Open Questions in Arithmetic Algebraic Geometry

Alice Silverberg

Contents

Open Questions in Arithmetic Algebraic Geometry 1

Chapter 1. Overview 1
1.1. Introduction. 1
1.2. Elliptic curves. 2
1.3. Abelian varieties. 3
1.4. Mordell-Weil groups. 4
1.5. Torsion subgroups. 5
1.6. Ranks. 6
1.7. Looking ahead. 6
1.8. Suggested reading. 6

Chapter 2. Torsion subgroups 7
2.1. Torsion subgroups for elliptic curves. 7
2.2. A quick look at modular curves. 7
2.3. Conjectures. 9
2.4. Other results for elliptic curves. 9
2.5. Abelian varieties over number fields. 11
2.6. Abelian varieties over other fields. 14
2.7. Digression on complex multiplication. 14

Chapter 3. Ranks 15
3.1. Examples. 15
3.2. Unboundedness/boundedness. 16
3.3. Vary the field. 17
3.4. Quadratic twists. 17
3.5. Average ranks. 19
3.6. Distribution of ranks. 20

Chapter 4. Conjectures of Birch and Swinnerton-Dyer 23
4.1. The L-function of an elliptic curve. 23
4.2. Modularity. 25
4.3. BSD I. 26
4.4. The Congruent Number Problem. 28
4.5. Evidence for BSD I. 28
4.6. BSD II. 29
4.7. Evidence for BSD II. 31
4.8. Selmer groups. 32
4.9. Examples — descents. 33

Chapter 5. ABC and related conjectures 39
5.1. ABC Conjectures. 39
5.2. ABC Conjectures for function fields. 41
5.3. Szpiro Conjecture. 41
5.4. Goldfeld-Szpiro Conjecture. 42
5.5. de Weger Conjectures. 43
5.6. Additional remarks. 44

Chapter 6. Some other conjectures 45
6.1. Integral points on elliptic curves. 45
6.2. Bounds on numbers of rational points on curves. 45
6.3. Conductors of elliptic curves. 46
6.4. Abelian varieties, Shimura varieties, and open questions. 46

Bibliography 49

IAS/Park City Mathematics Series
Volume 00, 0000

Open Questions in Arithmetic Algebraic Geometry

Alice Silverberg

CHAPTER 1
Overview

1.1. Introduction.

This series of lectures introduces some important conjectures in Arithmetic Algebraic Geometry. Arithmetic Algebraic Geometry can be viewed as a branch of Number Theory where one solves number theoretic questions using powerful techniques from Algebraic Geometry. Number Theory and Arithmetic Algebraic Geometry grew out of studying classical questions concerned with finding whole number solutions to polynomial equations (with whole number coefficients). Fermat's Last Theorem is one such classical question. Starting with the simplest polynomial equations, one first encounters linear and quadratic equations, which are easy to solve. Next one is naturally led to consider cubic equations, and here one is already in an area with deep mathematical ideas, results, and conjectures. Elliptic curves are smooth projective cubics in the plane, and their study is part of a rich and beautiful theory, with many as yet unanswered questions.

Our central objects of study will be elliptic curves and (their higher-dimensional generalizations) abelian varieties, along with modular curves, Shimura curves, modular forms, automorphic forms, L-functions, and ℓ-adic representations.

[1]Department of Mathematics, Ohio State University, 231 West 18 Avenue, Columbus, Ohio 43210-1174, USA.
E-mail address: `silver@math.ohio-state.edu`.
Key words and phrases. Arithmetic algebraic geometry, elliptic curves, abelian varieties, conjectures.
The author was supported in part by the NSF, the NSA, and the Alexander von Humboldt Foundation. She would like to thank B. Birch, A. Brumer, B. Conrad, N. Elkies, H. Lange, K. Rubin, J-P. Serre, G. Shimura, and B. de Weger for helpful comments on earlier versions of the manuscript, the audience at the lectures for helpful feedback, A. Agashe for help collecting the references, and the Mathematics Institute of the University of Erlangen for its hospitality. Chapter 5 owes a lot to de Weger's paper [**183**].

I hope that at least the first few chapters will be accessible to a wide audience (including undergraduates, teachers,...).

The exercises are designed to help the reader explore and become more at home with the topics, ideas, and objects. They are of varying difficulties, and can sometimes be explored from several directions or on several levels (computationally, theoretically, etc.). The exercises are not necessary for following the course.

