb{Z} : n \text{ is even}\} \\ 2 & \Leftarrow \quad E(\mathbb{Q})_{\text{tor}} \in \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} : 1 \leq n \leq 4\} \end{cases}$$

This is enough to determine the group type of $Ш(E/\mathbb{Q})(2)$ in the following cases:

1. If $\text{ord}_2(\#Ш(E/\mathbb{Q})) = 2n$ and $r_2Ш = 2$, then

$$Ш(E/\mathbb{Q})(2) \cong (\mathbb{Z}/2^n\mathbb{Z})^2$$

2. If $\text{ord}_2(\#Ш(E/\mathbb{Q})) = 4$ and $r_2Ш = 4$, then

$$Ш(E/\mathbb{Q})(2) \cong (\mathbb{Z}/2\mathbb{Z})^4$$

3. If $\text{ord}_2(\#Ш(E/\mathbb{Q})) = 6$ and $r_2Ш = 4$, then

$$Ш(E/\mathbb{Q})(2) \cong (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/4\mathbb{Z})^2$$

4. If $\text{ord}_2(\#Ш(E/\mathbb{Q})) = 6$ and $r_2Ш = 6$, then

$$Ш(E/\mathbb{Q})(2) \cong (\mathbb{Z}/2\mathbb{Z})^6$$

However, in the rest of the cases that I found, I needed to compute the number of 2-coverings of E that have 4-covering curves obtained by performing four descent on each of the elements of $Sel_2(E/\mathbb{Q})$.

Remark 4. *Recall here that for a rank* 0 *elliptic curve* E *with*

$$Ш(E/\mathbb{Q})(2) \cong \prod_{i=1}^{j} \left(\frac{\mathbb{Z}}{p^i\mathbb{Z}}\right)^{2\lambda_j}$$

there are

$$2^t \cdot 2^{2(\lambda_2+\ldots+\lambda^j)} = 2^t \cdot 2^{r_2Ш-2\lambda_1}$$

elements of $Sel_2(E/\mathbb{Q})$ *that have* 4*-covering curves obtained from Four Descent, where* t *is defined above.*

This is enough to determine the group type of $Ш(E/\mathbb{Q})(2)$ in the following cases:

1. If $\text{ord}_2(\#Ш(E/\mathbb{Q})) = 8$, $r_2Ш = 4$, $\#E(\mathbb{Q})_{tor} = 2$, and there are 24 elements of $Sel_2(E/\mathbb{Q})$ without 4-coverings and 8 such elements with 4-coverings, actually each one has sixteen 4-coverings, then

$$Ш(E/\mathbb{Q})(2) \cong (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/8\mathbb{Z})^2$$

2. If $\text{ord}_2(\#Ш(E/\mathbb{Q})) = 8$, $r_2Ш = 4$, $\#E(\mathbb{Q})_{tor} = 2$, and all 32 elements of $Sel_2(E/\mathbb{Q})$ have 4-coverings, actually each one has sixteen 4-coverings, then

$$Ш(E/\mathbb{Q})(2) \cong (\mathbb{Z}/4\mathbb{Z})^4$$

3. If $\mathrm{ord}_2(\#Ш(E/\mathbb{Q})) = 10$, $r_2Ш = 4$, $\#E(\mathbb{Q})_{tor} = 2$, and all 32 elements of $Sel_2(E/\mathbb{Q})$ have 4-coverings, actually each one has sixteen 4-coverings, then

$$Ш(E/\mathbb{Q})(2) \cong (\mathbb{Z}/4\mathbb{Z})^2 \times (\mathbb{Z}/8\mathbb{Z})^2$$

Since these are all cases found, then I did not need to perform eight descent for these curves, which is implemented in *Magma*.

Asymptotic proportions

Recall that according to Delaunay's asymptotic proportions, 58.06% of rank 0 elliptic curves have $\#Ш(E/\mathbb{Q})$ divisible by 2.

Proposition 3. *While Delaunay predicted that* 55.92% *rank* 0 *rational elliptic curves have* $\mathrm{rank}_{\mathbb{F}_2} Ш(2) = 2$*, the best-fit statistical proportion models of the form* $p = D - a\exp(bN)$ *for Cremona's and Stein-Watkins' such curves where* p *is the proportion of such curves up to conductor* N*, and* $D \approx 0.5592$ *is Delaunay's proportion of such curves are given respectively by:*

$$p_{CRE} \approx 0.5592 - 0.4739 \cdot e^{-(3.2353\times 10^{-7})x}$$

$$p_{SW} \approx 0.5592 - 0.4635 \cdot e^{-(1.1327\times 10^{-7})x}$$

Moreover, these models predict that one would need to compute all rank 0 *rational elliptic curves up to conductors* 6.6×10^6*,* 8.7×10^6*,* 1.4×10^7*, and all rank* 0 *curves of bounded discriminant up to conductors* $1.9\times 10^7, 2.5\times 10^7, 3.9\times 10^7$ *in order to achieve* $90\%, 95\%, 99\%$ *of Delaunay's proportion respectively. See figure 2.1.*

Remark 5. *However, based on the ratio* $|\Delta|/N$ *for rank* 0 *rational elliptic curves, I expect that the proportion of rank* 0 *elliptic curves in Stein-Watkins' database with respect to the total of such curves up to a conductor* X *keeps decreasing as* $X \to 10^8$*, and thus the margin of error of the second predictions largely increases.*

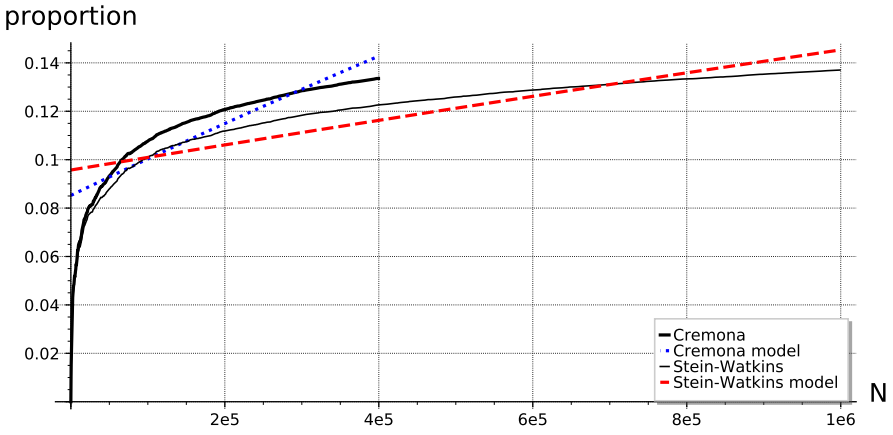

Figure 2.1: The proportion of rank 0 elliptic curves with $\text{rank}_{\mathbb{F}_2} Ш(E/\mathbb{Q})[2] = 2$

Proposition 4. *While Delaunay predicted that* 1.86% *rank* 0 *rational elliptic curves have* $\text{rank}_{\mathbb{F}_2} Ш(2) = 4$*, the best-fit statistical model of the form* $p = D - a\exp(bN)$ *for Cremona's and Stein-Watkins rank* 0 *elliptic curves where* p *is the proportion of such curves up to conductor* N*, and* D *is Delaunay's proportion of such curves are respectively given by:*

$$p_{CRE} \approx 0.0186 - 0.0183 \cdot e^{-(8.40\times 10^{-8})x}$$

$$p_{SW} \approx 0.0186 - 0.0181 \cdot e^{-(2.23\times 10^{-8})x}$$

Moreover, these models suggest that one would need to compute all rank 0 *elliptic curves up to conductors* 2.7×10^7*,* 3.5×10^7*,* 5.5×10^7 *for Cremona's database, and up to conductors* $1.0 \times 10^8, 1.3 \times 10^8, 2.0 \times 10^8$ *for Stein-Watkins' database in order to achieve* $90\%, 95\%, 99\%$ *of Delaunay's proportion respectively. See figure 2.2.*

Remark 6. *Delaunay also predicted that:*

$$Prob(Ш(E_{r=0}/\mathbb{Q}) \cong (\mathbb{Z}/p^k\mathbb{Z})^2) = \frac{1}{p^k(1-p^{-2})}\prod_{k=1}^{\infty} 1 - p^{1-2k}$$

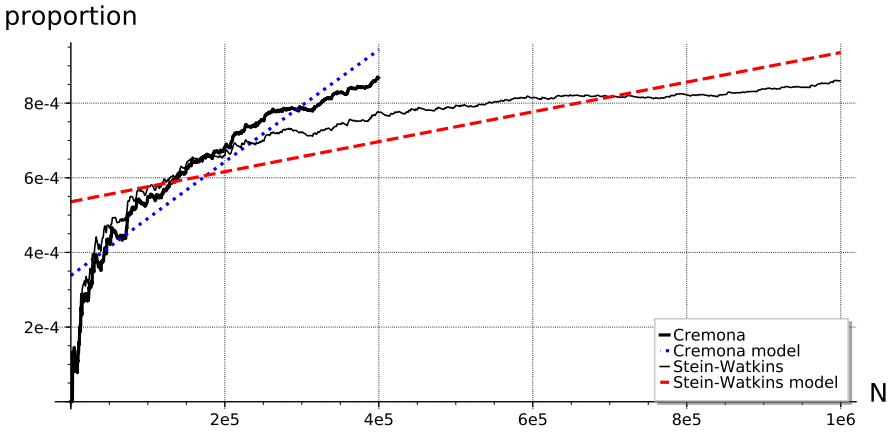

Figure 2.2: The proportion of rank 0 curves with $\operatorname{rank}_{\mathbb{F}_2} Ш(E/\mathbb{Q})[2] = 4$.

see [Del01, Examples B-E]. Therefore, among the curves of $\operatorname{rank}_{\mathbb{F}_2} Ш[2] = 2$*, one should expect* $1/2$ *of the curves to have* $\operatorname{ord}_2(\#Ш) = 2$*,* $1/4$ *of the curves to have* $\operatorname{ord}_2(\#Ш) = 4$*, and so on. In this case, the relative proportion of curves with* $\operatorname{ord}_2(\#Ш) = 2$ *starts around* 90% *and it is decreasing; the relative proportion of curves with* $\operatorname{ord}_2(\#Ш) = 4$ *starts around* 9% *and it is increasing. There are not many examples with* $\operatorname{ord}_2(\#Ш) > 4$*, and their relative proportions is too small to account them for. See figures 2.3, 2.4, 2.5, 2.6.*

2.3.5 Distribution when the order is divisible by 3

Proposition 5. *There are 73187 elliptic curves of rank* 0 *in our database where* $\#Ш(E/\mathbb{Q})$ *is divisible by* 3*. Assuming the BSD conjecture, the distribution of these curves by* $r_3Ш$ *and* $\operatorname{ord}_3 \#Ш(E/\mathbb{Q})$ *is given in tables 2.6 and 2.7.*

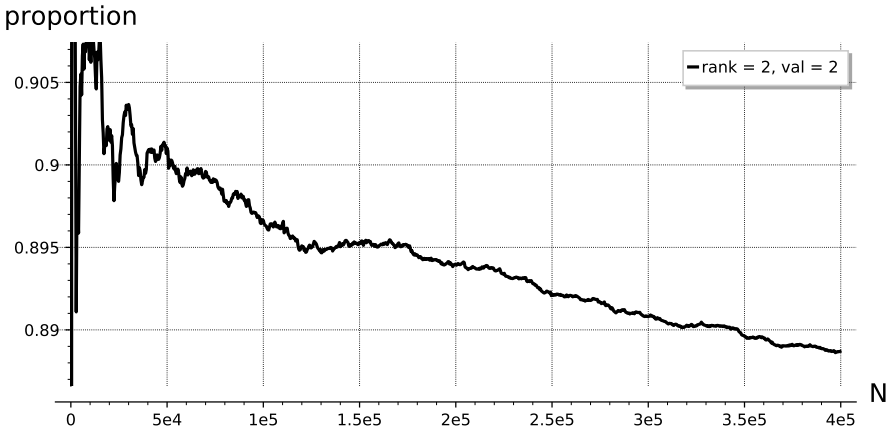

Figure 2.3: The proportion of rank 0 elliptic curves in Cremona's database with $\mathrm{ord}_2(\#Ш) = 2$ among these with $\mathrm{rank}_{\mathbb{F}_2} Ш(E/\mathbb{Q})[2] = 2$.

The strategy to determine the 3 primary part

I computed $r_3Ш := \mathrm{rank}_{\mathbb{F}_3} Ш(E/\mathbb{Q})[3]$. Using the torsion subgroup type of E as described above, I computed the order of the 3-Selmer group of E, i.e. $\#\,\mathrm{Sel}_3(E/\mathbb{Q})$, in *Magma* using three descent and assuming the **General Riemann Hypothesis** to speed up the computations. Recall that *Magma* returns only one element of each non-trivial pair of inverse elements, and the $\mathrm{Sel}_3(E/\mathbb{Q})$ cardinality is given by:

$$\#\,\mathrm{Sel}_3(E/\mathbb{Q}) = 3^s \cdot 3^{r_3Ш}$$

where

$$s = \begin{cases} 0 & \Leftarrow \quad \#E(\mathbb{Q})_{tor} \text{ is not divisible by 3} \\ 1 & \Leftarrow \quad \#E(\mathbb{Q})_{tor} \text{ is divisible by 3} \end{cases}$$

This is enough to determine the group type of $Ш(E/\mathbb{Q})(3)$ in the following cases:

1. If $\mathrm{ord}_3(\#Ш(E/\mathbb{Q})) = 2n$ and $r_3Ш = 2$, then

$$Ш(E/\mathbb{Q})(3) \cong (\mathbb{Z}/3^n\mathbb{Z})^2$$

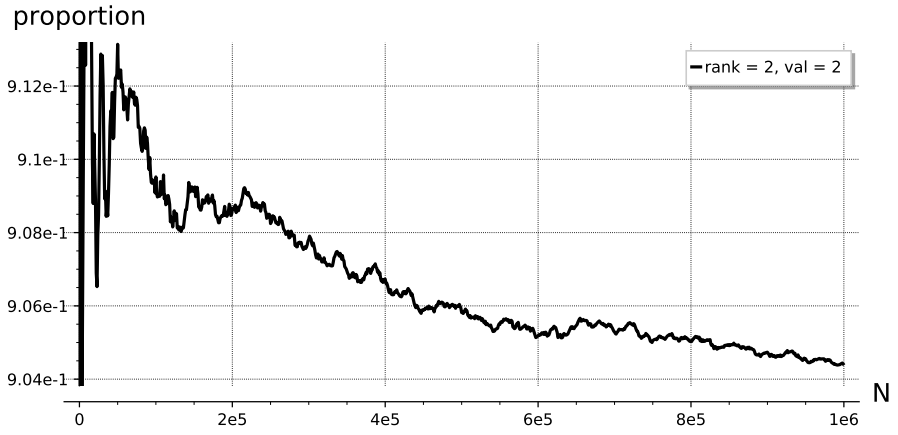

Figure 2.4: The proportion of rank 0 elliptic curves in Stein-Watkins' database with $\mathrm{ord}_2(\#Ш) = 2$ among these with $\mathrm{rank}_{\mathbb{F}_2} Ш(E/\mathbb{Q})[2] = 2$.

2. If $\mathrm{ord}_3(\#Ш(E/\mathbb{Q})) = 4$ and $r_3Ш = 4$, then

$$Ш(E/\mathbb{Q})(3) \cong (\mathbb{Z}/3\mathbb{Z})^4$$

Since these are all cases found, then I did not need to perform nine descent for these curves, which is implemented in *Magma*.

Asymptotic proportions

Recall that according to Delaunay's asymptotic proportions, 36.10% of rank 0 elliptic curves have $\#Ш(E/\mathbb{Q})$ divisible by 3.

Proposition 6. *While Delaunay predicted that* 35.94% *rank* 0 *rational elliptic curves have* $r_3Ш = 2$*, the best-fit statistical models of the form* $p = D - a\exp(bN)$ *for Cremona's and Stein-Watkins' rank* 0 *elliptic curves where* p *is the proportion of such curves up to conductor* N*, and* D *is Delaunay's proportion of such curves are given respectively by:*

$$p_{CRE} \approx 0.3594 - 0.3345 \cdot e^{-(1.68\times10^{-7})x}$$

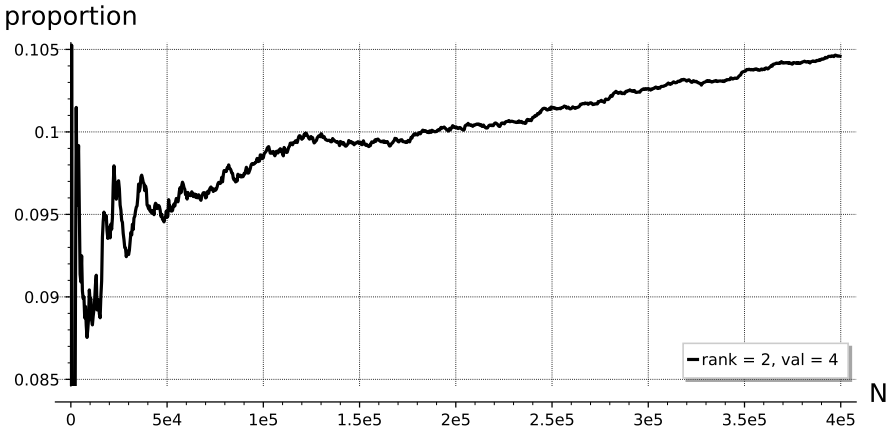

Figure 2.5: The proportion of rank 0 elliptic curves in Cremona's database with $\mathrm{ord}_2(\#Ш) = 4$ among these with $\mathrm{rank}_{\mathbb{F}_2} Ш(E/\mathbb{Q})[2] = 2$.

$$p_{SW} \approx 0.3594 - 0.3329 \cdot e^{-(4.86\times 10^{-8})x}$$

Moreover, these models suggest that one would need to compute all rank 0 *elliptic curves up to conductors* $1.3 \times 10^7, 1.7 \times 10^7, 2.7 \times 10^7$ *for Cremona's database, and up to conductors* $4.6 \times 10^7, 6.0 \times 10^7, 9.3 \times 10^7$ *for Stein-Watkins' database in order to achieve* $90\%, 95\%, 99\%$ *of Delaunay's proportion respectively. See figure 2.7.*

Proposition 7. *While Delaunay predicted that* 0.15% *rank* 0 *rational elliptic curves have* $\mathrm{rank}_{\mathbb{F}_3} Ш(E/\mathbb{Q})(3) = 4$*, the best-fit statistical models of the form* $p = D - a\exp(bN)$ *for Cremona's and Stein-Watkins' rank* 0 *elliptic curves where* p *is the proportion of such curves up to conductor* N*, and* D *is Delaunay's proportion of such curves are given respectively by:*

$$p_{CRE} \approx 0.0015 - 0.0015 \cdot e^{-(2.76\times 10^{-8})x}$$

$$p_{SW} \approx 0.0015 - 0.0015 \cdot e^{-(4.39\times 10^{-9})x}$$

Moreover, these models suggest that one would need to compute all rank 0 *elliptic curves up to conductors* $8.3 \times 10^7, 1.1 \times 10^8, 1.7 \times 10^8$ *for Cremona's database, and up to conductors*

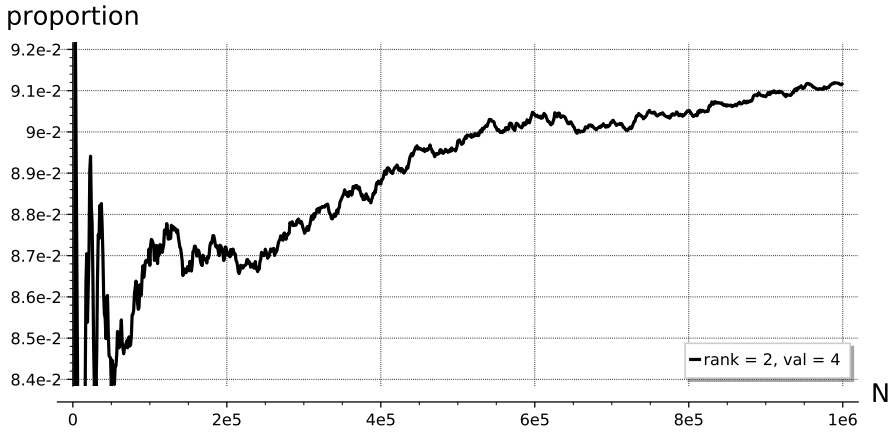

Figure 2.6: The proportion of rank 0 elliptic curves in Stein-Watkins' database with $\mathrm{ord}_2(\#Ш) = 4$ among these with $\mathrm{rank}_{\mathbb{F}_2} Ш(E/\mathbb{Q})[2] = 2$.