I do not claim to be complete in these notes, nor do I claim to always focus on the most interesting or deepest problems or results (sometimes I have chosen what's fun or easy to explain, rather than what's cutting edge).

The first chapter gives an overview and introduction. We introduce elliptic curves, abelian varieties, and Mordell-Weil groups, and ask some questions about them. In later chapters we examine these questions and others in more detail, discussing some of the progress that has been made, and identifying which questions are still open.

This write-up combines my talks in Princeton and Park City. The chapters do not precisely correspond to the lectures. In Park City I gave (approximately) one lecture of overview, one lecture on torsion subgroups, two lectures on ranks, two lectures on the conjectures of Birch and Swinnerton-Dyer, and one lecture on ABC and other conjectures. In Princeton I gave an overview and a more compact treatment of the topics, focusing on Mordell-Weil groups, ranks, and the conjectures of Birch and Swinnerton-Dyer.

1.2. Elliptic curves.

Definition 1.2.1. An *elliptic curve* over the rational numbers $\mathbf{Q}$ is the projective curve associated to an affine equation of the form

$$y^2 = x^3 + ax + b \tag{1}$$

where a and b are integers such that

$$4a^3 + 27b^2 \neq 0.$$

The *discriminant* of the above elliptic curve E is

$$\Delta(E) = -16(4a^3 + 27b^2).$$

The condition $4a^3 + 27b^2 \neq 0$ is equivalent to the curve being smooth.

Exercise 1.2.2. *Show that if a and b are complex numbers, then the following are equivalent:*

(i) $4a^3 + 27b^2 \neq 0$,
(ii) *the cubic $x^3 + ax + b$ has three distinct complex roots,*
(iii) *there are no complex values of x and y for which both partial derivatives of $x^3 + ax + b - y^2$ vanish.*

Example 1.2.3. Consider the elliptic curve

$$E : y^2 = x^3 - x.$$

This curve was considered by Fermat. He showed that the only rational solutions are $(0,0), (1,0), (-1,0)$.

Definition 1.2.4. An *elliptic curve* E over a field K is a smooth projective curve of genus one with a point $P \in E(K)$. Equivalently, it is a smooth projective plane cubic over K with a point over K. Equivalently, it is a smooth projective curve with an affine equation of the form

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

where the a_i are in K. If the characteristic of K is not 2 or 3, then E has an equation (called a *Weierstrass form* for E) of the form (1), with $a, b \in K$. Equation (2) is called a *generalized Weierstrass form*.

The K-rational points of E form an abelian group. The group law (since it's abelian we will call it an addition law) is based on the principle that a line meets a cubic in 3 points, and is defined by the rule that the 3 points of intersection of a line with the cubic sum to O in the addition law. The identity element for the group law, O, is the point with projective coordinates $(x, y, z) = (0, 1, 0)$, where we are viewing the curve as a projective curve with homogeneous equation

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

In affine coordinates we would call this point (∞, ∞). This point is often called the *point at infinity*, and can be viewed as the point where all vertical lines meet (if we graph the affine equation in the plane).

Exercise 1.2.5. *Verify that when the elliptic curve E has equation $y^2 = x^3+ax+b$, then the points of order 2 for the group law are exactly the points with $y = 0$.*

Exercise 1.2.6. *Verify that if P is a point on an elliptic curve with an equation as in (2), then the x-coordinate of P is the same as the x-coordinate of $-P$ (where $-P$ is the inverse of P with respect to the addition law).*

Definition 1.2.7. A *homomorphism* of elliptic curves over a field K is a map which is both a morphism over K (i.e., is defined by polynomial equations with coefficients in K) and a group homomorphism.

Exercise 1.2.8. *If E is an elliptic curve over K in generalized Weierstrass form, show that every isomorphism of E to another elliptic curve over K in generalized Weierstrass form can be given by a change of variables of the form $x \mapsto u^2x + r$, $y \mapsto u^3y + u^2sx + t$ with $r, s, t, u \in K$ and $u \neq 0$. Further, show that every such change of variables produces an isomorphism.*

1.3. Abelian varieties.

In these lectures I will sometimes state results and conjectures for abelian varieties over number fields. If you prefer a more concrete approach, you can substitute the phrase "elliptic curve over $\mathbf{Q}$" for the phrase "abelian variety over a number field" throughout the lectures. However, some of the conjectures will be theorems in the case of elliptic curves.

Definition 1.3.1. An *abelian variety* is a connected projective variety which is also an algebraic group.