$5.2 \times 10^8, 6.8 \times 10^8, 1.0 \times 10^9$ *for Stein-Watkins' database in order to achieve* $90\%, 95\%, 99\%$ *of Delaunay's proportion respectively. See figure 2.8.*

2.3.6 Distribution when the order is divisible by 5

Proposition 8. *There are 10049 curves where* $\#Ш(E/\mathbb{Q})$ *is divisible by* 5*. In all but twelve of these curves,* $\mathrm{ord}_5(\#Ш(E/\mathbb{Q})) = 2$ *and thus* $Ш(E/\mathbb{Q})(5) \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$*. For the remaining twelve curves* $\mathrm{ord}_5(\#Ш(E/\mathbb{Q})) = 4$ *and they are listed in table 2.8. See [Fis].*

Remark 7. *As well as in the cases for* $p = 2$ *and* $p = 3$*, from here on out I will denote* $r_p Ш := \mathrm{rank}_{\mathbb{F}_p} Ш(E/\mathbb{Q})(p)$.

Proposition 9. *Delaunay predicted that* 20.67% *rank* 0 *rational elliptic curves have the order of their Tate-Shafarevich group* $\#Ш(E/\mathbb{Q})$ *divisible by* 5*, most of them with* $r_5 Ш = 2$*. The best-fit statistical models of the form* $p = D - a\exp(bN)$ *for Cremona's and Stein-Watkins' rank* 0 *elliptic curves where* p *is the proportion of such curves up to conductor* N*, and*

$\text{rank}_{\mathbb{F}_3}$ Ш[3] $\text{ord}_3(\#Ш)$	2	npm	4	npm	Total	npm
2	40831	989338	–	––	40831	989338
4	421	10200	18	436	439	10637
6	1	24	0	0	1	24
Total	41253	999563	18	436	41271	1000000

Table 2.6: Cremona's rank 0 elliptic curves with #Ш divisible by 3.

$\text{rank}_{\mathbb{F}_3}$ Ш[3] $\text{ord}_3(\#Ш)$	2	npm	4	npm	Total	npm
2	54849	992760	0	0	54849	992760
4	385	6968	14	253	399	7221
6	0	0	1	18	1	18
Total	55234	999728	15	271	55249	1000000

Table 2.7: Stein-Watkins's rank 0 elliptic curves with #Ш divisible by 3.

$D \approx 0.1653$ is Delaunay's proportion of curves with $Ш(5) \cong (\mathbb{Z}/5\mathbb{Z})^2$ *are given respectively by:*

$$p_{CRE} \approx 0.1.65 - 0.161e^{-(5.86\times10^{-8})x}$$

$$p_{SW} \approx 0.165 - 0.162e^{-(1.25\times10^{-8})x}$$

Moreover, p_{CRE} suggest that one would need to compute all rank 0 elliptic curves up to conductors 3.88×10^7, 5.07×10^7, 7.81×10^7 and all rank 0 elliptic curves of discriminant $|\Delta| \leq 10^{12}$ bounded by up to conductors 1.83×10^8, 2.38×10^8, 3.67×10^8 in order to achieve $90\%, 95\%, 99\%$ of Delaunay's proportion respectively. See figure 2.9.

n	a-inv	$\text{rank}_{\mathbb{F}_5}\, Ш(5)$
132858	[1,-1,1,-127693145273,-17562999979494021]	2
165066	[1,0,0,-1773878330125,-909355979228841397]	4
287175	[1,1,0,-190814326171875,-1014529347971625321000]	2
287175	[1,1,0,-190814176635750,-1014531017596742559375]	2
287175	[1,1,0,-3053029218750000,-64929874453897846024125]	2
287175	[1,1,0,-11925904731750,-15851998701003965625]	2
287175	[1,1,0,-12089534653625,-15394625415906543750]	2
287175	[1,1,0,-735151521625,-254808079119776000]	2
321398	[1,-1,0,-1531069681,-23060083371235]	2
366100	[0,-1,0,-4466595048333,-3633396603029145463]	?
387838	[1,0,0,-33887345256,-2401070685435262]	?
729243	[0,0,1,-59554359,-176896176271]	?

Table 2.8: Elliptic Curves whose Tate-Shafarevich order is divisible by 625.

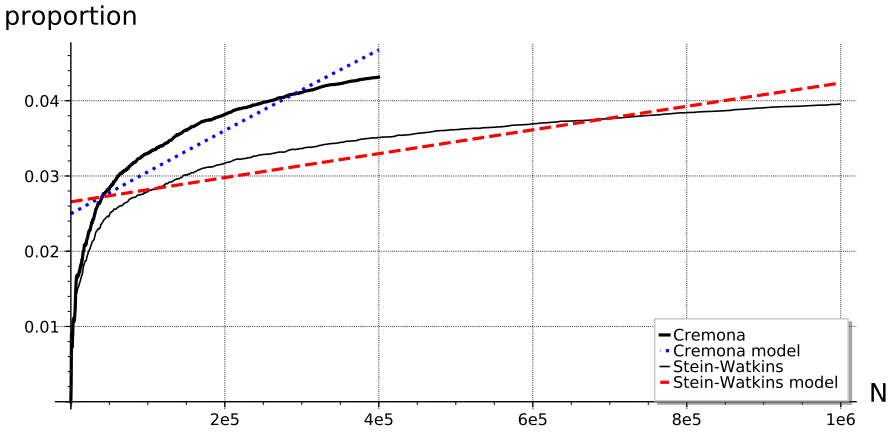

Figure 2.7: The proportion of rank 0 elliptic curves with $\text{rank}_{\mathbb{F}_3} Ш(E/\mathbb{Q})[3] = 2$.

Remark 8. *The peaks in this bumpy graph are due to how sporadic the examples are. Every example bumps the proportion, and they are usually followed by several non-examples, which bring down the proportion again.*

2.3.7 Asymptotic proportion for larger primes

Proposition 10. *Delaunay predicted that* 14.54% *rank* 0 *rational elliptic curves have the order of their Tate-Shafarevich group* $\#Ш(E/\mathbb{Q})$ *divisible by* 7*, most of them with* $r_7 Ш = 2$*. The best-fit statistical models of the form* $p = D - a\exp(bN)$ *for Cremona's and Stein-Watkins' rank* 0 *elliptic curves where* p *is the proportion of such curves up to conductor* N*, and* $D \approx 0.1246$ *is Delaunay's proportion of curves with* $Ш(7) \cong (\mathbb{Z}/7\mathbb{Z})^2$ *are given respectively by:*

$$p_{CRE} \approx 0.125 - 0.124 \cdot e^{-(1.93\times 10^{-8})x}$$

$$p_{SW} \approx 0.125 - 0.124 \cdot e^{-(4.79\times 10^{-9})x}$$

Moreover, these models suggest that one would need to compute all rank 0 *elliptic curves up to conductors* 1.19×10^8*,* 1.55×10^8*,* 2.38×10^8 *and all rank* 0 *elliptic curves of discriminant* $|\Delta| \leq 10^{12}$ *up to conductors* 4.8×10^8*,* 6.25×10^8*,* 9.61×10^8 *in order to achieve* $90\%, 95\%, 99\%$

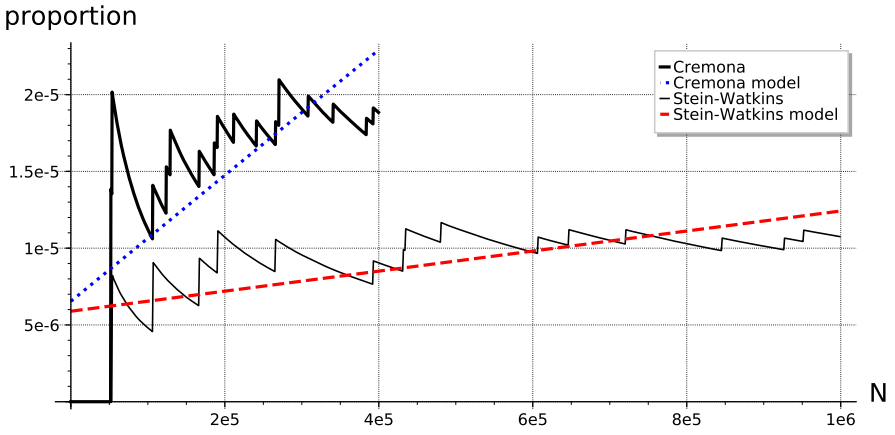

Figure 2.8: The proportion of rank 0 elliptic curves with $\text{rank}_{\mathbb{F}_3} Ш(E/\mathbb{Q})[3] = 4$.

of Delaunay's proportion respectively. See figure 2.10.

Proposition 11. *Delaunay predicted that* 9.16% *rank* 0 *rational elliptic curves have have the order of their Tate-Shafarevich group* $\#Ш(E/\mathbb{Q})$ *divisible by* 11*, most of them with* $r_{11}Ш = 2$*. The best-fit statistical models of the form* $p = D - a\exp(bN)$ *for Cremona's and Stein-Watkins' rank* 0 *elliptic curves where* p *is the proportion of such curves up to conductor* N*, and* $D \approx 0.0833$ *is Delaunay's proportion of curves with* $Ш(11) \cong (\mathbb{Z}/11\mathbb{Z})^2$ *is given by:*

$$p_{CRE} \approx 0.0833 - 0.0832 \cdot e^{-(5.63\times10^{-9})x}$$

That for Stein-Watkins' curves is given by

$$p_{SW} \approx 0.0833 - 0.0833 \cdot e^{-(8.74\times10^{-10})x}$$

Moreover, these models suggest that one would need to compute all rank 0 *elliptic curves up to conductors* 4.09×10^8*,* 5.32×10^8*,* 8.18×10^8 *and all rank* 0 *elliptic curves of discriminant* $|\Delta| \leq 10^{12}$ *up to conductors* 2.64×10^9*,* 3.43×10^9*,* 5.27×10^9 *in order to achieve* 90%, 95%, 99% *of Delaunay's proportion respectively. See figure 2.11.*

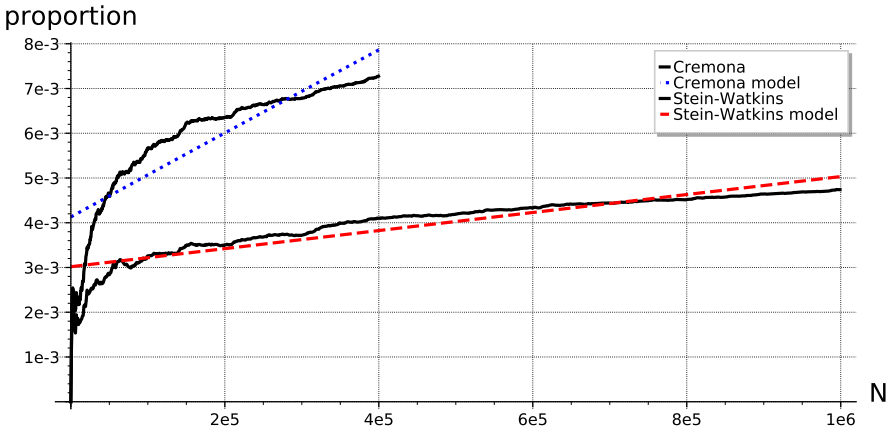

Figure 2.9: On the proportion of rank 0 elliptic curves with $\text{rank}_{\mathbb{F}_5} Ш(E/\mathbb{Q})[5] = 2$.

Proposition 12. *Delaunay predicted that* 7.33% *rank* 0 *rational elliptic curves have the order of their Tate-Shafarevich group* $\#Ш(E/\mathbb{Q})$ *divisible by* 13*, most of them with* $r_{13}Ш = 2$*. The best-fit statistical models of the form* $p = D - a\exp(bN)$ *for Cremona's and Stein-Watkins' rank* 0 *elliptic curves where* p *is the proportion of such curves up to conductor* N*, and* $D \approx 0.0714$ *is Delaunay's proportion of curves with* $Ш(13) \cong (\mathbb{Z}/13\mathbb{Z})^2$ *are given respectively by:*

$$p_{CRE} \approx 0.0714 - 0.0714 \cdot e^{-(4.13\times 10^{-9})x}$$

$$p_{SW} \approx 0.0714 - 0.0714 \cdot e^{-(3.59\times 10^{-10})x}$$

Moreover, these models suggest that one would need to compute all rank 0 *elliptic curves up to conductors* 5.58×10^8*,* 7.25×10^8*,* 1.12×10^9 *all rank* 0 *elliptic curves of discriminant* $|\Delta| \leq 10^{12}$ *up to conductors* 6.41×10^9*,* 8.34×10^9*,* 1.28×10^{10} *in order to achieve* $90\%, 95\%, 99\%$ *of Delaunay's proportion respectively. See figure 2.12.*

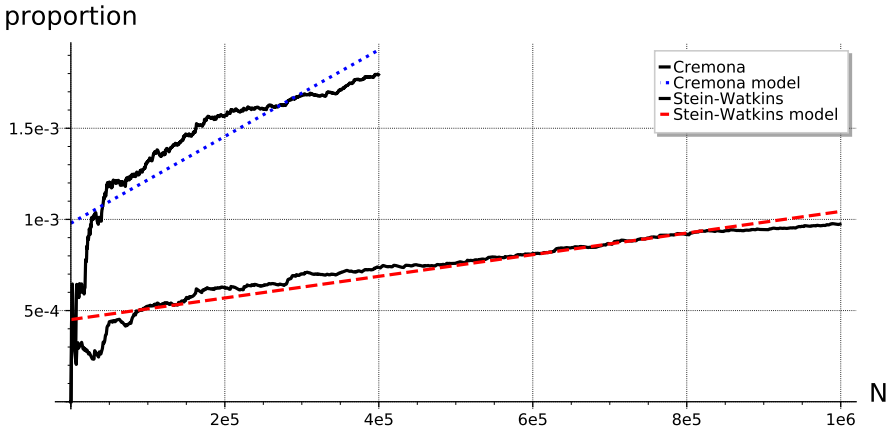

Figure 2.10: On the proportion of rank 0 elliptic curves with $\mathrm{rank}_{\mathbb{F}_7} Ш(E/\mathbb{Q})[7] = 2$.

2.4 Elliptic curves of rank 1

2.4.1 Origin of the tables

I took all rank 1 rational elliptic curves from Cremona's database and all elliptic curves from Stein-Watkins' database up to conductor 10^6, which only contain elliptic curves whose discriminant $|\Delta| \leq 10^{12}$. For the 2263284 elliptic curves of rank 1, I took the torsion order tor, the Tamagawa product tam, the leading coefficient lc of the associated L-series. The main difference with the rank 0 case is that for elliptic curves only in Stein-Watkins' database, I did not have their regulator, a non-torsion generator, and the order of their Tate-Shafarevich group. The origins of the curves are summarized in table 2.9.

2.4.2 Strategy for rank 1 rational elliptic curves

Given a rank 1 rational elliptic curve, known through the a-invariants of its minimal equation, where I did not know any non-torsion element of the Mordell-Weil group $E(\mathbb{Q})$, I wanted to compute its Tate-Shafarevich group order and type. However, in some cases, I was just able to find an upper bound $B_{Ш}$ on its Tate-Shafarevich group order. My strategy is presented below. Over the following steps, I always assumed that the **strong Birch and Swinnerton-**

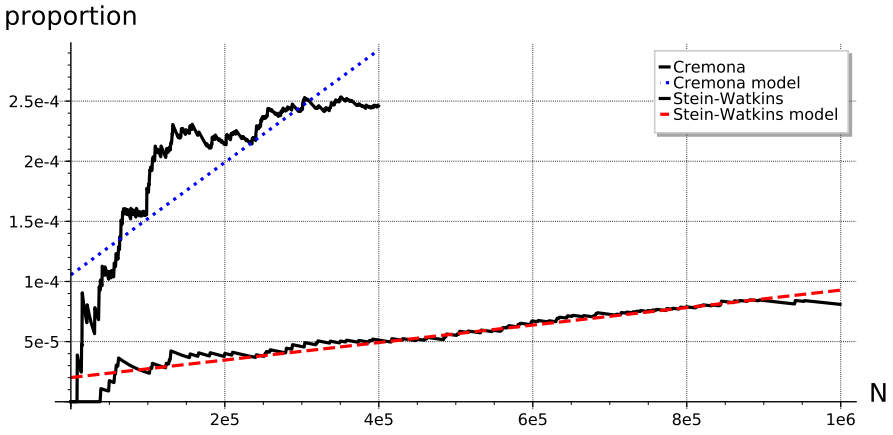

Figure 2.11: On the proportion of rank 0 elliptic curves with $\text{rank}_{\mathbb{F}_{11}} Ш(E/\mathbb{Q})[11] = 2$.

Dyer conjecture on elliptic curves holds, and through certain steps, I also assume the **Generalized Riemann Hypothesis** and Mazur's et. al ***p*-adic BSD strong conjecture** in the case of a prime of good ordinary reduction.

What the BSD conjecture says

I used the BSD conjecture to compute $\text{reg}(E) \cdot \#Ш(E/\mathbb{Q})$:

$$\text{reg}(E) \cdot \#Ш(E/\mathbb{Q}) = L'(E,1) \cdot \frac{(\#E(\mathbb{Q})_{tor})^2}{\prod_p \tau_p \cdot \Omega_E}$$

Using Point Searches to bound the regulator

I computed the Cremona-Prickett-Siksek height bound cps using *SageMath*, which is a floating point number such that if P is a rational point on E, then:

$$h(P) \leq \hat{h}(P) + \text{cps}$$

where $h(P)$ and $\hat{h}(P)$ are the naive logarithmic and the canonical heights of P respectively.

I also ran a point search up to the naive logarithmic height psb, which reads *point search bound*, using *SageMath*, which includes Prickett's saturation algorithm. In general, I picked

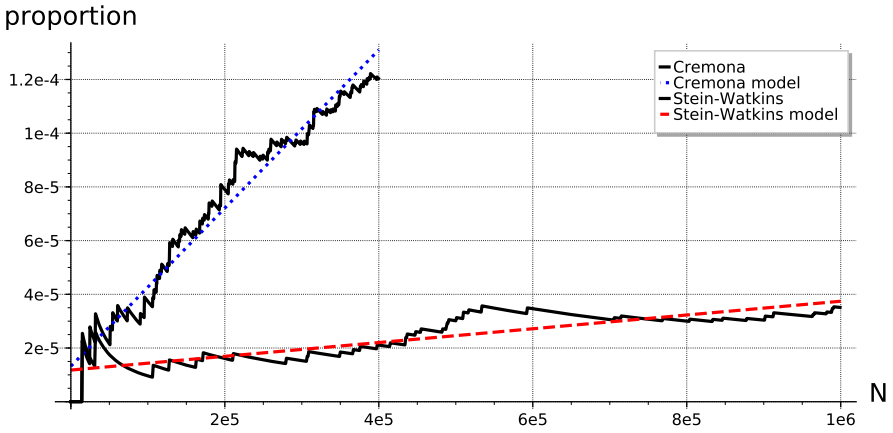

Figure 2.12: On the proportion of rank 0 elliptic curves with $\text{rank}_{\mathbb{F}_{13}} Ш(E/\mathbb{Q})[13] = 2$.

$\text{psb} > \text{cps} + \delta$, so if the search did not return a generator, I found a lower bound of $\text{reg}(E)$ and thus an upper bound of $\#Ш(E/\mathbb{Q})$. Indeed, any non-torsion generator P with minimal naive logarithmic height $h(P)$ has $\text{psb} < h(P)$, thus:

$$\text{psb} < h(P) < \hat{h}(P) + \text{cps} \Rightarrow \hat{h}(P) > \text{psb} - \text{cps}$$

Remark 9. *In practice, since I had a long dataset, I initially ran point searches up to* $\text{psb} = 12$, $\text{psb} = 16$, *and* $\text{psb} = 18$. *However, notice that a point search up to* $\text{psb} = \text{cps} + \text{reg}(E) \cdot \#Ш(E/\mathbb{Q})$ *guarantees to find a generator, and a point search up to* $\text{cps} + \frac{\text{reg}(E) \cdot \#Ш(E/\mathbb{Q})}{n^2} + \delta$ *either finds a generator, or determines that* $\#Ш(E/\mathbb{Q}) < n^2$. *Moreover,* $\delta > 0$ *is a term to avoid precision errors, and to guarantee strict inequality. In practice I used* $\delta \in [0.05, 0.2]$.