Examples 1.3.2. The one-dimensional abelian varieties are exactly the elliptic curves. Products of abelian varieties are abelian varieties. Jacobian varieties of curves of genus g are abelian varieties of dimension g. For example, if C is a curve given by a smooth (i.e., there is no point at which all partial derivatives vanish) homogeneous polynomial in x, y, and z of degree N (for example, the Fermat equation $x^N + y^N = z^N$), then C has genus $(N-1)(N-2)/2$, and its Jacobian variety $J(C)$ has dimension $(N-1)(N-2)/2$.

1.4. Mordell-Weil groups.

If A is an abelian variety over a field K, then the group of K-rational points of A is denoted $A(K)$. This group is called the *Mordell-Weil group* of A over K if K is a number field (because of the following theorem, proved for elliptic curves over $\mathbf{Q}$ by Mordell, and generalized by Weil).

Theorem 1.4.1 (Mordell-Weil Theorem). *If A is an abelian variety over a number field K, then $A(K)$ is a finitely generated abelian group.*

In other words, if A is an abelian variety over a number field K, then

$$A(K) \cong \mathbf{Z}^r \oplus A(K)_{\mathrm{tors}} \tag{3}$$

where r is a non-negative integer, called the *rank* of $A(K)$, and $A(K)_{\mathrm{tors}}$ is a finite group, called the *torsion subgroup* of $A(K)$. The elements of $A(K)_{\mathrm{tors}}$ (i.e., the points of finite order with respect to the group law on A) are called the *torsion points* of $A(K)$.

In these notes we will discuss what is known and what is not yet known about Mordell-Weil groups of abelian varieties. We begin with some examples (without proof). Later, we will learn more about how to compute Mordell-Weil groups.

Example 1.4.2. Consider

$$E : y^2 = x^3 - x.$$

Then

$$E(\mathbf{Q}) = \{O, (0,0), (1,0), (-1,0)\} \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z},$$

as shown by Fermat. Further,

$$\begin{aligned} E(\mathbf{Q}(i)) &= \{O, (0,0), (1,0), (-1,0), (i, i-1), (i, 1-i), (-i, 1+i), (-i, -1-i)\} \\ &\cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}, \end{aligned}$$

where i is a square root of -1.

Exercise 1.4.3. *Calculate directly the orders of the points in $E(\mathbf{Q}(i))$ (by using the group law) in the previous example.*

Example 1.4.4. Consider

$$E : y^2 = x^3 - 2x.$$

Then

$$E(\mathbf{Q}) \cong \mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z},$$

and $E(\mathbf{Q})$ is generated by the point of infinite order $(-1, 1)$ and the point of order two $(0, 0)$.

Example 1.4.5. Consider

$$E : y^2 = x^3 + 17.$$

Then

$$E(\mathbf{Q}) \cong \mathbf{Z}^2,$$

and $E(\mathbf{Q}) = \mathbf{Z}P_1 + \mathbf{Z}P_2$ where $P_1 = (-2, 3)$ and $P_2 = (2, 5)$.

Exercise 1.4.6. *The equation*

$$y^2 = x^3 + 17$$

has exactly 16 *solutions with* x *and* y *both integers. Find them.*

Example 1.4.7. Consider

$$E : y^2 = x^3 - 17x.$$

Then

$$E(\mathbf{Q}) \cong \mathbf{Z}^2 \oplus \mathbf{Z}/2\mathbf{Z},$$

and $E(\mathbf{Q})/E(\mathbf{Q})_{\text{tors}}$ is generated by $(-1, 4)$ and $(9, 24)$.

1.5. Torsion subgroups.

By the following result, given an elliptic curve E over $\mathbf{Q}$ (and clearing denominators to make the coefficients integers), the torsion subgroup $E(\mathbf{Q})_{\text{tors}}$ can be computed in a finite amount of time.

Theorem 1.5.1 (Nagell [**110**], Lutz [**84**]). *If* $E : y^2 = x^3 + ax + b$ *is an elliptic curve with* $a, b \in \mathbf{Z}$, *and* (x, y) *is a non-zero rational point on* E *of finite order, then* x *and* y *are integers, and either* $y = 0$ *or* y^2 *is a divisor of* $4a^3 + 27b^2$.

Exercise 1.5.2. *Compute* $E(\mathbf{Q})_{\text{tors}}$, *for*

$$E : y^2 = x^3 + 4x.$$

Find the orders of all the torsion points.