Whenever I found a non-torsion point P, I knew $\hat{h}(P) = \text{reg}(E)$. Thus,

$$\#Ш(E/\mathbb{Q}) = \frac{\text{reg}(E) \cdot \#Ш(E/\mathbb{Q})}{\hat{h}(P)}$$

If the search did not return a point, then I had a primitive upper bound on the Tate-Shafarevich group order:

$$\#Ш(E/\mathbb{Q}) \leq B_{Ш} := \frac{\text{reg}(E) \cdot \#Ш(E/\mathbb{Q})}{\text{psb} - \text{cps}}$$

Moreover, in many cases I obtained $B_{Ш} = 1$. Hence, I have $\#Ш(E/\mathbb{Q}) = 1$.

$\lfloor \frac{n}{10^5} \rfloor$	CRE	SW	%
0	332314	263834	14.68
1	314745	223189	13.91
2	303375	203801	13.4
3	296103	193912	13.08
4	0	183312	8.1
5	0	176755	7.81
6	0	171440	7.57
7	0	166382	7.35
8	0	161661	7.14
9	0	157197	6.95
Total	1246537	1901483	2263284

Table 2.9: Origin of rank 1 rational elliptic curves.

Using descent methods in Magma

I computed $r_2Ш := \text{rank}_{\mathbb{F}_2} Ш(E/\mathbb{Q})[2]$. I first computed the torsion subgroup type of E, which by Lutz-Nagel's theorem and Mazur's theorem, I can identify $E(\mathbb{Q})_{\text{tor}}$ with one of the following groups:

$$\{\mathbb{Z}/n\mathbb{Z} : 1 \leq n \leq 10, \text{ or } n = 12\} \cup \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} : 1 \leq n \leq 4\}$$

Then I computed the order of the 2-Selmer group of E, i.e. $\#\,\text{Sel}_2(E/\mathbb{Q})$, in *Magma* by performing two descent. Recall that *Magma* returns all elements but the trivial one, and the $\text{Sel}_2(E/\mathbb{Q})$ cardinality is given by:

$$\#\,\text{Sel}_2(E/\mathbb{Q}) = 2^{t+1} \cdot 2^{r_2Ш}$$

where

$$t = \begin{cases} 0 & \Leftarrow \quad E(\mathbb{Q})_{tor} \in \{\mathbb{Z}/n\mathbb{Z} : n \text{ is odd}\} \\ 1 & \Leftarrow \quad E(\mathbb{Q})_{\text{tor}} \in \{\mathbb{Z}/n\mathbb{Z} : n \text{ is even}\} \\ 2 & \Leftarrow \quad E(\mathbb{Q})_{\text{tor}} \in \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} : 1 \leq n =\leq 4\} \end{cases}$$

Similarly, I computed $r_3Ш := \text{rank}_{\mathbb{F}_3} Ш(E/\mathbb{Q})[3]$. I computed the order of the 3-Selmer group of E, i.e. $\#\,\text{Sel}_3(E/\mathbb{Q})$, in *Magma* by performing three descent. Since three descent requires to compute units in a number field, and this in turn requires knowledge of its ideal class group, then one may assume the **General Riemann Hypothesis** to speed up the computations. Recall that *Magma* only returns one element of each non-trivial pair of inverse elements, that means *Magma* returns only $\frac{1}{2}(\#\,\text{Sel}_3(E/\mathbb{Q})-1)$ elements of $\text{Sel}_3(E/\mathbb{Q})$, and the $\text{Sel}_3(E/\mathbb{Q})$ cardinality is given by:

$$\#\,\text{Sel}_3(E/\mathbb{Q}) = 3^{s+1} \cdot 3^{r_3Ш}$$

where

$$s = \begin{cases} 0 & \Leftarrow \quad E(\mathbb{Q})_{tor} \in \{\mathbb{Z}/n\mathbb{Z} : n \text{ is not divisible by } 3\} \\ & \qquad \cup \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} : n \in \{1, 2, 4\}\} \\ 1 & \Leftarrow \quad E(\mathbb{Q})_{\text{tor}} \in \{\mathbb{Z}/n\mathbb{Z} : n \text{ is divisible by } 3\} \\ & \qquad \cup \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}\} \end{cases}$$

Furthermore, I used these ranks of Ш to update the psb and to run another point search in some cases, and to improve the primitive bound $B_Ш$ in some case. Indeed, if $r_2Ш = 2r$ and $r_3Ш = 2s$, I did another point search up to

$$\text{psb} = \text{cps} + \frac{\text{reg}(E) \cdot \#Ш(E/\mathbb{Q})}{2^{2r} \cdot 3^{2s} \cdot 25} + \delta$$

whenever this satisfies $\text{psb} < 25$, and where δ is a term added for precision. If the search found a generator P, then I proceeded as above. But if the search did not find a generator, then $\#Ш(E/\mathbb{Q}) = 2^{2(r+\rho)} \cdot 3^{2(s+\sigma)}$ where $1 \leq 2^\rho \cdot 3^\sigma < 25$, $r = 0 \Rightarrow \rho = 0$ and $s = 0 \Rightarrow \sigma = 0$, i.e. $B_Ш = 2^{2(r+\max(\rho))} \cdot 3^{2(s+\max(\sigma))}$.

In some cases, I computed the number of 2-coverings of E that have 4-covering curves obtained by performing four descent on each of the elements of $Sel_2(E/\mathbb{Q})$. Similarly, I

computed the number of 4-coverings of E that have 8-covering curves obtained by performing eight descent on these 4-coverings.

Indeed, let E be an elliptic curve of rank r such that the 8-torsion part of its Tate-Shafarevich group satisfies:

$$Ш(E/\mathbb{Q})[8] \cong \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{2\lambda_1} \times \left(\frac{\mathbb{Z}}{4\mathbb{Z}}\right)^{2\lambda_2} \times \left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^{2\lambda_3}$$

and let $\Lambda = \lambda_1 + \lambda_2 + \lambda_3$. Then one notices the following results depending on the torsion subgroup of $E(\mathbb{Q})$:

No	$E(\mathbb{Q})_{tor}$	$\frac{E(\mathbb{Q})_{tor}}{2E(\mathbb{Q})_{tor}}$	$\frac{E(\mathbb{Q})_{tor}}{4E(\mathbb{Q})_{tor}}$	$\frac{E(\mathbb{Q})_{tor}}{8E(\mathbb{Q})_{tor}}$
1	$\{\mathbb{Z}/n\mathbb{Z}\}_{n=1,3,5,7,9}$	$\{0\}$	$\{0\}$	$\{0\}$
2	$\{\mathbb{Z}/n\mathbb{Z}\}_{n=2,6,10}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$
3	$\{\mathbb{Z}/n\mathbb{Z}\}_{n=4,12}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$
4	$\{\mathbb{Z}/n\mathbb{Z}\}_{n=8}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z}$
5	$\{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}\}_{n=1,3}$	$(\mathbb{Z}/2\mathbb{Z})^2$	$(\mathbb{Z}/2\mathbb{Z})^2$	$(\mathbb{Z}/2\mathbb{Z})^2$
6	$\{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}\}_{n=2}$	$(\mathbb{Z}/2\mathbb{Z})^2$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
7	$\{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}\}_{n=4}$	$(\mathbb{Z}/2\mathbb{Z})^2$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$

And from the short exact sequence:

$$0 \to \frac{E(\mathbb{Q})}{nE(\mathbb{Q})} \to \mathrm{Sel}_n(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[n] \to 0$$

one can deduce the orders of $\mathrm{Sel}_2(E/\mathbb{Q}), \mathrm{Sel}_4(E/\mathbb{Q}), \mathrm{Sel}_8(E/\mathbb{Q})$ in the corresponding case:

No	$\#\,\mathrm{Sel}_2(E/\mathbb{Q})$	$\#\,\mathrm{Sel}_4(E/\mathbb{Q})$	$\#\,\mathrm{Sel}_8(E/\mathbb{Q})$
1	$2^{r+2\Lambda}$	$2^{2r+2\lambda_1+2(\Lambda-\lambda_1)}$	$2^{3r+2\lambda_1+4\lambda_2+6\lambda_3}$
2	$2^{1+r+2\Lambda}$	$2^{1+2r+2\lambda_1+2(\Lambda-\lambda_1)}$	$2^{1+3r+2\lambda_1+4\lambda_2+6\lambda_3}$
3	$2^{1+r+2\Lambda}$	$2^{2+2r+2\lambda_1+2(\Lambda-\lambda_1)}$	$2^{2+3r+2\lambda_1+4\lambda_2+6\lambda_3}$
4	$2^{1+r+2\Lambda}$	$2^{2+2r+2\lambda_1+2(\Lambda-\lambda_1)}$	$2^{3+3r+2\lambda_1+4\lambda_2+6\lambda_3}$
5	$2^{2+r+2\Lambda}$	$2^{2+2r+2\lambda_1+2(\Lambda-\lambda_1)}$	$2^{2+3r+2\lambda_1+4\lambda_2+6\lambda_3}$
6	$2^{2+r+2\Lambda}$	$2^{3+2r+2\lambda_1+2(\Lambda-\lambda_1)}$	$2^{3+3r+2\lambda_1+4\lambda_2+6\lambda_3}$
7	$2^{2+r+2\Lambda}$	$2^{3+2r+2\lambda_1+2(\Lambda-\lambda_1)}$	$2^{4+3r+2\lambda_1+4\lambda_2+6\lambda_3}$

Notice that *Magma*'s two descent gives $2^{\mathrm{rank}(\mathrm{Sel}_2(E/\mathbb{Q}))}-1$ curves representing the nontrivial elements in $\mathrm{Sel}_2(E/\mathbb{Q})$. Then *Magma*'s four descent on each of these 2-coverings C of E gives either $2^{\mathrm{rank}(\mathrm{Sel}_2(E/\mathbb{Q}))-1}$ curves D in $\mathrm{Sel}_4(E/\mathbb{Q})$ covering C, or an empty list. By the definition of a 4-covering as in [Cas62a, Eq.1.12], the number of curves in $\mathrm{Sel}_2(E/\mathbb{Q})$ that have coverings in $\mathrm{Sel}_4(E/\mathbb{Q})$ is given by:

$$2^{\delta+r+2(\lambda_2+\lambda_3)} \text{ where } \delta = \begin{cases} 0 & \Leftarrow \text{ Case } 1 \\ 1 & \Leftarrow \text{ Cases } 2,3,4 \\ 2 & \Leftarrow \text{ Cases } 5,6,7 \end{cases}$$

For completeness, the forementioned equation is:

$$\begin{array}{ccccccccc} 0 & \to & \frac{E(\mathbb{Q})}{4E(\mathbb{Q})} & \to & \mathrm{Sel}_4(E/\mathbb{Q}) & \to & Ш(E/\mathbb{Q})[4] & \to & 0 \\ & & \downarrow i & & \downarrow u^* & & \downarrow & & \\ 0 & \to & \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} & \to & \mathrm{Sel}_2(E/\mathbb{Q}) & \to & Ш(E/\mathbb{Q})[2] & \to & 0 \end{array}$$

where i is induced by the identity map in $E(\mathbb{Q})$, and u^* is induced by the map the multiplication by 2 map $u : E[4] \to E[2]$.

Thus, even in the cases where I did not know a non-torsion generator of $E(\mathbb{Q})$, I was able to identify the group type of $Ш(E/\mathbb{Q})[4]$ by performing two and four descents. Moreover, I obtained similar results using also eight descent in very few cases where I could not find a non-torsion generator of $E(\mathbb{Q})$, $r_2Ш = 2$, and the upper bound on $\#Ш(E/\mathbb{Q})$ was 64.

What the p-adic BSD conjecture for primes of good ordinary reduction says

Finally, I assumed the **p-adic Birch and Swinnerton-Dyer conjecture** for the case of primes $p \geq 5$ of good ordinary reduction in order to attempt to rule out some primes dividing $\#Ш(E/\mathbb{Q})$. For a prime $p \geq 5$ of good ordinary reduction for E such that $p^2 < B_{Ш}$, I did the following:

1. I computed the p-adic L-series leading coefficient $\mathcal{L}_p^*(E, 0)$. These can be achieved for curves of large conductor due to Wuthrich's numerical modular symbols.

2. I computed the p-adic valuation v of $\#Ш(E/\mathbb{Q}) \cdot \mathrm{reg}_\gamma(E/\mathbb{Q})$, by computing that of the right hand side:

$$\#Ш(E/\mathbb{Q}) \cdot \mathrm{reg}_\gamma(E/\mathbb{Q}) = \mathcal{L}_p^*(E, 0) \cdot \frac{1}{\epsilon_p} \cdot \frac{(\#E(\mathbb{Q})_{tor})^2}{\prod_l \tau_l}$$

3. If the least common multiple of the Tamagawa numbers τ_l at the primes of bad reduction for E, and the number of points at the reduction of E at p, i.e. $\#\tilde{E}(\mathbb{F}_p)$ is not divisible by p, then $\mathrm{reg}_\gamma(E/\mathbb{Q}) \in \mathbb{Z}_p^*$, thus if $v = 0$, then p does not divide $\#Ш(E/\mathbb{Q})$.

Remark 10. *Assuming that $25 \leq \#Ш(E/\mathbb{Q}) \leq n^2$, then one starts attempting to use this result for the primes dividing $B_{Ш} = n^2$, and it is enough to prove that a prime $l|n$ does not divide $\#Ш(E/\mathbb{Q})$ to show that $B_{Ш} < n^2$.*

The results

There are 2229192 curves where $\#Ш(E/\mathbb{Q}) = 1$. As expected by Delaunay's conjectures, the proportion of elliptic curves with non-trivial Tate-Shafarevich group highly reduces for curves of positive rank as compared to this proportion for curves of rank 0. Moreover, I could not find the Tate-Shafarevich group order of 210 curves. And I found $\#Ш(E/\mathbb{Q})$ for 67 of these curves using the p-adic BSD conjecture. For all primes $p \geq 11$, I could not find a single example where $\#Ш(E/\mathbb{Q})$ is divisible by p, and only around 20 curves where I could

not find $\#Ш(E/\mathbb{Q})$ are candidates to generate such an example. For a proportion of rank 1 curves where $\#Ш(E/\mathbb{Q})$ is divisible by a prime see table 2.10.

p	No. in CRE	npm in CRE	No. in SW	npm in SW
2	14372	11530	26397	13882
3	1060	850	1753	921
5	69	55	56	29
7	9	7	6	3

Table 2.10: Number of rank 1 elliptic curves whose $\#Ш$ is divisible by a prime.

Remark 11. *For any of the curves here where* $p|\#Ш(E/\mathbb{Q})$ *with* $p \geq 5$*, the* p*-valuation of* $\#Ш(E/\mathbb{Q})$ *is exactly* 2*. Hence,* $Ш(E/\mathbb{Q})(p) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$*. Additionally, there is only one curve of conductor* 637392 *where* $\mathrm{ord}_3(\#Ш(E/\mathbb{Q})) = 4$ *and* $r_3Ш = 2$*, and thus*

$$Ш(E/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$$

See table 2.11 for Delaunay's conjectures on the p-primary parts of the Tate-Shafarevich group of rank 1 rational elliptic curves. For rank 1 curves,

p	$p\|\#Ш(E/\mathbb{Q})$	$\mathrm{r}_{\mathbb{F}_p}Ш(p) = 2$	$(\mathbb{Z}/p\mathbb{Z})^2$	$(\mathbb{Z}/p^2\mathbb{Z})^2$	$(\mathbb{Z}/p\mathbb{Z})^4$
2	16.116	15.978	13.981	1.748	0.117
3	4.149	4.147	3.994	0.148	0.002
5	0.833	0.833	0.826	0.007	0.0
7	0.298	0.298	0.297	0.001	0.0

Table 2.11: Delaunay's conjectured percentages for rank 1 rational elliptic curves.

Proposition 13. *Analogously to Brumer-McGuiness' and Watkins' heuristic, the best-fit log-log approximations for the numbers of rank* 1 *rational elliptic curves* $N_{cre}(X,1)$ *and* $N_{sw}(X,1)$ *of rank* 1 *rational elliptic curves in Cremona's and Stein-Watkins' databases are given respectively by:*

$$N_{cre}(X,1) = 5.3 \cdot X^{0.939}$$

$$N_{sw}(X,1) = 11.6 \cdot X^{0.849}$$

See figure 2.13

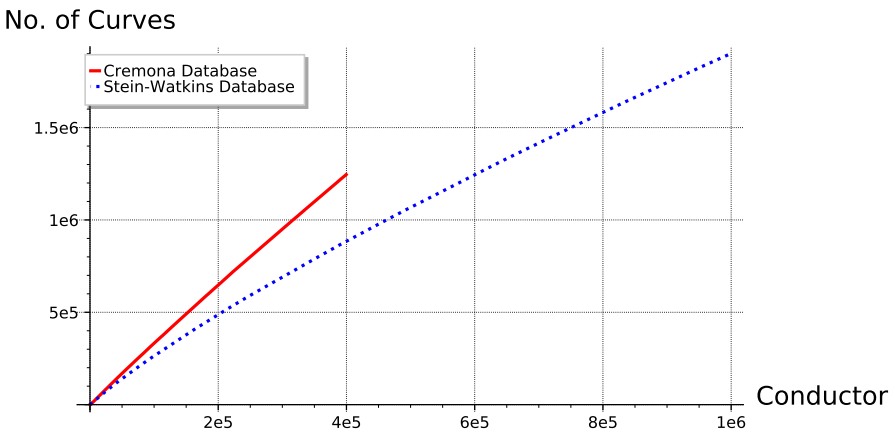

Figure 2.13: Number of rank 1 elliptic curves up to conductor N.

The Tate-Shafarevich group order and type is shown in table 2.12. Some estimates of an upper bound for the group order is given in table 2.13

Remark 12. *Recall that for all rank* 1 *elliptic curves in Cremona's database, which is about* 55% *of them, I took the generator from the database. On the other hand, for around* 90% *of the rank* 1 *rational elliptic curves exclusively in Stein-Watkins database, I found a non-torsion generator from a point search in SageMath of up to* cps $= 20$. *In some the rest, I performed point searches using Magma's functions Points, PointSearch, and PointsIQ on*

$\#Ш(E/\mathbb{Q})$	Gp Inv	Frequency
1	[1]	2229266
4	[2, 2]	30844
9	[3, 3]	2291
9	[4, 4]	1
16	[2, 2, 2, 2]	51
16	[4, 4]	496
25	[5, 5]	103
36	[2, 2, 3, 3]	4
49	[7, 7]	12
64	[2, 2, 4, 4]	1
64	[8, 8]	4
81	[9, 9]	1
None	None	210
	Total	2263284

Table 2.12: Frequency of Tate-Shafarevich group orders and types of rank 1 elliptic curves

the curves returned by two, three and four descent respectively. And then I saturated the generator obtained in SageMath.

2.4.3 Distribution when the order is divisible by 2.

Proposition 14. *There are* 31402 *elliptic curves of rank* 1 *and conductor up to* 10^6 *in our database where the order of their Tate-Shafarevich group* $\#Ш(E/\mathbb{Q})$ *is divisible by* 2*. Assuming the BSD conjecture, the distribution of these curves according to their* 2*-valuation* $\mathrm{ord}_2(\#Ш(E/\mathbb{Q}))$ *and their* $\mathbb{F}_2$*-rank* $r_2Ш$ *is given in table 2.14. Here npm means number of curves per million.*

$\#Ш(E/\mathbb{Q})$ bound	Frequency
25	120
49	75
100	2
121	10
169	3
Total	210

Table 2.13: Estimated bounds on $\#Ш$ for rank 1 elliptic curves whenever it is unknown.