Exercise 1.5.3. *Compute* $E(\mathbf{Q})_{\text{tors}}$, *for*

$$E : y^2 = x^3 + 1.$$

Find the orders of all the torsion points.

There are many questions one can ask about torsion points and torsion subgroups, for elliptic curves and for abelian varieties.

Which positive integers occur as orders of torsion points on elliptic curves over $\mathbf{Q}$? (In the examples in §1.4, we have only seen the integers 2 and 1. There are more in the exercises.) Do they all occur? Do infinitely many occur? What about over number fields other than $\mathbf{Q}$? For example, can one find an integer d and an elliptic curve over $\mathbf{Q}(\sqrt{d})$ with a point over $\mathbf{Q}(\sqrt{d})$ of order 17?

Which finite abelian groups can occur as $E(\mathbf{Q})_{\text{tors}}$'s, with E an elliptic curve over $\mathbf{Q}$? (We have seen $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z}$, and the trivial group. Other groups appear in the above exercises.) Do all finite abelian groups occur? Do infinitely many occur? What about over number fields other than $\mathbf{Q}$? (We have seen $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ over $\mathbf{Q}(i)$.) What about abelian varieties over $\mathbf{Q}$ (of a fixed dimension, say)? Or abelian varieties (of a fixed dimension) over a fixed number field? Or abelian varieties (of a fixed dimension) over all number fields of a fixed degree over $\mathbf{Q}$?

We will discuss these questions in Chapter 2.

1.6. Ranks.

We have seen (above) examples of elliptic curves over **Q** of ranks 0, 1, and 2. There are many interesting questions about ranks. For example, what integers can occur as the ranks of Mordell-Weil groups of elliptic curves over **Q**? Do all non-negative integers occur? Is the set of non-negative integers which occur unbounded? If r is a non-negative integer, how "often" does r occur as the rank of the Mordell-Weil group of an elliptic curve over **Q**?

What is the "average rank" as one runs over elliptic curves over **Q**? This depends on how one defines "average rank". Once we define it, what is its numerical value? Is it unbounded? Is it zero?

Suppose we restrict to a family of elliptic curves over **Q** (or a family of abelian varieties of fixed dimension over a fixed number field, or a family of abelian varieties of fixed dimension over all number fields of a fixed degree over **Q**). For this family, we can ask the above questions about ranks. Are they bounded or unbounded in the family? What is the average rank in the family? An example of a family is the family of quadratic twists of a given elliptic curve (i.e, the family $dy^2 = x^3 + ax + b$, where a and b are fixed and d ranges over square-free integers). Another example is the family of cubic twists of $y^2 = x^3 - 432$. This latter family is usually written as the family $x^3 + y^3 = d$, where d is a cube-free integer (a Weierstrass model for the Fermat cubic $x^3 + y^3 = 1$ is $y^2 = x^3 - 432$).

We can ask the same questions for ranks of Mordell-Weil groups of elliptic curves over number fields other than **Q**. Moreover, we can consider ranks of Mordell-Weil groups of abelian varieties over **Q**, or over other number fields.

We will discuss some of these questions in Chapters 3 and 4.

1.7. Looking ahead.

Here are some of the major topics we will discuss in these lectures:

- **Torsion** Conjectures (for elliptic curves and abelian varieties);
- Conjectures about **ranks** (mostly for elliptic curves: average ranks in families, boundedness/unboundedness, density of curves of a given rank, ...);
- **Birch and Swinnerton-Dyer** Conjectures (These conjectures relate arithmetic properties or invariants of the variety to properties of its L-function, an analytic object. This includes a conjecture about ranks of Mordell-Weil groups of elliptic curves and abelian varieties, and leads to questions about the Tate-Shafarevich group Ш.);
- **ABC** Conjectures, and relations with other conjectures.

1.8. Suggested reading.

For introductions to elliptic curves, see the books written by Husemöller [**64**], Koblitz [**73**], Silverman [**156**], and Silverman and Tate [**160**]. Cremona's book [**35**] gives elliptic curve algorithms and data. See Cohen's book [**33**] for number theory algorithms, including a chapter on elliptic curves. See Smart's book [**162**] for algorithms for solving Diophantine equations.

Useful elliptic curve software packages include PARI [**4**], mwrank [**36**], and the Maple package Apecs [**34**].

CHAPTER 2
Torsion subgroups

The torsion subgroup is the group of points of finite order in the Mordell-Weil group of an abelian variety or elliptic curve. For elliptic curves, the torsion subgroups are now fairly well understood, as we shall see below. For higher-dimensional abelian varieties there is still much work to be done.

2.1. Torsion subgroups for elliptic curves.

Recall the following theorem stated in the last chapter:

Theorem 2.1.1 (Nagell-Lutz). *If $E : y^2 = x^3 + ax + b$ is an elliptic curve with $a, b \in \mathbf{Z}$, and (x, y) is a non-zero rational point on E of finite order, then x and y are integers, and either $y = 0$ or y^2 is a divisor of $4a^3 + 27b^2$.*

Example 2.1.2. Consider
$$E : y^2 = x^3 + 4x.$$
Then
$$E(\mathbf{Q}) = \{O, (0,0), (2,4), (2,-4)\} \cong \mathbf{Z}/4\mathbf{Z}.$$

Example 2.1.3. Consider
$$E : y^2 = x^3 + 1.$$
Then
$$E(\mathbf{Q}) = \{O, (-1,0), (0,1), (0,-1), (2,3), (2,-3)\} \cong \mathbf{Z}/6\mathbf{Z}.$$

Theorem 2.1.4 (Mazur [**96**]). *If E is an elliptic curve over $\mathbf{Q}$, then the torsion subgroup $E(\mathbf{Q})_{\mathrm{tors}}$ is one of the following 15 groups:*
$$\begin{array}{lll} \mathbf{Z}/N\mathbf{Z} & \textit{for} & N = 1, \ldots, 10 \textit{ or } 12, \\ \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2N\mathbf{Z} & \textit{for} & N = 1, 2, 3, \textit{ or } 4. \end{array}$$

Further, it is known that each of these groups occurs infinitely often (i.e., for infinitely many $\mathbf{Q}$-isomorphism classes).

2.2. A quick look at modular curves.

If K is a subfield of the field $\mathbf{C}$ of complex numbers, and $E : y^2 = x^3 + ax + b$ is an elliptic curve over K, then the points of order 2 are the points where $y = 0$. Therefore the subgroup $E(K)[2]$ of $E(K)$ of points of order 1 or 2 either is the trivial group, or is isomorphic to $\mathbf{Z}/2\mathbf{Z}$ or to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

Exercise 2.2.1. *Show that if E is an elliptic curve over K with $E[2](K) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, then E is isomorphic over K to*

$$E^{d,\lambda} : dy^2 = x(x-1)(x-\lambda) \tag{4}$$

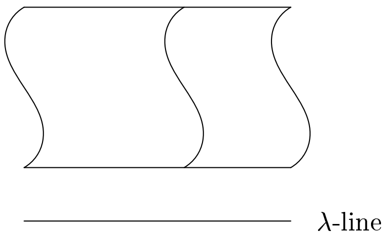
for some $\lambda \in K - \{0,1\}$ and some $0 \neq d \in K$.

Note that conversely, if $\lambda \in K - \{0,1\}$ and $0 \neq d \in K$, then $E^{d,\lambda}$ is an elliptic curve over K with the property that $E^{d,\lambda}(K)[2] \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

We can view the "λ-line" as parametrizing elliptic curves E over K with $E(K)[2] \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ (up to isomorphisms and twists). The equation

$$y^2 = x(x-1)(x-\lambda)$$

can be viewed as the equation of a surface "over" the λ-line (the fibers are the elliptic curves $E^{1,\lambda}$).



Suppose now that we want to write down all the elliptic curves over $\mathbf{Q}$ with a rational point of order 5. Here's what to do.

Suppose more generally that K is a subfield of $\mathbf{C}$, E is an elliptic curve over K, and $P \in E(K)$ is a point of finite order ≥ 4.

By doing a change of variables over K, we can translate P to the point $(0,0)$. This puts the equation for E in the form

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

Note that $a_3 \neq 0$, since otherwise $(0,0)$ would be a point of order 2 (check this!). After the change of variables $y \mapsto y + a_4x/a_3$ we obtain an equation of the above form where the coefficient of x is 0. The coefficient of x^2 must be non-zero, since otherwise $(0,0)$ would be a point of order 3 (check this!). The change of variables $x \mapsto (a_3/a_2)^2x$, $y \mapsto (a_3/a_2)^3y$ now gives an equation of the form

$$y^2 + \alpha xy + \beta y = x^3 + \beta x^2.$$

A computation (for example, using the program PARI) shows that

$$2P = (-\beta, \beta(\alpha - 1)) \quad \text{and} \quad 3P = (1-\alpha, \alpha - \beta - 1).$$