$\text{rank}_{\mathbb{F}_2} Ш(E/\mathbb{Q})[2]$ $\text{ord}_2(\#Ш)$	2	npm	4	npm	Total	npm
2	30854	13632	0	0	30854	13632
4	461	203	41	18	502	221
6	4	1	1	0	5	2
Total	31319	13837	42	18	31361	13856

Table 2.14: Distribution of rank 1 elliptic curves with $\#Ш(E/\mathbb{Q})$ divisible by 2

Lemma 2. *Let E be an elliptic curve over $\mathbb{Q}$ with Tate-Shafarevich group order $\#Ш(E/\mathbb{Q})$ and $r_2Ш := \text{rank}_{\mathbb{F}_2} Ш(E/\mathbb{Q})[2]$. Let*

- *If $r_2Ш = 2$ and $\text{ord}_2(\#Ш(E/\mathbb{Q})) = 2v$, then*

$$Ш(E/\mathbb{Q})(2) \cong \frac{\mathbb{Z}}{2^v\mathbb{Z}} \times \frac{\mathbb{Z}}{2^v\mathbb{Z}}$$

- *If $r_2Ш = 4$ and $\text{ord}_2(\#Ш(E/\mathbb{Q})) = 4$, then*

$$Ш(E/\mathbb{Q})(2) \cong \frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$$

- *If* $r_2Ш = 4$ *and* $\mathrm{ord}_2(\#Ш(E/\mathbb{Q})) = 6$*, then*

$$Ш(E/\mathbb{Q})(2) \cong \frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$$

Remark 13. *Contrary to the rank* 0 *case, I didn't find any rank* 1 *elliptic curve with* $\#Ш(E/\mathbb{Q})$ *being divisible by* 64*, hence I did not need to perform Four Descent on any of these curves in order to obtain its Tate-Shafarevich group type. However, in some cases I found out that* $\#Ш(E/\mathbb{Q}) \leq 64$ *and* $r_2Ш = 2$*, and I needed to perform four descent and eight descent to find out* $\#Ш(E/\mathbb{Q})$*.*

2.4.4 Asymptotic Proportions

Recall that Delaunay predicted that around 16.1% of rank 1 elliptic curves ordered by conductor have $\#Ш(E/\mathbb{Q})$ divisible by 2, and most of them have $\mathrm{rank}_{\mathbb{F}_2} Ш(E/\mathbb{Q})[2] = 2$.

Proposition 15. *The best fit models of the form* $p = D - a\exp(bN)$ *where* D *is the Delaunay's conjectured proportion of rank* 1 *elliptic curves with* $\mathrm{rank}_{\mathbb{F}_2} Ш(E/\mathbb{Q})[2] = 2$ *for Cremona and Stein-Watkins databases are:*

$$y_{CRE} \approx 0.1598 - 0.1562 \cdot e^{-1.48\times10^{-7}\cdot x}$$

$$y_{SW} \approx 0.1598 - 0.1542 \cdot e^{-6.43\times10^{-8}\cdot x}$$

Moreover, these models predict that one would need to compute all rank 1 *elliptic curves up to conductors* 1.53×10^7*,* 2.00×10^7*,* 3.09×10^7*, or all rank* 1 *elliptic curves of absolute discriminant bounded by* 10^{12} *up to conductors* 3.52×10^7*,* 4.59×10^7*,* 7.09×10^7 *in order to achieve* 90%*,* 95%*, and* 99% *of Delaunay's proportion respectively. See figure 2.14.*

Proposition 16. *The best fit models of the form* $p = D - a\exp(bN)$ *where* D *is the Delaunay's conjectured proportion of rank* 1 *elliptic curves with* $\mathrm{rank}_{\mathbb{F}_2} Ш(E/\mathbb{Q})[2] = 4$ *for Cremona and Stein Watkins databases are:*

$$y_{CRE} \approx 0.0213 - 0.0213 \cdot e^{-1.64\times10^{-9}\cdot x}$$

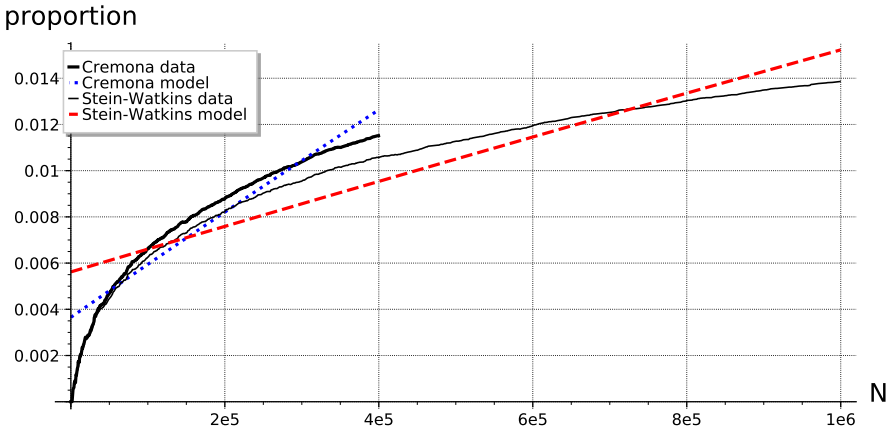

Figure 2.14: The proportion of rank 1 elliptic curves with $\text{rank}_{\mathbb{F}_2} Ш(E/\mathbb{Q})[2] = 2$.

$$y_{SW} \approx 0.0213 - 0.0213 \cdot e^{-1.22\times 10^{-9}\cdot x}$$

Moreover, these models predict that one would need to compute all rank 1 *elliptic curves up to conductors* 1.41×10^9, 1.83×10^9, 2.81×10^9, *or all rank* 1 *elliptic curves of absolute discriminant bounded by* 10^{12} *up to conductors* 1.90×10^9, 2.47×10^9, 3.79×10^9 *in order to achieve* 90%, 95%, *and* 99% *of Delaunay's proportion respectively. See figure 2.15.*

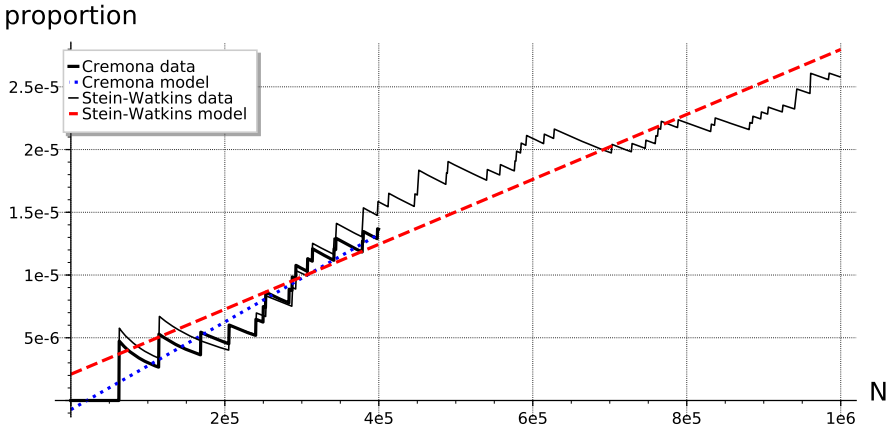

Figure 2.15: The proportion of rank 1 elliptic curves with $\text{rank}_{\mathbb{F}_2} Ш(E/\mathbb{Q})[2] = 4$.

Proposition 17. *The best fit models of the form* $p = D - a\exp(bN)$ *where* D *is the Delaunay's conjectured proportion of rank* 1 *elliptic curves with* $Ш(E/\mathbb{Q})(3) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ *for Cremona and Stein Watkins databases are:*

$$y_{CRE} \approx 0.0399 - 0.0397 \cdot e^{-4.36\times10^{-8}\cdot x}$$

$$y_{SW} \approx 0.0399 - 0.0397 \cdot e^{-2.34\times10^{-8}\cdot x}$$

Moreover, these models predict that one would need to compute all rank 1 *elliptic curves up to conductors* 5.3×10^7, 6.9×10^7, 1.1×10^8, *or all rank* 1 *elliptic curves of absolute discriminant bounded by* 10^{12} *up to conductors* 9.8×10^7, 1.3×10^8, 2.0×10^8 *in order to achieve* 90%, 95%, *and* 99% *of Delaunay's proportion respectively. See figure 2.16.*

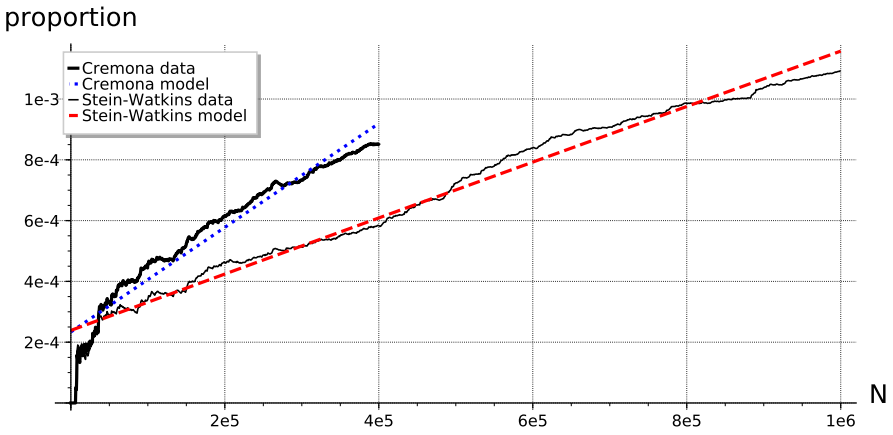

Figure 2.16: The proportion of rank 1 elliptic curves with $Ш(E/\mathbb{Q})(3) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Proposition 18. *The best fit models of the form* $D - a\exp(bN)$ *where* D *is the Delaunay's conjecture proportion of rank* 1 *elliptic curves with* $Ш(E/\mathbb{Q})(5) \cong \mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ *for Cremona and Stein-Watkins databases are:*

$$y_{CRE} \approx 0.0083 - 0.0082 \cdot e^{-1.1\times10^{-8}\cdot x}$$

$$y_{SW} \approx 0.0083 - 0.0083 \cdot e^{-2.7\times10^{-8}\cdot x}$$

Moreover, these models predict that one would need to compute all rank 1 *elliptic curves up to conductors* 2.1×10^8, 2.7×10^8, 4.1×10^8, *or all rank* 1 *elliptic curves of absolute discriminant bounded by* 10^{12} *up to conductors* 8.5×10^7, 1.1×10^8, 1.7×10^8 *in order to achieve* 90%, 95%, *and* 99% *of Delaunay's proportion respectively. See figure 2.17.*

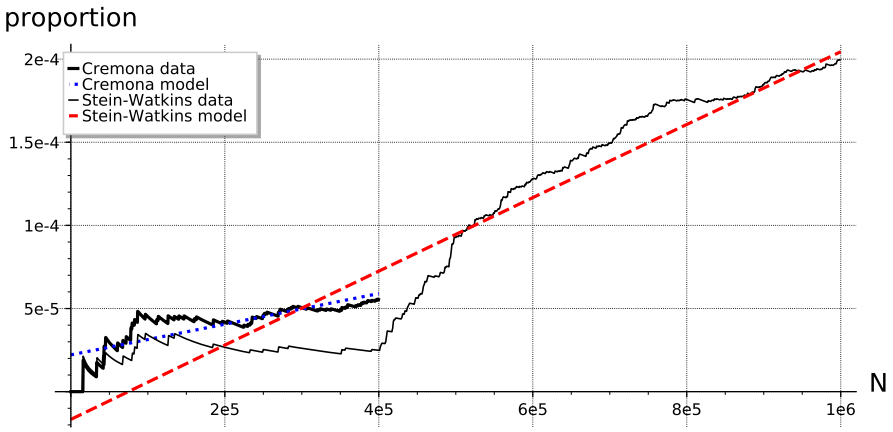

Figure 2.17: The proportion of rank 1 elliptic curves with $Ш(E/\mathbb{Q})(5) \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Proposition 19. *The best fit models of the form* $p = D - a\exp(bN)$ *where* D *is the Delaunay's conjectured proportion of rank* 1 *elliptic curves with* $Ш(E/\mathbb{Q})(7) \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ *for Cremona and Stein-Watkins databases are:*

$$y_{CRE} \approx 0.003 - 0.003 \cdot e^{-7.1\times10^{-10}\cdot x}$$

$$y_{SW} \approx 0.003 - 0.003 \cdot e^{-7.2\times10^{-8}\cdot x}$$

Moreover, these models predict that one would need to compute all rank 1 *elliptic curves up to conductors* 3.3×10^9, 4.2×10^9, 6.5×10^9, *or all rank* 1 *elliptic curves of absolute discriminant bounded by* 10^{12} *up to conductors* 3.2×10^7, 4.2×10^7, 6.4×10^7 *in order to achieve* 90%, 95%, *and* 99% *of Delaunay's proportion respectively. See figure 2.18.*

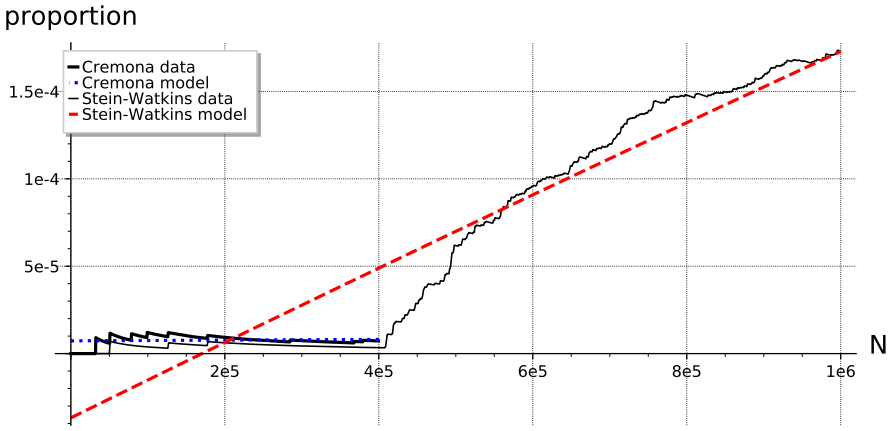

Figure 2.18: The proportion of rank 1 elliptic curves with $Ш(E/\mathbb{Q})(7) \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$.

2.5 Curves of rank larger than one

2.5.1 Construction of the tables

Similarly to the rank 1 case, I did not have non-torsion generators for curves exclusively in Stein-Watkins' database. Thus, I performed point searches using *SageMath* and *Magma* on all elliptic curves of rank larger than 1. In all cases where the rank $r \geq 3$, I found a full set of non-torsion generators for the Mordell-Weil group of each elliptic curve. Moreover, due to the following Diphantine inequality mentioned by Lang in [Lan83, §4], one expects not to need a long point search, as compared to these psb for curves of rank 1, in order to find the generators of these curves.

Remark 14. *Indeed, by theorem 1 and its corollary, one has:*

- *If E is an elliptic curve over $\mathbb{Q}$ of rank 2, and P is a point in the Mordell-Weil group $E(\mathbb{Q})$ of minimal positive canonical height $\hat{h}(P)$, then*

$$Reg(E) \geq \frac{3}{4}\hat{h}(P)^2$$

- *If E is an elliptic curve over $\mathbb{Q}$ of rank 3, and P is a point in the Mordell-Weil group*

$E(\mathbb{Q})$ *of minimal positive canonical height* $\hat{h}(P)$*, then*

$$Reg(E) \geq \frac{27}{64}\hat{h}(P)^3$$

For the sake of completeness, we prove the theorem here,

Theorem 1 (Lang)**.** *Let* L *be a lattice in* $\mathbb{R}^r$ *with a positive quadratic form called height* $h(v)$ *with corresponding height pairing given by* $\langle v, w\rangle = \frac{1}{2}\left(h(u+v) - h(u) - h(v)\right)$*. Then there exists an orthogonal basis* $\mathbb{R}^r = \langle u_1, \ldots, u_r\rangle_{\mathbb{R}}$ *and a basis* $L = \langle e_1, \ldots, e_r\rangle_{\mathbb{Z}}$ *satisfying:*

1. $e_1 = u_1$ *is a vector of minimal length in* L*, so* $h(e_1) = h(u_1)$*.*

2. *There are constants* $b_{i,j} \in \mathbb{R}$ *for* $1 \leq j < i \leq r$ *all satisfying* $|b_{i,j}| \leq 1/2$ *such that*

$$e_i = u_i + \sum_{j=1}^{i-1} b_{i,j}u_j$$

3. *For all* $i = 1, \ldots, r$*:* $h(u_i) \leq h(e_i) \leq \frac{4}{3}h(u_i)$*.*

4. *For all* $i = 1, \ldots, r-1$*:* $\frac{3}{4}h(u_{i-1}) \leq h(u_i)$*.*

Proof. First, choose $0 \neq e_1 \in L$ to be any vector of minimal height $h(e_i)$, and let $u_1 = e_1$. Then choose $0 \neq e_2 \in L$ to be any vector such that $u_2 := e_2 - \text{Proj}_{u_1} e_2$ has minimal height $h(u_2)$. Therefore, $e_2 = b'_{2,1}u_1 + u_2$ where $b'_{2,1} = \frac{\langle u_1, e_2\rangle}{h(u_1)}$. Decompose $b'_{2,1} = m + s$ where $m \in \mathbb{Z}$ and $s \in (-1/2, 1/2]$ and replace e_2 by $e_2 - me_1$, so $e_2 = b_{2,1}u_1 + u_2$ where $|b_{2,1}| \leq 1/2$. Clearly $h(e_2) = b_{2,1}^2 h(u_1) + h(u_2) \geq h(u_2)$. By the choice of e_1, $h(e_2) \geq h(e_1)$ or

$$b_{2,1}^2 h(u_1) + h(u_2) \geq (1 - b_{2,1}^2)h(u_1) \geq \frac{3}{4}h(u_1)$$

Therefore, $h(e_2) = b_{2,1}^2 h(u_1) + h(u_2) \leq \frac{4}{3}h(u_2)$.

Inductive Step: Having chosen linearly independent vectors $e_1, \ldots, e_{i-1}$ in L and orthogonal nonzero vectors $u_1, \ldots, u_{i-1}$ in $\mathbb{R}^r$, all with the given properties, choose $0 \neq e_i \in L$ to be any vector such that $u_i := e_i - \text{Proj}_{\langle u_1, \ldots, u_{i-1}\rangle} e_i$ has minimal height $h(u_i)$. Assume

$e_i = u_i + \sum_{j=1}^{i-1} b_{i,j}u_j$. Replace e_i by an appropriate vector $e_i - m_{i-1}e_{i-1}$ so $|b_{i,i-1}| \leq 1/2$; replace again e_i by an appropriate vector $e_i - m_{i-2}e_{i-2}$ so $|b_{i,i-2}| \leq 1/2$; etc. Then we obtain a vector $e_i = u_i + \sum_{j=1}^{i-1} b_{i,j}u_j \in L$ where all $|b_{i,j}| \leq 1/2$. Moreover, u_i remains unchanged. Thus by this choice:

$$\begin{aligned} h(u_{i-1}) &= h\left(\mathrm{Proj}_{\langle u_1,\ldots u_{i-2}\rangle} e_{i-1}\right) \\ &\leq h\left(\mathrm{Proj}_{\langle u_1,\ldots u_{i-2}\rangle} e_i\right) \\ &= h\left(u_i + b_{i,i-1}u_{i-1}\right) \\ &= h(u_i) + b_{i,i-1}^2 h(u_{i-1}) \end{aligned}$$

Therefore, $h(u_i) \geq (1 - b_{i,i-1}^2)h(u_{i-1}) \geq \frac{3}{4}h(u_{i-1})$ and moreover,

$$\begin{aligned} h(e_i) &= h(u_i) + \textstyle\sum_{j=1}^{i-1} b_{i,j}^2 h(u_j) \leq h(u_i) + \frac{1}{4}\sum_{j=1}^{i-1} \left(\frac{4}{3}\right)^{i-j} h(u_j) \\ &\leq \left(\frac{4}{3}\right)^{i-1} h(u_i) \end{aligned}$$

■

Corollary 1. *Given a lattice $L = \langle e_1, \ldots, e_r\rangle_{\mathbb{Z}}$ in $V = \langle u_1, \ldots, u_r\rangle_{\mathbb{R}}$ where these bases satisfy the conditions above, then*

$$\det(L) = \det\left(\langle e_i, e_j\rangle\right) = \prod_{i=1}^{r} h(u_i) \geq \left(\frac{3}{4}\right)^{r(r-1)/2} h(e_1)^r$$

After common point searches up to naive height 16, there were still several curves where one does not know a basis for the Mordell-Weil group.

Example 1. *The elliptic curve of rank* 2

$$E : y^2 + xy = x^3 - x^2 - 11672007426x - 485359836231992$$

has $\mathrm{reg} \cdot \#Ш(E/\mathbb{Q}) \approx 76.88$ *and* $\mathrm{cps} \approx 17.58$. *Assuming that* $\#Ш(E/\mathbb{Q}) = 1$, *by Lang's inequality, one would need to do a point search up to* 23.31 *in order to guarantee finding one generator. Yet a point search up to naive height* $\mathrm{psb} = 19.95$ *using SageMath gives us the generator of least canonical height* $1.53 < \mathrm{psb} - \mathrm{cps}$. *Hence, in order to guarantee finding the second generator, one would need to perform a point search up to naive height* 30.92.

Since one can compute $\text{rank}_{\mathbb{F}_2} Ш(E)$ and $\text{rank}_{\mathbb{F}_3} Ш(E)$ using *Magma* Descent methods, one can use the following bounds in order to guarantee that $\#Ш(E/\mathbb{Q}) < 25$ and thus being able to determine $\#Ш(E/\mathbb{Q})$:

Lemma 3. *Let $E/\mathbb{Q}$ be a rank 2 rational elliptic curve. Assume a point search up to naive height $\text{psb} > \text{cps} + \hat{h}_1$ returns only one generator P_1 of canonical height $\hat{h}_1 = \hat{h}_1(P_1)$ and no other generator. Then P_1 is the generator with minimal canonical height, and*

$$\#Ш(E/\mathbb{Q}) < \frac{\text{reg}(E) \cdot \#Ш(E/\mathbb{Q})}{(\text{psb} - \text{cps} - \hat{h}_1/4)\hat{h}_1}$$

Proof. Assume that $\#Ш(E/\mathbb{Q}) = n^2$, then $\text{reg}(E) = \frac{\text{reg}(E)\cdot\#Ш(E/\mathbb{Q})}{n^2}$, which in the notation of theorem 1 translates as:

$$\hat{h}_1(u_1)\hat{h}(u_2) = \frac{\text{reg}(E) \cdot \#Ш(E/\mathbb{Q})}{n^2} \Rightarrow \hat{h}(u_2) = \frac{\text{reg}(E) \cdot \#Ш(E/\mathbb{Q})}{n^2\hat{h}_1(e_1)}$$

And thus

$$\text{psb} - \text{cps} < \hat{h}(P_2) \leq \frac{\text{reg}(E) \cdot \#Ш(E/\mathbb{Q})}{n^2\hat{h}_1(e_1)} + \frac{\hat{h}_1(e_1)}{4}$$

Therefore, the result follows. ■

Corollary 2. *Assume $E/\mathbb{Q}$ is a rank 2 rational elliptic curve with $r_2Ш = r_3Ш = 0$. Also assume that a point search up to naive height $\text{psb} > \text{cps} + \hat{h}_1$ only finds a generator P_1 of canonical height $\hat{h}_1 = \hat{h}_1(P_1)$, and no other generator. If $psb - \text{cps} > \frac{\text{reg}(E)\cdot\#Ш(E/\mathbb{Q})}{25\cdot\hat{h}_1} + \frac{\hat{h}_1}{4}$, then P_1 is the generator with minimal canonical height and $\#Ш(E/\mathbb{Q}) = 1$.*

Proof. By the proof of the theorem, if Q is another independent generator, then $\hat{h}_2 = \hat{h}(Q) \leq \frac{\text{reg}(E)}{\hat{h}_1} + \frac{\hat{h}_1}{4}$. Assume $\#Ш(E/\mathbb{Q}) = n^2$, then

$$\frac{\text{reg}(E) \cdot \#Ш(E/\mathbb{Q})}{25\hat{h}_1} + \frac{\hat{h}_1}{4} < \text{psb} - \text{cps} \leq \frac{\text{reg}(E) \cdot \#Ш(E/\mathbb{Q})}{n^2\hat{h}_1} + \frac{\hat{h}_1}{4}$$

Then $\#Ш(E/\mathbb{Q}) = n^2 < 25$, which is not divisible by 2 or 3, and thus $Ш(E/\mathbb{Q}) \cong \{0\}$. ■

Remark 15. *This corollary only illustrates the strategy when $r_2Ш = r_3Ш = 0$, but it can easily be modified to other situations.*

Example 2. *Continuing with the example 1, by using Magma descent methods, one finds that* $\#Ш(E/\mathbb{Q})$ *is not divisible by* 2 *or* 3*, and by using Lang's inequality, one finds that this point search bound* $\text{psb} = 19.95$ *is enough to conclude that* $Ш(E/\mathbb{Q}) \cong \{0\}$*, i.e. it is trivial.*

Example 3. *The elliptic curve of rank* 2 *that represented the maximal challenge was*

$$y^2 + xy + y = x^3 - x^2 - 2616540370823x - 1629067573052867294$$

whose conductor is 606015*, where after finding the first generator*

$$P = (-3589933141/3844, 111290214311/238328)$$

one would need to perform a point search up to 175.6 *in order to guarantee finding the second generator. I tried to find rational point in the elements provided by Magma's descent methods, but I always ran out of memory. However, I know that* $r_2Ш = r_3Ш = 0$*, and a* $\text{psb} = 25.5$ *guaranteed that* $Ш(E/\mathbb{Q}) \cong \{0\}$*, i.e. it is trivial.*

2.5.2 Elliptic curves of rank 2

I studied 572393 elliptic curves over $\mathbb{Q}$ of rank 2 of conductor up to 10^6, taking from Cremona's and Stein-Watkins' databases as in table 2.15.

As it was conjectured by Delaunay et al., there are very few curves with rank > 1 and non-trivial Tate-Shafarevich group. I only found examples of curves where $\#Ш(E/\mathbb{Q}) = 1$ or 4. In the former case $Ш(E/\mathbb{Q}) \cong \{0\}$, and in the later case $Ш(E/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The origins of these examples where Ш is non-trivial is in table 2.16.

2.5.3 Curves of Rank 3

I studied 23172 elliptic curves over $\mathbb{Q}$ of rank 3 of conductor up to 10^6, taken mostly from Stein-Watkins' databases as in table 2.17. All these curves have trivial Tate-Shafarevich group, i.e. $Ш(E/\mathbb{Q}) \cong \{0\}$. Moreover, I found a basis for the Mordell-Weil group of each curve by doing point searches in *SageMath*.

$\lfloor \frac{n}{10^6} \rfloor$	CRE	SW
0	56975	49516
1	69868	54774
2	72987	54374
3	74516	53455
4	0	51659
5	0	50461
6	0	49953
7	0	49661
8	0	48227
9	0	48086
Total	274346	510166

Table 2.15: Origins of rank 2 elliptic curves.

2.5.4 Curves of Rank 4

I studied 21 elliptic curves over $\mathbb{Q}$ of rank 4 of conductor up to 10^6, taken mostly from Stein-Watkins' databases as in table 2.18. All these curves have trivial Tate-Shafarevich group. Moreover, I found a basis for the Mordell-Weil group of each curve.

2.6 A further note

The database with the conductor, the a-invariants, the rank, the Tate-Shafarevich group order and type will be soon posted in my website `menosgeze.github.io`.

$\lfloor \frac{n}{10^6} \rfloor$	CRE No.	CRE npm	SW No.	SW npm
0	0	0.0	0	0.0
1	2	7.29	2	3.92
2	6	21.87	3	5.88
3	13	47.39	8	15.68
4	0	0.0	14	27.44
5	0	0.0	9	17.64
6	0	0.0	6	11.76
7	0	0.0	18	35.28
8	0	0.0	18	35.28
9	0	0.0	22	43.12

Table 2.16: Number per million Curves of rank = 2 and $\#Ш(E/\mathbb{Q}) = 4$.

$\lfloor \frac{n}{10^6} \rfloor$	CRE	SW
0	542	541
1	1571	1506
2	2101	1939
3	2465	2237
4	0	2438
5	0	2597
6	0	2848
7	0	2808
8	0	2810
9	0	2992

Table 2.17: Origins of rank 3 elliptic curves.

$\left\lfloor \frac{n}{10^6} \right\rfloor$	CRE	SW
0	0	0
1	0	0
2	1	1
3	0	0
4	0	0
5	0	3
6	0	2
7	0	6
8	0	3
9	0	6

Table 2.18: Origins of rank 4 elliptic curves.

Chapter 3

ON THE P-ADIC REGULATOR OF ELLIPTIC CURVES

3.1 Introduction

While attempting to compute the Tate-Shafarevich group order of some elliptic curves, I recurred to Mazur, Tate and Teitelbaum's p-adic BSD conjecture for the case of good ordinary reduction on a rational prime $p \geq 5$. Contrary to my initial intuition, the data demostrated that the p-adic regulator is not always integral, even for non-anomalous primes, see remark 18, so I present several examples of this phenomena that I could not find in literature. Moreover, for a non-anomalous prime of good ordinary reduction, I computed a lower bound on the valuation of the p-adic regulator as described in [SW13]. Finally, I used this bound to compute the Tate-Shafarevich group order of some rank 1 elliptic curves.

3.2 The p-adic height on rational elliptic curves

In [MTT86], Mazur, Tate and Teitelbaum conjectured an analogous p-adic version of the Birch and Swinnerton-Dyer conjecture for elliptic curves over $\mathbb{Q}$, which can be summarized as follows:

Conjecture 4 (Conj. 5.1 [SW13])**.** *For a rational prime $p \geq 5$ and a rational elliptic curve E of good ordinary or multiplicative reduction at p, one has:*

(a) The order of vanishing of the p-adic L-function $L_p(E,T)$ at $T = 0$ is equal to the rank $r = \mathrm{rank}(E(\mathbb{Q}))$ of the elliptic curve, unless E has split multiplicative reduction at p, in which case the order of vanishing is equal to $r + 1$.

(b) For rational primes $p \geq 5$ of good ordinary or non-split multiplicative reduction, the

leading coefficient $\mathcal{L}_p^*(E,0)$ *satisfies:*

$$\mathcal{L}_p^*(E,0) = \varepsilon_p \cdot \frac{\prod_v \tau_v \cdot \#Ш(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{tor})^2} \cdot \mathrm{reg}_\gamma(E/\mathbb{Q})$$

On the other hand, for rational primes $p \geq 5$ *of split multiplicative reduction, the leading coefficient* $L_p^*(E,0)$ *satisfies:*

$$\mathcal{L}_p^*(E,0) = \frac{\mathscr{L}_p}{\log(\kappa(\gamma))} \cdot \frac{\prod_v \tau_v \cdot \#Ш(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{tor})^2} \cdot \mathrm{reg}_\gamma(E/\mathbb{Q})$$

Remark 16. *This conjecture is an equality and not just "an equality up to a p-adic unit." Notice that the p-adic BSD conjecture uses the product of the Tamagawa numbers, which are rational integers and thus p-adic integers, and the Tate-Shafarevich group order, which I assume by the standard BSD conjecture to be a positive integer.*

For a prime of good or semistable reduction, the p-adic L-series of an elliptic curve E is defined to be the integral of the character defined by the following composition:

$$\langle \bullet \rangle : z \in \mathbb{Z}_p^* \leftrightarrow (\zeta, z_0)\mu_{p-1} \times 1 + p\mathbb{Z}_p \twoheadrightarrow z_0 \in 1 + p\mathbb{Z}_p \subseteq \overline{\mathbb{Q}_p}$$

against a measure μ_α on $\mathbb{Z}_p^*$, which depends on the modular symbols of E at rationals whose denominators are powers of p.

$$L_\alpha(E,s) = \int_{\mathbb{Z}_p^*} \langle x \rangle^{s-1} d\mu_\alpha(x)$$

Here, α is either the root of the characteristic of the Frobenious $X^2 - a_p(E) \cdot X + p$ that satisfies $\mathrm{ord}_p(\alpha) < 1$ for a prime p of good reduction, or α is $a_p(E)$ for a prime p of multiplicative reduction. The p-adic multiplier ε_p is given by

$$\varepsilon_p = \begin{cases} (1-\alpha^{-1})^2 & \text{if } E \text{ has good ordinary reduction at } p. \\ (1-1/\alpha) & \text{if } E \text{ has multiplicative reduction at } p. \end{cases}$$

On the other hand, let $\kappa : Gal(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \to \mathbb{Z}_p^*$ be the cyclotomic character, which takes a a topological generator γ of $Gal(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})^{(p-1)}$ into a topological generator $\kappa(\gamma)$ of $1+p\mathbb{Z}_p^*$,

which in our computations will be taken to be $\kappa(\gamma) = 1 + p$. By letting $T = \kappa(\gamma)^{s-1} - 1$, one obtains:

$$\mathcal{L}_\alpha(E, T) = \int_{\mathbb{Z}_p^*} (1+T)^{\frac{\log_p \langle x \rangle}{\log_p \kappa(\gamma)}} d\mu_\alpha(x) \in \mathbb{Q}_p(\alpha)[\![T]\!]$$

These p-adic L-functions satisfy the following interpolation property with respect to the complex L-function:

$$\mathcal{L}_\alpha(E, 0) = L_\alpha(E, 1) = \epsilon_p \cdot \frac{L(E, 1)}{\Omega_E}$$

which for primes p of split multiplicative reduction indicates an extra 0 because $\epsilon_p = 0$. This explains the difference in the conjecture for split multiplicative reduction. In this case, one has the p-adic L-invariant

$$\mathscr{L}_p = \frac{\mathrm{ord}_p(q_E)}{\log_p(q_E)} \neq 0$$

which is known to be nonzero, see [BS+96]. Here q_E is the Tate's uniformizer of E. Moreover, the p-adic L function can be approximated via polynomials using the generator $\kappa(\gamma)$, and Stein and Wuthrich [SW13] established how to obtain as much p-adic precision as desired in these results.

In all of these computations, one defines the p-adic logarithm on $1 + p\mathbb{Z}_p$ by the standard series

$$\log_p(x) = \sum_{n \geq 1} \frac{(-1)^{n+1}(x-1)^n}{n}$$

and extended to $\mathbb{Q}_p^*$ by defining $\log(\zeta_{p-1}) = 0$ and $\log_p(p) = 0$, i.e.: for $x \in \mathbb{Q}_p^*$, let $u = xp^{-\mathrm{ord}_p(x)} \in \mathbb{Z}_p^*$, then $u^{p-1} \in 1 + p\mathbb{Z}_p$, and thus $\log_p(x) = \frac{1}{p-1} \log_p(u^{p-1})$.

Remark 17. *Hence,* $\log_p : \mathbb{Q}_p^* \to (\mathbb{Q}_p, +)$ *is a group homomorphism, and* $\mathrm{ord}_p(\log_p(z)) = \mathrm{ord}_p(z-1) \geq 1$.

Recall the short exact sequence:

$$0 \to E_1(\mathbb{Q}_p) \cong \hat{E}(p\mathbb{Z}_p) \to E_0(\mathbb{Q}_p) \to \tilde{E}_{ns}(\mathbb{F}_p) \to 0$$

where $E_0(\mathbb{Q}_p)$ is the set of points with nonsingular reduction to $\tilde{E}(\mathbb{F}_p)$, and the kernel of the reduction $E_1(\mathbb{Q}_p)$ is isomorphic to the formal group $\hat{E}(p\mathbb{Z}_p)$. In particular, in the split

multiplicative reduction case, Tate [Sil94, §V.3-6], [CY97, §12] showed that $E(\mathbb{Q}_p) \cong \mathbb{Q}_p/q_E^{\mathbb{Z}}$ where the uniformizing parameter $q_E \in \mathbb{Q}_p$ is obtained by inverting the series defining the j-invariant, see [SW13, Eq.3.4]. Then the p-adic L-invariant $\mathscr{L}_p = \log_p(q_E)/ord_p(q_E)$ can be quickly approximated to any desired p-adic precision.

Moreover, in this p-adic BSD conjecture, the standard regulator from the standard BSD conjecture is replaced by "a p-adic regulator." The p-adic height in this conjecture depends on an Eisenstein p-adic form $\mathbb{E}_2(E, \omega_E)$ of weight 2 and the p-adic canonical σ-function, see [MTT86, §II.2], [MT91]. In particular, for the split multiplicative case, one has:

$$\begin{array}{rcl} \mathbb{E}_2(E, \omega_E) & = & 1 - 24 \sum_{n \geq 1} \sigma_1(n) q_E^n = 1 - 24 \sum_{n \geq 1} \frac{q_E^n}{(1-q_E^n)^2} \\ \sigma^2_{\omega_E}(P) & = & C^2 \frac{u}{(u-1)^2} \prod_{n \geq 1} (1-uq^n)^2 (1-u^{-1}q^n)^2 (1-q^n)^{-4} \end{array} \tag{3.1}$$

where $u \in \mathbb{Z}_p^*$ corresponds to P in the Tate's uniformization $E_0(\mathbb{Q}_p) \cong \mathbb{Q}_p^*/q_E^{\mathbb{Z}}$. In the other reduction cases, Mazur et al. [MTT86, §II.4] defined σ_E at the points that reduce to the identity in $\hat{E}(\mathbb{F}_p)$ and to the connected component of the identity in $\hat{E}(\mathbb{F}_q)$ for all other primes $q|N_E$, which is a subgroup of $E_1(\mathbb{Q})$. Using one of the characterizations of σ in [MT91, Thm. 3.1], one can slowly compute the definition of σ depending on the formal parameter t. However thanks to Katz' reinterpretation of $\mathbb{E}_2(E, \omega_E)$ as the direction of the unit root eigenspace of Frobenius acting on the one-dimensional de Rham cohomology of E, see [Kat76], Mazur, Stein and Tate developed a fast algorithm to compute both $\mathbb{E}_2(E, \omega_E) \in \mathbb{Z}_p$ and $\sigma(E, \omega_E) \in t + t^2\mathbb{Z}_p[\![t]\!]$, see [MST, §3]. As explained in [SW13], Perrin Riu defined the p-adic regulator as the p-adic integral of the invariant differential, which generalizes to primes of good super-singular reduction. Indeed, for a prime p of good ordinary reduction or non-split multiplicative reduction, one has:

$$\hat{h}_p(P) = 2 \log_p \left(\frac{d(P)}{\sigma_p(P)} \right)$$

where $d(P)$ is the square root of the denominator of the x-coordinate of P. Additionally, for a prime p of split multiplicative reduction, one has:

$$\hat{h}_p(P) = 2 \log_p \left(\frac{d(P)}{\sigma_p(P)} \right) - \frac{\log_p(u)^2}{\log_p(q_E)}$$

which makes the p-adic height a quadratic p-adic form on $E(\mathbb{Q})$. Schneider conjectured that the p-adic regulator $\mathrm{reg}_p(E)$ derived from the p-adic height pairing is non-zero.

Since these heights depend on the choice of the isomorphism $Gal(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \to \mathbb{Z}_p$, it is natural to normalize the regulator as follows:

$$\mathrm{reg}_\gamma(E/\mathbb{Q}) = \frac{\mathrm{reg}_p(E/\mathbb{Q})}{\log(\kappa(\gamma))^r}$$

3.2.1 On the integrality of the p-adic regulator.

For a rational prime $p \geq 5$ where the elliptic curve E has a good ordinary reduction, rewrite the p-adic BSC conjecture as:

$$\mathcal{L}_p^*(E,0) \cdot \mathrm{tor}^2 = \varepsilon_p \,\mathrm{tam} \cdot \#Ш(E/\mathbb{Q}) \cdot \frac{\mathrm{reg}_p(E/\mathbb{Q})}{\log_p(\kappa(\gamma))^r} \tag{3.2}$$

Example 4. *Following the notation in [SW13], consider the elliptic curve of conductor* 1646 *given by:*

$$y^2 + xy = x^3 - 756x - 368$$

for which 5 *is a non-anomalous prime of good ordinary reduction. This curve has a generator* $P = (-24, 76)$*, trivial torsion subgroup, Tamagawa product* $\mathrm{tam} = 25$*, trivial Tate-Shafarevich group, p-adic multiplier* $\varepsilon_p \approx 4 + 4 \cdot 5 + 4 \cdot 5^2 + O(5^4)$*, and p-adic regulator* $3 \cdot 5^{-1} + 1 + 3 \cdot 5 + 2 \cdot 5^2 + 4 \cdot 5^3 + O(5^4)$*. Using Wuthrich's numerical modular symbols [Wut18], I was able to compute the leading coefficient of its* 5*-adic L-series* $L_5^*(E,0) = 2 + 4 \cdot 5 + O(5^2)$*. Hence the left hand side, in equation 3.2 is* $2 + 4 \cdot 5 + O(5^2)$*, and the right hand side is:*

$$(4 + 4 \times 5 + O(5^2)) \cdot 25 \cdot \frac{(3 \cdot 5^{-1} + 1 + 3 \cdot 5 + O(5^2))}{5 + 2 \cdot 5^2 + O(5^3)}$$

which evidenciates the 5*-adic BSD conjecture as stated above and shows that the regulator* $\mathrm{reg}_p(E/\mathbb{Q})$ *may not be a p-adic integer, even in the case where p is not an anomalous prime as defined by Mazur, i.e. p does not divide* $\#\tilde{E}(\mathbb{F}_p)$*.*

Lemma 4. *For a rational elliptic curve E with good ordinary reduction at the anomalous* $p \geq 5$*, the p-adic multiplier* ε_p *has valuation at least* 2*.*

Proof. Since $\#\tilde{E}(\mathbb{F}_p) \equiv 0(p)$, then $a_p = p + 1 - \#\tilde{E}(\mathbb{F}_p) \equiv 1\,(p)$. Therefore,

$$\begin{aligned} &\Rightarrow \quad 1/\alpha \equiv 1\,(p) \\ &\Rightarrow \quad -1/\alpha \equiv p - 1\,(p) \\ &\Rightarrow \quad 1 - 1/\alpha \equiv 0\,(p) \\ &\Rightarrow \quad \varepsilon_p = (1 - 1/\alpha)^2 \equiv 0\,(p^2) \end{aligned}$$

■

Remark 18. *Among the rank* 1 *elliptic curves in the data with a known generator* $P \in E(\mathbb{Q})$ *and with either good ordinary or split multiplicative reduction at the primes* $p = 5, 7,$ *or* 11*, I computed the p-adic regulator. The findings are as follows:*

- *I found* 350 *elliptic curves of good ordinary reduction at the non-anomalous prime* 5 *which have a non-integral* 5*-adic regulator* $\mathrm{reg}_5(E/\mathbb{Q}) = -1$*. In all cases,* $5^2 | \,\mathrm{tam}$*,* $\#Ш(E/\mathbb{Q}) = 1$*, and* $\mathrm{ord}_5(\mathrm{reg}_5(E/\mathbb{Q})) = -1$*. See tables 3.1, 3.2.*

- *I found* 28 *elliptic curves of good ordinary reduction at the non-anomalous prime* 7 *which have a non-integral* 7*-adic regulator* $\mathrm{reg}_7(E/\mathbb{Q})$*. In all cases,* $7^2 | \,\mathrm{tam}$*,* Ш *is trivial, and* $\mathrm{ord}_7(\mathrm{reg}_7(E/\mathbb{Q})) = -1$*. See tables 3.3, 3.4.*

- *I did not found any elliptic curve of good ordinary reduction at the non-anomalous prime* 11 *with a non-integral* 11*-adic regulator* $\mathrm{reg}_{11}(E/\mathbb{Q})$*. See tables 3.5, 3.6.*

The data led me to try to find a lower bound on the valuation of the p-adic regulator of an elliptic curve E when p is a non-anomalous prime of good ordinary reduction for E.

Proposition 20. *Let* E *be a rank* 1 *rational ellipt curve with Tamagawa numbers* τ_l *at the primes* l *of bad reduction. Assume* E *has good ordinary reduction at* $p \geq 5$*. Let* v *be the valuation of least common multiple of the Tamagawa numbers of* E *and* $\#\tilde{E}(\mathbb{F}_p)$*, then*

$$\mathrm{ord}_p(\mathrm{reg}_p(E/\mathbb{Q})) \geq 1 - 2v$$

In particular, if the Tamagawa product of E is coprime to p, then

$$\mathrm{ord}_p(\mathrm{reg}_p(E/\mathbb{Q})) \geq 1$$

Remark 19. *The importance of this proposition is that I may find some primes that don't divide the Tate-Shafarevich group order of a rank* 1 *rational elliptic curve E by assuming the p-adic BSD conjecture.*

Proof. Assume P is a non-torsion generator for $E(\mathbb{Q})$. As described in [MST, Alg.3.4], let $Q = mP = \left(\frac{a}{d^2}, \frac{b}{d^3}\right)$ where m is the least common multiple of the Tamagawa numbers of E and $\#\tilde{E}(\mathbb{F}_p)$, which has valuation $v = \mathrm{ord}_p(m)$. Since Q reduces to the identity in $\tilde{E}(\mathbb{F}_p)$, one knows that $\mathrm{ord}_p(d) \geq 1$ and $\mathrm{ord}_p(a) = \mathrm{ord}_p(b) = 0$. Recall that σ is a p-adic series in $t + t^2\mathbb{Z}_p[\![t]\!]$. Therefore,

$$\mathrm{ord}_p(\sigma(-x/y)) = \mathrm{ord}_p(-x/y) = \mathrm{ord}_p(-ad/b) = \mathrm{ord}_p(d)$$

Hence, the argument $\sigma(-x/y)/d$ of the p-adic logarithm is a p-adic unit. Moreover, the p-adic logarithm return values in $p\mathbb{Z}_p$, therefore,

$$\mathrm{ord}_p(h_p(Q)) = \mathrm{ord}_p\left(-2\log_p\left(\frac{\sigma(-x/y)}{d}\right)\right) \geq 1$$

Finally, since $h_p(P) = \frac{1}{m^2}h_p(Q)$ and $v = \mathrm{ord}_p(m)$, one has:

$$\mathrm{ord}_p(h_p(P)) = \mathrm{ord}_p(h_p(Q)) - 2v \geq 1 - 2v$$

Remark 20. *Moreover, this computation agrees with the data in our tables.*

■

In particular, assuming both the BSD conjecture and Mazur's et al. p-adic BSD conjecture for primes of good ordinary reduction, and the Generalized Riemann Hypothesis to compute the cardinality of $Sel_3(E/\mathbb{Q})$, one can compute the Tate-Shafarevich order of some rank 1 rational elliptic curves for which the generator is not known.

Example 5. *Let E be the rank 1 rational elliptic curve with minimal equation*

$$y^2 = x^3 + x^2 - 122825070512x - 16568367536411052$$

whose conductor is 722832, with torsion subgroup order $\mathrm{tor} = 2$*, and with Tamagawa product* $\mathrm{tam} = 16$*. Through descent methods one finds that:*

$$\mathrm{rank}_{\mathbb{F}_2} Ш(E/\mathbb{Q})[2] = \mathrm{rank}_{\mathbb{F}_3} Ш(E/\mathbb{Q})[3] = 0$$

The product of the regulator times the Tate-Shafarevich group order conjecture by the BSD formula is 464.7385. The Cremona-Prickett-Siksek height bound is $\mathrm{cps} = 16.92$*. A point search bound up to naive height of $h = 22$ returns no non-torsion Mordell-Weil group generator. Hence, $\#Ш(E/\mathbb{Q}) \leq 49$ and it is not divisible by 2 or 3, i.e. the only candidates are $\#Ш(E/\mathbb{Q}) = 1, 25, 49$.*

Now, $p = 5$ is a non-anomalous prime. The 5-adic multiplier is $\varepsilon_5 = 4+5+2\cdot 5^2+O(5^4)$ and the leading coefficient of the 5-adic L-series is approximated by $L_5^*(E,0) = 2+2\cdot 5+O(5^2)$. Recall that the factor $\log_5(1+5)$ has valuation $\mathrm{ord}_5(\log_5(1+5)) = 1$. Therefore, by the 5-adic BSD conjecture $\#Ш(E/\mathbb{Q})$ is not divisible by 5.

Similarly, $p = 7$ is a non-anomalous prime. The 7-adic multiplier is $\varepsilon_7 = 1 + 5 \cdot 7 + 2 \cdot 7^2 + O(7^4)$ and the leading coefficient of the 7-adic L-series is approximated by $L_7^*(E,0) = 4+4\cdot 7+O(7^2)$. Recall that the factor $\log_7(1+7)$ has valuation $\mathrm{ord}_7(\log_7(1+7)) = 1$. Therefore, by the 7-adic BSD conjecture $\#Ш(E/\mathbb{Q})$ is not divisible by 7. Therefore, $Ш(E/\mathbb{Q})$ is trivial or $\#Ш(E/\mathbb{Q}) = 1$.

Anomalous	$\mathrm{ord}_5(\mathrm{reg}_5(E/\mathbb{Q}))$	frequency
False	-1	350
False	0	41423
False	1	583743
False	2	117486
False	3	23155
False	4	4772
False	5	939
False	6	207
False	7	51
False	8	6
True	-1	109867
True	0	22171
True	1	12803
True	2	2548
True	3	523
True	4	111
True	5	20
True	6	4
Total		920179

Table 3.1: The distribution of the 5-adic regulator valuation of rank 1 rational elliptic curves with good ordinary reduction at 5.

$\mathrm{ord}_5(\mathrm{reg}_5(E/\mathbb{Q}))$	frequency
-5	24
-4	62
-3	321
-2	1776
-1	9341
0	60480
1	219531
2	43186
3	8614
4	1738
5	402
6	69
7	22
9	2
Total	345568

Table 3.2: The distribution of the 5-adic regulator valuation of rank 1 rational elliptic curves with split-multiplicative reduction at 5.

Anomalous	$\mathrm{ord}_7(\mathrm{reg}_7(E/\mathbb{Q}))$	frequency
False	-1	28
False	0	34388
False	1	895311
False	2	127769
False	3	18144
False	4	2561
False	5	425
False	6	42
False	7	9
False	8	1
True	-1	90340
True	0	12836
True	1	5336
True	2	723
True	3	110
True	4	14
True	5	2
Total		1188039

Table 3.3: The distribution of the 7-adic regulator valuation of rank 1 rational elliptic curves with good ordinary reduction at 7.

$\mathrm{ord}_7(\mathrm{reg}_7(E/\mathbb{Q}))$	frequency
-4	11
-3	78
-2	550
-1	4313
0	36404
1	198320
2	28642
3	3927
4	559
5	69
6	19
Total	272892

Table 3.4: The distribution of the 7-adic regulator valuation of rank 1 rational elliptic curves with split-multiplicative reduction at 7.

Anomalous	$\mathrm{ord}_{11}(\mathrm{reg}_{11}(E/\mathbb{Q}))$	frequency
False	0	9948
False	1	1199237
False	2	109019
False	3	10046
False	4	815
False	5	107
False	6	13
False	7	2
True	-1	51769
True	0	4586
True	1	1368
True	2	122
True	3	9
True	4	1
Total		1387042

Table 3.5: The distribution of the 11-adic regulator valuation of rank 1 rational elliptic curves with good ordinary reduction at 11.

$\mathrm{ord}_{11}(\mathrm{reg}_{11}(E/\mathbb{Q}))$	frequency
-4	4
-3	6
-2	93
-1	1301
0	14468
1	146999
2	13199
3	1258
4	114
5	7
6	2
7	1
Total	177452

Table 3.6: The distribution of the 11-adic regulator valuation of rank 1 rational elliptic curves with split multiplicative reduction at 11.

Chapter 4

EXAMPLES OF THE P-ADIC REGULATOR VALUATION OF RANK 1 ELLIPTIC CURVES

4.1 Examples of the 5-adic regulator valuation

The valuation of the 5-adic regulator of rank 1 elliptic curves in our data, where we know a generator and 5 is a non-anomalous prime, is between -1 and 8. The same valuation when 5 is anomalous is between -1 and 6. However, finding examples with non-integral 5-adic regulator when 5 is an anomalous prime (109867 examples) is far more frequent than when 5 is non-anomalous (350 examples.) The same valuation when 5 is a prime of split multiplicative reduction is between -5 and 9. Here I list some examples representing this phenomena.

4.1.1 Examples when 5 is a prime of good ordinary reduction.

Example 6. *The rank* 1 *elliptic curve*

$$y^2 - xy = x^3 - 81939x + 29885985$$

has conductor 5406*. It has a trivial torsion subgroup, the product of its Tamagawa numbers is* 750*, its Tate-Shafarevich group is trivial, and* 5 *is* ***not-anomalous****. The generator for the Mordell-Weil group is* $P = (282, -5547)$*. The leading coefficient of the* 5*-adic L-series is* $L_5^*(E, 0) = 3 \cdot 5 + O(5^2)$*. The* 5*-adic multiplier is* $\varepsilon_5 = 1 + 4 \cdot 5^2 + 5^3 + O(5^4)$*, and the* 5*-adic regulator is:*

$$\mathrm{reg}_5(E/\mathbb{Q}) = 3 \cdot 5^{-1} + 2 + 4 \cdot 5 + O(5^2)$$

Remark 21. *In all* 350 *examples of rank* 1 *elliptic curves where* 5 *is not anomalous and the* 5*-adic regulator is not integral, I found that* $\mathrm{ord}_5(\mathrm{tor}) = 0$*,* $\mathrm{ord}_5(\#Ш(E/\mathbb{Q})) = 0$*. However, the*

factor that balances the negative valuation of the 5*-adic regulator is the Tamagawa product. Indeed, one finds that* $\mathrm{ord}_5(\mathrm{tam}) \in \{2, 3\}$*. In all the cases where* $\mathrm{ord}_5(\mathrm{tam}) = 3$*, the leading coefficient of the* 5*-adic L-series has valuation* 1*.*

Example 7. *The rank* 1 *elliptic curve*

$$y^2 = x^3 + 6566x + 46305$$

has conductor 590744*. It has torsion subgroup of order* $\mathrm{tor} = 2$*, Tamagawa product* $\mathrm{tam} = 8$*, trivial Tate-Shafarevich group,* 5 *is* ***non-anomalous****, and a non-torsion generator is* $P = (282177/121, 149984100/1331)$*. The* 5*-adic multiplier is* $\varepsilon_5 = 4 + 5 + 2 \cdot 5^2 + O(5^4)$*. And the* 5*-adic regulator is:*

$$\mathrm{reg}_5(E/\mathbb{Q}) = 2 \cdot 5^8 + 2 \cdot 5^9 + O(5^{10})$$

I was not able to compute the leading coefficient of the 5*-adic L-series, but this is not surprising, since all these evidence suggest that I need to approximate the leading coefficient to precision at least* $O(5^9)$*, and it would require too many modular symbols of* E *and hence too many terms when using Wuthrich'es numerical methods.*

Example 8. *The rank* 1 *elliptic curve*

$$y^2 = x^3 + x^2 - 5x + 2$$

has conductor 3664*. It has trivial torsion subgroup, the product of the Tamagawa numbers is* $\mathrm{tam} = 1$*, it has a trivial Tate-Shafarevich group, the generator for the Mordell-Weil group is* $P = (2, 2)$*, and* 5 *is* ***anomalous****. The* 5*-adic multiplier is* $\varepsilon_5 = 5^2 + 4 \cdot 5^3 + 4 \cdot 5^4 + O(5^5)$*. The* 5*-adic L-series leading coefficient is* $L_5^*(E, 0) = 2 + 4 \cdot 5 + O(5^2)$*. And the* 5*-adic regulator is:*

$$\mathrm{reg}_5(E/\mathbb{Q}) = 2 \cdot 5^{-1} + 5^2 + O(5^4)$$

Example 9. *The rank* 1 *elliptic curve*

$$y^2 = x^3 - x^2 - 280x + 136$$

has conductor 53088*. It torsion subgroup has order* $\mathrm{tor} = 2$*, the product of its Tamagawa numbers is* 8*, it has a trivial Tate-Shafarevich group, a generator for the Mordell-Weil group is* $P = (-11, 42)$*, and* 5 *is* ***anomalous****. The* 5*-adic multiplier is* $\varepsilon_5 = 4 \cdot 5^2 + 4 \cdot 5^3 + 3 \cdot 5^4 + O(5^5)$*, which is evidence that* $\mathrm{ord}_p(\varepsilon_5) \geq 2$ *in this case. And the* 5*-adic regulator is:*

$$\mathrm{reg}_5(E/\mathbb{Q}) = 3 \cdot 5^6 + 5^8 + 3 \cdot 5^9 + O(5^{10})$$

I was not able to compute the leading coefficient of the 5*-adic L-series, but this is not surprising, since all these evidence suggest that I need to approximate it to precision at least* $O(5^7)$*.*

4.1.2 Examples where 5 is a prime of split multiplicative reduction.

Example 10. *The rank* 1 *elliptic curve*

$$y^2 + xy + y = x^3 + x^2 - 20x - 268$$

has conductor 65685*. It has torsion subgroup of order* $\mathrm{tor} = 2$*, the product of its Tamagawa numbers is* $\mathrm{tam} = 8$*, it has trivial Tate-Shafarevich group, and a generator for the Mordell-Weil group is* $P = (12, 31)$*. The* 5*-adic L-invariant is* $\mathscr{L}_5 = 3 \cdot 5^7 + 3 \cdot 5^8 + 3 \cdot 5^9 + O(5^{10})$ *and the leading coefficient of the* 5*-adic L series is* $L_5^*(E, 0) = 1 + 5 + O(5^2)$*. And the* 5*-adic regulator is:*

$$\mathrm{reg}_5(E/\mathbb{Q}) = 5^{-5} + 3 \cdot 5^{-4} + 4 \cdot 5^{-3} + 3 \cdot 5^{-2} + 2 \cdot 5^{-1} + O(5)$$

Example 11. *The rank* 1 *elliptic curve*

$$y^2 = x^3 + x^2 - 10440x - 413505$$

has conductor 184080*. It has trivial torsion subgroup, the product of the Tamagawa numbers is* $\mathrm{tam} = 9$*, its has trivial Tate-Shafarevich group, and a generator for the Mordell-Weil group is* $P = (-243/4, 117/8)$*. The* 5*-adic L-invariant is* $\mathscr{L}_5 = 5 + 4 \cdot 5^2 + 4 \cdot 5^4 + O(5^5)$*. And the* 5*-adic regulator is:*

$$\mathrm{reg}_5(E/\mathbb{Q}) = 4 \cdot 5^9 + 4 \cdot 5^{10} + O(5^{12})$$

Again, computing the leading coefficient of the 5-adic L-series was not possible.

4.2 Examples of the 7-adic regulator valuation

The valuation of the 7-adic regulator of rank 1 elliptic curves in our data, where we know a non-torsion generator and 7 is a non-anomalous prime, is between -1 and 8. The same valuation when 7 is anomalous is between -1 and 5. However, finding examples with non-integral 7-adic regulator when 7 is anomalous (90340 examples) is far more frequent than when 7 is anomalous (28 examples.) The same valuation when 7 is a prime of split multiplicative reduction is between -4 and 6. Here I show some examples representing this phenomena.

4.2.1 Examples when 7 is a prime of good ordinary reduction.

Example 12. *The rank* 1 *elliptic curve*

$$y^2 + xy + y = x^3 + x^2 - 1911556x + 1139589125$$

has conductor 5034*. It has a trivial torsion subgroup, the product of its Tamagawa numbers is* $\text{tam} = 49$*, It has a trivial Tate-Shafarevich group, the generator for the Mordell-Weil group is* $P = (-1571, 17169)$*, and* 7 *is* ***non-anomalous****. The leading coefficient of the* 7*-adic L-series* $L_7^*(E, 0) = 5 + O(7^2)$*. The* 7*-adic multiplier* $\varepsilon_7 = 1 + 5 \cdot 7 + 2 \cdot 7^2 + O(7^3)$*. And the* 7*-adic regulator is:*

$$\text{reg}_7(E/\mathbb{Q}) = 5 \cdot 7^{-1} + 4 + 4 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + O(7^4)$$

Example 13. *The rank* 1 *elliptic curve*

$$y^2 + xy + y = x^3 + 16x + 30$$

has conductor 5034*. It has a trivial torsion subgroup, the product of its Tamagawa numbers is* $\text{tam} = 2$*, it has a trivial Tate-Shafarevich group, the generator for the Mordell-Weil group is* $P = (0, 5)$*, and* 7 *is* ***anomalous****. The leading coefficient of the* 7*-adic L-series*

$L_7^*(E,0) = 5 + 5\cdot 7 + 7^2 + O(7^4)$, *the* 7*-adic multiplier* $\varepsilon_7 = 7^2 + 4\cdot 7^3 + O(7^5)$, *and the* 7*-adic regulator is:*

$$\mathrm{reg}_7(E/\mathbb{Q}) = 6\cdot 7^{-1} + 3 + 3\cdot 7 + 3\cdot 7^3 + O(7^4)$$

4.3 Examples where the generator is unknown

Previously, I presented some examples where the p-adic BSD conjecture helped me to determine the order of the Tate-Shafarevich group of some rank 1 rational elliptic curves. Here, I present two more examples where the p-adic BSD conjecture helps me to reduce the upper bound on $\#Ш(E/\mathbb{Q})$.

Example 14. *The rank* 1 *rational elliptic curve of conductor* 980115 *with equation:*

$$y^2 + xy = x^3 + x^2 - 127714865197x + 17574740363980354$$

has torsion subgroup of order $\mathrm{tor} = 2$*, and the product of its Tamagawa numbers is* $\mathrm{tam} = 8$*. From descent methods, one knows that the* 2 *and* 3 *primary parts of* $Ш(E/\mathbb{Q})$ *are trivial. Using point search methods and Cremona-Prickett-Siksek height bound, one can estimate an upper bound for the Tate-Shafarevich group order* $\#Ш(E/\mathbb{Q}) \leq 169$*. Both* 11 *and* 13 *are non-anomalous primes of good ordinary reduction. The leading coefficient for the* 11*-adic L-series is* $4 + 9\cdot 11 + O(11^2)$*, and that for the* 13*-adic L-series is* $2\cdot 13 + O(13^2)$*. The* 11*-adic multiplier is* $\varepsilon_{11} = 5 + 6\cdot 11 + 7\cdot 11^2 + 3\cdot 11^3 + O(11^4)$*, and the* 13*-adic multiplier is* $\varepsilon_{13} = 10 + 4\cdot 13 + 13^2 + 2\cdot 13^3 + O(13^4)$*. By proposition 20, one knows that* $\#Ш(E/\mathbb{Q})$ *is not divisible by* 11 *or* 13*. However,* 7 *is a prime of super-singular reduction, and* 5 *is a prime of split multiplicative reduction. Thus I cannot conclude what* $\#Ш(E/\mathbb{Q})$ *is. However, I obtained that* $\#Ш(E/\mathbb{Q}) = 1$*,* 25*, or* 49*.*

Example 15. *The rank* 1 *elliptic curve of conductor* 835536 *and Weierstrass equation:*

$$y^2 = x^3 + x^2 - 39161015352x - 2982846669487788$$

has torsion subgroup of order $\mathrm{tor} = 2$*, and the product of its Tamagawa numbers is* $\mathrm{tam} = 16$*. From descent methods, we know that* $Ш(E/\mathbb{Q})$ *is not divisible by* 2 *or* 3*. From point search*

methods, we know that $\#Ш(E/\mathbb{Q}) \leq 49$. *Both* 5 *and* 7 *are non-anomalous primes. The leading coefficients of the* 5*-adic and the* 7*-adic L-series are* $2 \cdot 5^2 + 2 \cdot 5^3 + O(5^4)$ *and* $6 + 5 \cdot 7 + O(7^2)$ *respectively. By proposition 20, one concludes that* 7 *does not divide* $\#Ш(E/\mathbb{Q})$. *However, since the* 5*-adic leading coefficient has valuation* $\mathrm{ord}_5 L_5^*(E, 0) = 2$, *then all I can conclude is that* $\mathrm{ord}_5(\#Ш(E/\mathbb{Q})) \leq 2$, *and thus* $\#Ш(E/\mathbb{Q}) = 1$ *or* $\#Ш(E/Q) = 25$.

APPENDIX I: LIST OF ALL EXAMPLES OF THE USE OF THE P-ADIC BSD CONJECTURE TO DETERMINE THE TATE-SHAFAREVICH GROUP ORDER.

The elliptic curves in table 4.3 have $\text{rank}_{\mathbb{F}_2} Ш(E/\mathbb{Q})[2] = 0$ and $\text{rank}_{\mathbb{F}_3} Ш(E/\mathbb{Q})[3] = 0$, they have good ordinary reduction at the non-anomalous prime $p = 5$, and their torsion subgroup order and their Tamagawa numbers are coprime with 5. The previous methods described above showed that $\#Ш(E/\mathbb{Q}) = 1$ or 25. Moreover, the 5-adic BSD conjecture helped me to predict that they all have trivial Tate-Shafarevich groups.

The elliptic curves in table 4.4 have $\text{rank}_{\mathbb{F}_2} Ш(E/\mathbb{Q})[2] = 0$ and $\text{rank}_{\mathbb{F}_3} Ш(E/\mathbb{Q})[3] = 0$, they have good ordinary reduction at both $p = 5$ and $p = 7$, which are non-anomalous primes, and their torsion subgroup orders and their Tamagawa numbers are coprime with both 5 and 7. Moreover, previous methods showed me that $\#Ш \leq 49$ for these curves. Hence, the 5-adic and 7-adic BSD conjectures predict that they have a trivial Tate-Shafarevich group.

a-invariants	$L_5^*(E,0)$
$[0,0,0,-118607265516,-15722262885638320]$	$3+5+O(5^2)$
$[1,1,0,-7340609,-10308287178]$	$3+4\cdot 5+O(5^2)$
$[1,1,0,-8025594,-8753508225]$	$4+4\cdot 5+O(5^2)$
$[1,-1,0,-1632516768,-25387948473030]$	$2+O(5^2)$
$[1,1,1,-61530136,-3826200261179]$	$4+4\cdot 5+O(5^2)$
$[1,0,1,-48400807287,-4098523683875447]$	$1+2\cdot 5+O(5^2)$
$[1,1,0,-13099076,-18253199965]$	$2+3\cdot 5+O(5^2)$
$[1,0,1,-22906982145,-1334444606776844]$	$3+3\cdot 5+O(5^2)$
$[1,-1,0,-535421736,-4694240015933]$	$1+3\cdot 5+O(5^2)$
$[0,1,1,-329444456,-2301664465397]$	$2+O(5^2)$
$[1,-1,0,-1381626981,-19766361477560]$	$2+4\cdot 5+O(5^2)$
$[1,-1,0,-2548525896,18164914993255]$	$2+4\cdot 5+O(5^2)$
$[1,-1,0,-2293152768,-42266054145600]$	$4+3\cdot 5+O(5^2)$
$[1,1,0,-151878563,-720495131635]$	$2+O(5^2)$
$[1,0,0,-5690354272,-165218231300088]$	$4+3\cdot 5+O(5^2)$
$[0,0,0,-1431481004,-20846180671792]$	$1+2\cdot 5+O(5^2)$
$[1,1,0,-324781669,-2253001417802]$	$1+O(5^2)$
$[1,0,0,-697878529,-7096127798513]$	$1+O(5^2)$
$[1,1,1,303526941,3548360797965]$	$4+4\cdot 5+O(5^2)$
$[0,0,0,-4369463084,-112458596178992]$	$4+5+O(5^2)$
$[0,0,0,-70360938284,-7101123357924400]$	$4+5+O(5^2)$
$[0,0,0,-3811267731,-90563312743342]$	$4+O(5^2)$
$[1,1,0,-52137514,-144923463540]$	$2+O(5^2)$

Table 4.1: Elliptic curves where $\#Ш \leq 25$ and 5-adic BSD conjecture predicts $\#Ш = 1$.

a-invariants	$L_5^*(E,0)$
$[1,1,0,-17131926876,-863099814999096]$	$3+2\cdot 5+O(5^2)$
$[1,1,1,-130465010,-573628010309]$	$2+4\cdot 5+O(5^2)$
$[0,0,0,-12870747084,-562022559002000]$	$1+4\cdot 5+O(5^2)$
$[0,1,0,-47991992,-127983968000]$	$2+2\cdot 5+O(5^2)$
$[0,-1,0,-12350029889,-528258802068927]$	$2+3\cdot 5+O(5^2)$
$[1,-1,1,-665254839,-6604185143722]$	$2+3\cdot 5+O(5^2)$
$[1,0,0,-54581215049,-4908099010998816]$	$3+O(5^2)$
$[0,1,0,-1952382817,-33205046347777]$	$2+2\cdot 5+O(5^2)$
$[1,1,1,-5414497,-6526944391]$	$4+2\cdot 5+O(5^2)$
$[1,-1,0,-39455797698,-3016566605893100]$	$1+2\cdot 5+O(5^2)$
$[1,1,0,-373641823,-2780069538774]$	$3+2\cdot 5+O(5^2)$
$[0,1,0,-7676618672,-258878995935660]$	$1+5+O(5^2)$
$[0,0,0,-206114390604,-36017252917581168]$	$1+4\cdot 5+O(5^2)$
$[1,-1,0,-317497968,-2177427522065]$	$1+O(5^2)$
$[0,-1,0,-1289862144,-17830051050240]$	$4+O(5^2)$
$[0,0,0,-57510125323,-5308411539400774]$	$4+2\cdot 5+O(5^2)$
$[1,1,1,-118360635224,15673200089384666]$	$2+O(5^2)$
$[0,1,0,-22140257,-41713575393]$	$1+3\cdot 5+O(5^2)$
$[1,-1,0,-8841723696,320004821674395]$	$2+3\cdot 5+O(5^2)$
$[1,0,0,-9602885097,-362202662067255]$	$1+2\cdot 5+O(5^2)$
$[1,-1,0,-53729075808,-4793590789953890]$	$4+5+O(5^2)$
$[1,-1,1,-27552030473246,-556645208401177731 39]$	$4+4\cdot 5+O(5^2)$

Table 4.2: Elliptic curves where $\#Ш \leq 25$ and 5-adic BSD conjecture predicts $\#Ш = 1$.

a-invariants	$L_5^*(E,0)$
$[0,-1,0,-453083137,-3711908757503]$	$1+O(5^2)$
$[1,1,1,-286694199,-1868547907241]$	$3+2\cdot 5+O(5^2)$
$[0,-1,0,-4076937217,-100194355961855]$	$1+5+O(5^2)$
$[0,0,0,-439488029676,-112142097971715760]$	$3+5+O(5^2)$
$[0,0,1,-171462903,-864178330729]$	$2+2\cdot 5+O(5^2)$
$[0,-1,1,-1743532969,-28021046589408]$	$3+4\cdot 5+O(5^2)$
$[1,1,1,-181344097,-940022305651]$	$4+4\cdot 5+O(5^2)$
$[0,1,1,-3445559740,-77847415254097]$	$3+4\cdot 5+O(5^2)$

Table 4.3: Elliptic curves where $\#Ш \leq 25$ and 5-adic BSD conjecture predicts $\#Ш = 1$.

N_E	a-invariants	$L_5^*(E,0)$ $L_7^*(E,0)$
722832	$[0,1,0,-122825070512,-16568367536411052]$	$2+2\cdot 5+O(5^2)$ $4+4\cdot 7+O(7^2)$
951786	$[1,-1,1,-104026402679,-12914054345979795]$	$2+O(5^2)$ $1+O(7^2)$
968256	$[0,0,0,-438868345836,-112474106974166704]$	$1+3\cdot 5+O(5^2)$ $3+7+O(7^2)$

Table 4.4: Elliptic curves where $\#Ш \leq 49$ and 5-adic and 7-adic BSD conjectures predict $\#Ш = 1$.

BIBLIOGRAPHY

[AL70] A. O. L. Atkin and J. Lehner. "Hecke operators on $\Gamma_0(m)$". In: *Math. Ann.* 185 (1970), pp. 134–160. ISSN: 0025-5831. DOI: 10.1007/BF01359701.

[ARS06] Amod Agashe, Kenneth Ribet, and William A. Stein. "The Manin constant". In: *Pure Appl. Math. Q.* 2.2, Special Issue: In honor of John H. Coates. Part 2 (2006), pp. 617–636. ISSN: 1558-8599. DOI: 10.4310/PAMQ.2006.v2.n2.a11.

[Ata01] Daisuke Atake. "On elliptic curves with large Tate-Shafarevich groups". In: *J. Number Theory* 87.2 (2001), pp. 282–300. ISSN: 0022-314X. DOI: 10.1006/jnth.2000.2599.

[Bal+16] Jennifer S. Balakrishnan et al. "Databases of elliptic curves ordered by height and distributions of Selmer groups and ranks". In: *LMS J. Comput. Math.* 19.suppl. A (2016), pp. 351–370. ISSN: 1461-1570. DOI: 10.1112/S1461157016000152.

[BGZ85] Joe P. Buhler, Benedict H. Gross, and Don B. Zagier. "On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3". In: *Math. Comp.* 44.170 (1985), pp. 473–481. ISSN: 0025-5718. DOI: 10.2307/2007967.

[Bha+15] Manjul Bhargava et al. "Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves". In: *Camb. J. Math.* 3.3 (2015), pp. 275–321. ISSN: 2168-0930. DOI: 10.4310/CJM.2015.v3.n3.a1.

[BM90] Armand Brumer and Oisín McGuinness. "The behavior of the Mordell-Weil group of elliptic curves". In: *Bull. Amer. Math. Soc. (N.S.)* 23.2 (1990), pp. 375–382. ISSN: 0273-0979. DOI: 10.1090/S0273-0979-1990-15937-3.

[BMS16] Jennifer S. Balakrishnan, J. Steffen Müller, and William A. Stein. "A p-adic analogue of the conjecture of Birch and Swinnerton-Dyer for modular abelian varieties". In: *Math. Comp.* 85.298 (2016), pp. 983–1016. ISSN: 0025-5718. DOI: 10.1090/mcom/3029.

[Bob13] Jonathan W. Bober. "Conditionally bounding analytic ranks of elliptic curves". In: *ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium*. Vol. 1. Open Book Ser. Math. Sci. Publ., Berkeley, CA, 2013, pp. 135–144. DOI: 10.2140/obs.2013.1.135.

[Bru92] Armand Brumer. "The average rank of elliptic curves. I". In: *Invent. Math.* 109.3 (1992), pp. 445–472. ISSN: 0020-9910. DOI: 10.1007/BF01232033.

[BS+96] Katia Barré-Sirieix et al. "Une preuve de la conjecture de Mahler-Manin". In: *Invent. Math.* 124.1-3 (1996), pp. 1–9. ISSN: 0020-9910. DOI: 10.1007/s002220050044. URL: https://doi.org/10.1007/s002220050044.

[BS12] Robert Bradshaw and William Stein. "Heegner points and the arithmetic of elliptic curves over ring class extensions". In: *J. Number Theory* 132.8 (2012), pp. 1707–1719. ISSN: 0022-314X. DOI: 10.1016/j.jnt.2011.12.018.

[BS14a] Manjul Bhargava and Matthew Satriano. "On a notion of "Galois closure" for extensions of rings". In: *J. Eur. Math. Soc. (JEMS)* 16.9 (2014), pp. 1881–1913. ISSN: 1435-9855. DOI: 10.4171/JEMS/478.

[BS14b] Manjul Bhargava and Christopher Skinner. "A positive proportion of elliptic curves over $\mathbb{Q}$ have rank one". In: *J. Ramanujan Math. Soc.* 29.2 (2014), pp. 221–242. ISSN: 0970-1249.

[BS15a] Manjul Bhargava and Arul Shankar. "Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves". In: *Ann. of Math. (2)* 181.1 (2015), pp. 191–242. ISSN: 0003-486X. DOI: 10.4007/annals.2015.181.1.3.

[BS15b] Manjul Bhargava and Arul Shankar. "Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0". In: *Ann. of Math. (2)* 181.2 (2015), pp. 587–621. ISSN: 0003-486X. DOI: 10.4007/annals.2015.181.2.4.

[BSD63] B. J. Birch and H. P. F. Swinnerton-Dyer. "Notes on elliptic curves. I". In: *J. Reine Angew. Math.* 212 (1963), pp. 7–25. ISSN: 0075-4102. DOI: 10.1515/crll.1963.212.7.

[BSD65] B. J. Birch and H. P. F. Swinnerton-Dyer. "Notes on elliptic curves. II". In: *J. Reine Angew. Math.* 218 (1965), pp. 79–108. ISSN: 0075-4102. DOI: 10.1515/crll.1965.218.79.

[BSZ] Manjul Bhargava, Christopher Skinner, and Wei Zhang. "A majority of elliptic curves over $\mathbb{Q}$ satisfy the Birch and Swinnerton conjecture". In: (), pp. 1–17.

[Bye12] Dongho Byeon. "Heegner points on elliptic curves with a rational torsion point". In: *J. Number Theory* 132.12 (2012), pp. 3029–3036. ISSN: 0022-314X. DOI: 10.1016/j.jnt.2012.05.038.

[Cas18] Francesc Castella. "On the p-part of the Birch-Swinnerton-Dyer formula for multiplicative primes". In: *Camb. J. Math.* 6.1 (2018), pp. 1–23. ISSN: 2168-0930. DOI: 10.4310/CJM.2018.v6.n1.a1. URL: https://doi.org/10.4310/CJM.2018.v6.n1.a1.

[Cas59] J. W. S. Cassels. "Arithmetic on curves of genus 1. I. On a conjecture of Selmer". In: *J. Reine Angew. Math.* 202 (1959), pp. 52–99. ISSN: 0075-4102. DOI: 10.1515/crll.1959.202.52.

[Cas60] J. W. S. Cassels. "Arithmetic on curves of genus 1. II. A general result". In: *J. Reine Angew. Math.* 203 (1960), pp. 174–208. ISSN: 0075-4102. DOI: 10.1515/crll.1960.203.174.

[Cas62a] J. W. S. Cassels. “Arithmetic on curves of genus 1. III. The Tate-Šafarevič and Selmer groups”. In: *Proc. London Math. Soc. (3)* 12 (1962), pp. 259–296. ISSN: 0024-6115. DOI: 10.1112/plms/s3-12.1.259.

[Cas62b] J. W. S. Cassels. “Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung”. In: *J. Reine Angew. Math.* 211 (1962), pp. 95–112. ISSN: 0075-4102. DOI: 10.1515/crll.1962.211.95.

[Cas63a] J. W. S. Cassels. “Arithmetic on an elliptic curve”. In: *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*. Inst. Mittag-Leffler, Djursholm, 1963, pp. 234–246.

[Cas63b] J. W. S. Cassels. “Arithmetic on curves of genus 1. V. Two counterexamples”. In: *J. London Math. Soc.* 38 (1963), pp. 244–248. ISSN: 0024-6107. DOI: 10.1112/jlms/s1-38.1.244.

[Cas64a] J. W. S. Cassels. “Arithmetic on curves of genus 1. VI. The Tate-Šafarevič group can be arbitrarily large”. In: *J. Reine Angew. Math.* 214/215 (1964), pp. 65–70. ISSN: 0075-4102. DOI: 10.1515/crll.1964.214-215.65.

[Cas64b] J. W. S. Cassels. “Arithmetic on curves of genus 1. VII. The dual exact sequence”. In: *J. Reine Angew. Math.* 216 (1964), pp. 150–158. ISSN: 0075-4102. DOI: 10.1515/crll.1964.216.150.

[Cas65] J. W. S. Cassels. “Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer”. In: *J. Reine Angew. Math.* 217 (1965), pp. 180–199. ISSN: 0075-4102. DOI: 10.1515/crll.1965.217.180.

[Cas91] J. W. S. Cassels. *Lectures on elliptic curves*. Vol. 24. London Mathematical Society Student Texts. Cambridge University Press, Cambridge, 1991, pp. vi+137. ISBN: 0-521-41517-9; 0-521-42530-1. DOI: 10.1017/CBO9781139172530.

[CFS10] John E. Cremona, Tom A. Fisher, and Michael Stoll. "Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves". In: *Algebra Number Theory* 4.6 (2010), pp. 763–820. ISSN: 1937-0652. DOI: 10.2140/ant.2010.4.763.

[Cla+14] Pete L. Clark et al. "Computation on elliptic curves with complex multiplication". In: *LMS J. Comput. Math.* 17.1 (2014), pp. 509–535. ISSN: 1461-1570. DOI: 10.1112/S1461157014000072.

[CM00] John E. Cremona and Barry Mazur. "Visualizing elements in the Shafarevich-Tate group". In: *Experiment. Math.* 9.1 (2000), pp. 13–28. ISSN: 1058-6458.

[CPS06] J. E. Cremona, M. Prickett, and Samir Siksek. "Height difference bounds for elliptic curves over number fields". In: *J. Number Theory* 116.1 (2006), pp. 42–68. ISSN: 0022-314X. DOI: 10.1016/j.jnt.2005.03.001.

[Cre+08] J. E. Cremona et al. "Explicit n-descent on elliptic curves. I. Algebra". In: *J. Reine Angew. Math.* 615 (2008), pp. 121–155. ISSN: 0075-4102. DOI: 10.1515/CRELLE.2008.012.

[Cre+09] J. E. Cremona et al. "Explicit n-descent on elliptic curves. II. Geometry". In: *J. Reine Angew. Math.* 632 (2009), pp. 63–84. ISSN: 0075-4102. DOI: 10.1515/CRELLE.2009.050.

[Cre+15] J. E. Cremona et al. "Explicit n-descent on elliptic curves III. Algorithms". In: *Math. Comp.* 84.292 (2015), pp. 895–922. ISSN: 0025-5718. DOI: 10.1090/S0025-5718-2014-02858-5.

[Cre01a] J. E. Cremona. "Classical invariants and 2-descent on elliptic curves". In: *J. Symbolic Comput.* 31.1-2 (2001). Computational algebra and number theory (Milwaukee, WI, 1996), pp. 71–87. ISSN: 0747-7171. DOI: 10.1006/jsco.1998.1004.

[Cre01b] J. E. Cremona. "Corrigendum: "Reduction of binary cubic and quartic forms" [LMS J. Comput. Math. **2** (1999), 64–94 (electronic); MR1693411 (2000f:11040)]".

In: *LMS J. Comput. Math.* 4 (2001), p. 73. ISSN: 1461-1570. DOI: 10.1112/S1461157000000814.

[Cre14] Brendan Creutz. "Second p-descents on elliptic curves". In: *Math. Comp.* 83.285 (2014), pp. 365–409. ISSN: 0025-5718. DOI: 10.1090/S0025-5718-2013-02713-5.

[Cre97a] J. E. Cremona. *Algorithms for modular elliptic curves*. Second. Cambridge University Press, Cambridge, 1997, pp. vi+376. ISBN: 0-521-59820-6.

[Cre97b] John E. Cremona. "Computing periods of cusp forms and modular elliptic curves". In: *Experiment. Math.* 6.2 (1997), pp. 97–107. ISSN: 1058-6458.

[Cre99] J. E. Cremona. "Reduction of binary cubic and quartic forms". In: *LMS J. Comput. Math.* 2 (1999), pp. 64–94. ISSN: 1461-1570. DOI: 10.1112/S1461157000000073. URL: https://doi.org/10.1112/S1461157000000073.

[CY97] John Coates and S. T. Yau, eds. *Elliptic curves, modular forms & Fermat's last theorem*. International Press, Cambridge, MA, 1997, pp. iv+340. ISBN: 1-57146-049-7.

[Dan+18] Harris B. Daniels et al. "Torsion subgroups of rational elliptic curves over the compositum of all cubic fields". In: *Math. Comp.* 87.309 (2018), pp. 425–458. ISSN: 0025-5718. DOI: 10.1090/mcom/3213.

[Dar98] H. Darmon. "Stark-Heegner points over real quadratic fields". In: *Number theory (Tiruchirapalli, 1996)*. Vol. 210. Contemp. Math. Amer. Math. Soc., Providence, RI, 1998, pp. 41–69. DOI: 10.1090/conm/210/02783.

[DD15] Tim Dokchitser and Vladimir Dokchitser. "Growth of Sha in towers for isogenous curves". In: *Compos. Math.* 151.11 (2015), pp. 1981–2005. ISSN: 0010-437X. DOI: 10.1112/S0010437X15007423.

[Del01] Christophe Delaunay. "Heuristics on Tate-Shafarevitch groups of elliptic curves defined over $\mathbb{Q}$". In: *Experiment. Math.* 10.2 (2001), pp. 191–196. ISSN: 1058-6458. URL: http://projecteuclid.org/euclid.em/999188631.

[Del07] Christophe Delaunay. "Heuristics on class groups and on Tate-Shafarevich groups: the magic of the Cohen-Lenstra heuristics". In: *Ranks of elliptic curves and random matrix theory*. Vol. 341. London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 2007, pp. 323–340. DOI: 10.1017/CBO9780511735158.021.

[DI95] Fred Diamond and John Im. "Modular forms and modular curves". In: *Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994)*. Vol. 17. CMS Conf. Proc. Amer. Math. Soc., Providence, RI, 1995, pp. 39–133.

[Dok04] Tim Dokchitser. "Computing special values of motivic L-functions". In: *Experiment. Math.* 13.2 (2004), pp. 137–149. ISSN: 1058-6458. URL: http://projecteuclid.org/euclid.em/1090350929.

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*. Vol. 228. Graduate Texts in Mathematics. Springer-Verlag, New York, 2005, pp. xvi+436. ISBN: 0-387-23229-X.

[DS18] Andrzej Dabrowski and Lucjan Szymaszkiewicz. "Orders of Tate-Shafarevich groups for the Neumann-Setzer type elliptic curves". In: *Math. Comp.* 87.311 (2018), pp. 1509–1522. ISSN: 0025-5718. DOI: 10.1090/mcom/3248.

[DSS00] Z. Djabri, Edward F. Schaefer, and N. P. Smart. "Computing the p-Selmer group of an elliptic curve". In: *Trans. Amer. Math. Soc.* 352.12 (2000), pp. 5583–5597. ISSN: 0002-9947. DOI: 10.1090/S0002-9947-00-02535-6.

[Fis] *Elements of order 5 in the Tate-Shafarevich group*. https://www.dpmms.cam.ac.uk/~taf1000/g1data/order5.html. Accessed: 2019-02-04.

[Fis01] Tom Fisher. "Some examples of 5 and 7 descent for elliptic curves over $\mathbf{Q}$". In: *J. Eur. Math. Soc. (JEMS)* 3.2 (2001), pp. 169–201. ISSN: 1435-9855. DOI: 10.1007/s100970100030.

[Fis08a] Tom Fisher. "Finding rational points on elliptic curves using 6-descent and 12-descent". In: *J. Algebra* 320.2 (2008), pp. 853–884. ISSN: 0021-8693. DOI: 10.1016/j.jalgebra.2008.04.007.

[Fis08b] Tom Fisher. "The invariants of a genus one curve". In: *Proc. Lond. Math. Soc. (3)* 97.3 (2008), pp. 753–782. ISSN: 0024-6115. DOI: 10.1112/plms/pdn021.

[Fis12] Tom Fisher. "The Hessian of a genus one curve". In: *Proc. Lond. Math. Soc. (3)* 104.3 (2012), pp. 613–648. ISSN: 0024-6115. DOI: 10.1112/plms/pdr039.

[Fis13a] Tom Fisher. "Explicit 5-descent on elliptic curves". In: *ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium*. Vol. 1. Open Book Ser. Math. Sci. Publ., Berkeley, CA, 2013, pp. 395–411. DOI: 10.2140/obs.2013.1.395.

[Fis13b] Tom Fisher. "Minimisation and reduction of 5-coverings of elliptic curves". In: *Algebra Number Theory* 7.5 (2013), pp. 1179–1205. ISSN: 1937-0652. DOI: 10.2140/ant.2013.7.1179.

[Fis16] Tom Fisher. "Visualizing elements of order 7 in the Tate-Shafarevich group of an elliptic curve". In: *LMS J. Comput. Math.* 19.suppl. A (2016), pp. 100–114. ISSN: 1461-1570. DOI: 10.1112/S1461157016000243.

[GKZ87] B. Gross, W. Kohnen, and D. Zagier. "Heegner points and derivatives of L-series. II". In: *Math. Ann.* 278.1-4 (1987), pp. 497–562. ISSN: 0025-5831. DOI: 10.1007/BF01458081.

[Gol79] Dorian Goldfeld. "Conjectures on elliptic curves over quadratic fields". In: *Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979)*. Vol. 751. Lecture Notes in Math. Springer, Berlin, 1979, pp. 108–118.

[Gol92] Dorian Goldfeld. "On the computational complexity of modular symbols". In: *Math. Comp.* 58.198 (1992), pp. 807–814. ISSN: 0025-5718. DOI: 10.2307/2153219.

[Gre16] Ralph Greenberg. "On the structure of Selmer groups". In: *Elliptic curves, modular forms and Iwasawa theory*. Vol. 188. Springer Proc. Math. Stat. Springer, Cham, 2016, pp. 225–252.

[Gri+09] Grigor Grigorov et al. "Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves". In: *Math. Comp.* 78.268 (2009), pp. 2397–2425. ISSN: 0025-5718. DOI: 10.1090/S0025-5718-09-02253-4. URL: https://doi.org/10.1090/S0025-5718-09-02253-4.

[Gro91] Benedict H. Gross. "Kolyvagin's work on modular elliptic curves". In: *L-functions and arithmetic (Durham, 1989)*. Vol. 153. London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 1991, pp. 235–256. DOI: 10.1017/CBO9780511526053.009.

[GV83] D. Goldfeld and C. Viola. "Some conjectures on elliptic curves over cyclotomic fields". In: *Trans. Amer. Math. Soc.* 276.2 (1983), pp. 511–515. ISSN: 0002-9947. DOI: 10.2307/1999064.

[GZ86] Benedict H. Gross and Don B. Zagier. "Heegner points and derivatives of L-series". In: *Invent. Math.* 84.2 (1986), pp. 225–320. ISSN: 0020-9910. DOI: 10.1007/BF01388809.

[HB93] D. R. Heath-Brown. "The size of Selmer groups for the congruent number problem". In: *Invent. Math.* 111.1 (1993), pp. 171–195. ISSN: 0020-9910. DOI: 10.1007/BF01231285.

[HB94] D. R. Heath-Brown. "The size of Selmer groups for the congruent number problem. II". In: *Invent. Math.* 118.2 (1994). With an appendix by P. Monsky, pp. 331–370. ISSN: 0020-9910. DOI: 10.1007/BF01231536.

[HS00] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*. Vol. 201. Graduate Texts in Mathematics. An introduction. Springer-Verlag, New York, 2000, pp. xiv+558. ISBN: 0-387-98975-7; 0-387-98981-1. DOI: 10.1007/978-1-4612-1210-2.

[HS17] Robert Harron and Andrew Snowden. "Counting elliptic curves with prescribed torsion". In: *J. Reine Angew. Math.* 729 (2017), pp. 151–170. ISSN: 0075-4102. DOI: 10.1515/crelle-2014-0107.

[IP06] Adrian Iovita and Robert Pollack. "Iwasawa theory of elliptic curves at supersingular primes over $\mathbb{Z}_p$-extensions of number fields". In: *J. Reine Angew. Math.* 598 (2006), pp. 71–103. ISSN: 0075-4102. DOI: 10.1515/CRELLE.2006.069.

[JS07] Dimitar P. Jetchev and William A. Stein. "Visibility of the Shafarevich-Tate group at higher level". In: *Doc. Math.* 12 (2007), pp. 673–696. ISSN: 1431-0635.

[JSW17] Dimitar Jetchev, Christopher Skinner, and Xin Wan. "The Birch and Swinnerton-Dyer formula for elliptic curves of analytic rank one". In: *Camb. J. Math.* 5.3 (2017), pp. 369–434. ISSN: 2168-0930. DOI: 10.4310/CJM.2017.v5.n3.a2. URL: https://doi.org/10.4310/CJM.2017.v5.n3.a2.

[Kan13] Daniel Kane. "On the ranks of the 2-Selmer groups of twists of a given elliptic curve". In: *Algebra Number Theory* 7.5 (2013), pp. 1253–1279. ISSN: 1937-0652. DOI: 10.2140/ant.2013.7.1253.

[Kat76] Nicholas M. Katz. "p-adic interpolation of real analytic Eisenstein series". In: *Ann. of Math. (2)* 104.3 (1976), pp. 459–571. ISSN: 0003-486X. DOI: 10.2307/1970966.

[Kim13] Dohyeong Kim. "On the p-primary part of Tate-Shafarevich group of elliptic curves over (Q) when p is supersingular". In: *Bull. Korean Math. Soc.* 50.2 (2013), pp. 407–416. ISSN: 1015-8634. DOI: 10.4134/BKMS.2013.50.2.407.

[Klo05] Remke Kloosterman. "The p-part of the Tate-Shafarevich groups of elliptic curves can be arbitrarily large". In: *J. Théor. Nombres Bordeaux* 17.3 (2005), pp. 787–800. ISSN: 1246-7405.

[Koh96] David Russell Kohel. *Endomorphism rings of elliptic curves over finite fields.* Thesis (Ph.D.)–University of California, Berkeley. ProQuest LLC, Ann Arbor, MI, 1996, p. 117. ISBN: 978-0591-32123-4.

[Kol91a] V. A. Kolyvagin. "On the structure of Selmer groups". In: *Math. Ann.* 291.2 (1991), pp. 253–259. ISSN: 0025-5831. DOI: 10.1007/BF01445205.

[Kol91b] V. A. Kolyvagin. "On the structure of Shafarevich-Tate groups". In: *Algebraic geometry (Chicago, IL, 1989).* Vol. 1479. Lecture Notes in Math. Springer, Berlin, 1991, pp. 94–121. DOI: 10.1007/BFb0086267.

[Kol91c] Victor Alecsandrovich Kolyvagin. "On the Mordell-Weil group and the Shafarevich-Tate group of modular elliptic curves". In: *Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990).* Math. Soc. Japan, Tokyo, 1991, pp. 429–436.

[KS01] Leopoldo Kulesz and Colin Stahlke. "Elliptic curves of high rank with nontrivial torsion group over $\mathbb{Q}$". In: *Experiment. Math.* 10.3 (2001), pp. 475–480. ISSN: 1058-6458.

[Kub79] Daniel Sion Kubert. "Universal bounds on the torsion of elliptic curves". In: *Compositio Math.* 38.1 (1979), pp. 121–128. ISSN: 0010-437X.

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

[Lem00] Franz Lemmermeyer. "On Tate-Shafarevich groups of some elliptic curves". In: *Algebraic number theory and Diophantine analysis (Graz, 1998).* de Gruyter, Berlin, 2000, pp. 277–291.

[Mat09] Kazuo Matsuno. "Elliptic curves with large Tate-Shafarevich groups over a number field". In: *Math. Res. Lett.* 16.3 (2009), pp. 449–461. ISSN: 1073-2780. DOI: 10.4310/MRL.2009.v16.n3.a6.

[MMR07] Josep M. Miret, Ramiro Moreno, and Anna Rio. "Generalization of Vélu's formulae for isogenies between elliptic curves". In: *Publ. Mat.* Proceedings of the Primeras Jornadas de Teoría de Números (2007), pp. 147–163. ISSN: 0214-1493. DOI: 10.5565/PUBLMAT_PJTN05_07.

[MSS96] J. R. Merriman, S. Siksek, and N. P. Smart. "Explicit 4-descents on an elliptic curve". In: *Acta Arith.* 77.4 (1996), pp. 385–404. ISSN: 0065-1036. DOI: 10.4064/aa-77-4-385-404.

[MST] Barry Mazur, William Stein, and John Tate. "Computation of p-adic heights and log convergence". In: Extra Vol. (), pp. 577–614. ISSN: 1431-0635.

[MT91] B. Mazur and J. Tate. "The p-adic sigma function". In: *Duke Math. J.* 62.3 (1991), pp. 663–688. ISSN: 0012-7094. DOI: 10.1215/S0012-7094-91-06229-0.

[MTT86] B. Mazur, J. Tate, and J. Teitelbaum. "On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer". In: *Invent. Math.* 84.1 (1986), pp. 1–48. ISSN: 0020-9910. DOI: 10.1007/BF01388731.

[Pol03] Robert Pollack. "On the p-adic L-function of a modular form at a supersingular prime". In: *Duke Math. J.* 118.3 (2003), pp. 523–558. ISSN: 0012-7094. DOI: 10.1215/S0012-7094-03-11835-9.

[PR12] Bjorn Poonen and Eric Rains. "Random maximal isotropic subspaces and Selmer groups". In: *J. Amer. Math. Soc.* 25.1 (2012), pp. 245–269. ISSN: 0894-0347. DOI: 10.1090/S0894-0347-2011-00710-8.

[PS99] Bjorn Poonen and Michael Stoll. "The Cassels-Tate pairing on polarized abelian varieties". In: *Ann. of Math. (2)* 150.3 (1999), pp. 1109–1149. ISSN: 0003-486X. DOI: 10.2307/121064.

[SC02] Michael Stoll and John E. Cremona. "Minimal models for 2-coverings of elliptic curves". In: *LMS J. Comput. Math.* 5 (2002), pp. 220–243. ISSN: 1461-1570. DOI: 10.1112/S1461157000000760.

[SD08] Peter Swinnerton-Dyer. "The effect of twisting on the 2-Selmer group". In: *Math. Proc. Cambridge Philos. Soc.* 145.3 (2008), pp. 513–526. ISSN: 0305-0041. DOI: 10.1017/S0305004108001588.

[SD13] Peter Swinnerton-Dyer. "2^n-descent on elliptic curves for all n". In: *J. Lond. Math. Soc. (2)* 87.3 (2013), pp. 707–723. ISSN: 0024-6107. DOI: 10.1112/jlms/jds063.

[Set75] Bennett Setzer. "Elliptic curves of prime conductor". In: *J. London Math. Soc. (2)* 10 (1975), pp. 367–378. ISSN: 0024-6107. DOI: 10.1112/jlms/s2-10.3.367.

[Set78] Bennett Setzer. "Elliptic curves over complex quadratic fields". In: *Pacific J. Math.* 74.1 (1978), pp. 235–250. ISSN: 0030-8730.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513. ISBN: 978-0-387-09493-9. DOI: 10.1007/978-0-387-09494-6.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Vol. 151. Graduate Texts in Mathematics. Springer-Verlag, New York, 1994, pp. xiv+525. ISBN: 0-387-94328-5. DOI: 10.1007/978-1-4612-0851-8.

[SS04] Edward F. Schaefer and Michael Stoll. "How to do a p-descent on an elliptic curve". In: *Trans. Amer. Math. Soc.* 356.3 (2004), pp. 1209–1231. ISSN: 0002-9947. DOI: 10.1090/S0002-9947-03-03366-X.

[Ste04] William A. Stein. "Shafarevich-Tate groups of nonsquare order". In: *Modular curves and abelian varieties*. Vol. 224. Progr. Math. Birkhäuser, Basel, 2004, pp. 277–289.

[SW02] William A. Stein and Mark Watkins. “A database of elliptic curves—first report”. In: *Algorithmic number theory (Sydney, 2002)*. Vol. 2369. Lecture Notes in Comput. Sci. Springer, Berlin, 2002, pp. 267–275. DOI: 10.1007/3-540-45455-1_22.

[SW04] William Stein and Mark Watkins. “Modular parametrizations of Neumann-Setzer elliptic curves”. In: *Int. Math. Res. Not.* 27 (2004), pp. 1395–1405. ISSN: 1073-7928. DOI: 10.1155/S1073792804133916.

[SW13] William Stein and Christian Wuthrich. “Algorithms for the arithmetic of elliptic curves using Iwasawa theory”. In: *Math. Comp.* 82.283 (2013), pp. 1757–1792. ISSN: 0025-5718. DOI: 10.1090/S0025-5718-2012-02649-4.

[Tat63] John Tate. “Duality theorems in Galois cohomology over number fields”. In: *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*. Inst. Mittag-Leffler, Djursholm, 1963, pp. 288–295.

[Tat75] J. Tate. “Algorithm for determining the type of a singular fiber in an elliptic pencil”. In: (1975), 33–52. Lecture Notes in Math., Vol. 476.

[Wat02] Mark Watkins. “Computing the modular degree of an elliptic curve”. In: *Experiment. Math.* 11.4 (2002), 487–502 (2003). ISSN: 1058-6458.

[Wat08] Mark Watkins. “Some heuristics about elliptic curves”. In: *Experiment. Math.* 17.1 (2008), pp. 105–125. ISSN: 1058-6458.

[Wat12] Mark Watkins. “Some remarks on Heegner point computations”. In: *Explicit methods in number theory*. Vol. 36. Panor. Synthèses. Soc. Math. France, Paris, 2012, pp. 81–97.

[Wei07] André Weil. *Number theory*. Modern Birkhäuser Classics. An approach through history from Hammurapi to Legendre, Reprint of the 1984 edition. Birkhäuser Boston, Inc., Boston, MA, 2007, pp. xxii+377. ISBN: 978-0-8176-4565-6; 0-8176-4565-9.

[Wut18] Christian Wuthrich. "Numerical modular symbols for elliptic curves". In: *Math. Comp.* 87.313 (2018), pp. 2393–2423. ISSN: 0025-5718. DOI: 10.1090/mcom/3274.