Now suppose that P has order 5. Then $2P = -3P$, so the x-coordinates of $2P$ and $3P$ are the same (by Exercise 1.2.6). Therefore, $\alpha = 1+\beta$, and E is isomorphic to

$$y^2 + (1+\beta)xy + \beta y = x^3 + \beta x^2. \tag{5}$$

The discriminant of the elliptic curve (5) is $-\beta^5(\beta^2+11\beta-1)$. We can view (5) as the equation of a surface over the β-line, where the "bad", i.e., singular, fibers lie over the points $0, \frac{-11\pm5\sqrt{5}}{2}$, and infinity on the projective (β-)line $\mathbf{P}^1$. With $\beta \in \mathbf{Q}-\{0\}$, we obtain the elliptic curves over $\mathbf{Q}$ with a rational point (normalized to be $(0,0)$)

of order 5. If K is a subfield of $\mathbf{C}$, then for $\beta \in K$ with $\beta \notin \{0, \frac{-11\pm5\sqrt{5}}{2}\}$, we obtain the elliptic curves over K with a K-rational point of order 5.

Exercise 2.2.2. *Do the above with* 4 *instead of* 5.

Exercise 2.2.3. *Do the above with* 7 *instead of* 5.

Exercise 2.2.4. *In the above, check that* $(0,0)$ *is a point of order* 5 *on every elliptic curve given by (5).*

We write $Y_1(N)$ for the ("moduli" or "parameter") space of pairs (E,P) where E is an elliptic curve and P is a point of order N on E. (This only works nicely for $N \geq 3$ — think about why this is so! — but it can be fudged for $N = 1, 2$.) Then $Y_1(5)$ is the β-line minus the "bad" points. We write $X_1(N)$ for the compactification of $Y_1(N)$ (so $X_1(5)$ is $\mathbf{P}^1$). Then $X_1(N)$ is a curve defined over $\mathbf{Q}$, and is an example of what is called a modular curve. If K is a subfield of $\mathbf{C}$, then the elements of $Y_1(N)(K)$ correspond to isomorphism classes of pairs (E,P) where E is an elliptic curve over K and $P \in E(K)$ is a point of order N. The genus of $X_1(N)$ tends to grow as N grows.

Fact 2.2.5. The genus of $X_1(N)$ is zero (and $X_1(N)$ is $\mathbf{P}^1$) if and only if either $N \leq 10$ or $N = 12$.

Therefore, if either $1 \leq N \leq 10$ or $N = 12$, then there are infinitely many elliptic curves over $\mathbf{Q}$ with a rational point of order N (we wrote down these elliptic curves when $N = 5$).

B. Levi, and later A. Ogg, conjectured which groups can be torsion subgroups of Mordell-Weil groups of elliptic curves over $\mathbf{Q}$ (see [**131**]). Mazur (Theorem 2.1.4 above) proved that the conjectured set of finite groups was the correct one. Mazur's proof required a deep study of modular curves (see [**96**], [**95**]).

2.3. Conjectures.

Conjecture 2.3.1 (Torsion Conjecture for Abelian Varieties)**.** *If A is an abelian variety of dimension d defined over a number field K, then $\#A(K)_{\mathrm{tors}}$ is bounded above by a constant depending only on d and K.*

Conjecture 2.3.2 (Strong Torsion Conjecture for Abelian Varieties)**.** *If A is an abelian variety of dimension d defined over a number field K of degree m, then $\#A(K)_{\mathrm{tors}}$ is bounded above by a constant depending only on d and m.*

The Strong Torsion Conjecture is sometimes called the Uniform Boundedness Conjecture. In [**29**], Cassels said that the Torsion Conjecture for elliptic curves was "part of the folklore".

Mazur's theorem is the same as the (Strong) Torsion Conjecture for $d = 1$ and $m = 1$.

2.4. Other results for elliptic curves.

We begin by stating the famous result of Faltings:

Theorem 2.4.1 (Faltings [**43**]; formerly the Mordell Conjecture)**.** *If C is a (smooth projective) curve of genus > 1 defined over a number field K, then $C(K)$ is finite.*

Faltings' Theorem (from the 1980's) implies in particular that for N sufficiently large there are only finitely many rational points on $X_1(N)$. By the "modular interpretation" of $X_1(N)$, there are therefore only finitely many elliptic curves over $\mathbf{Q}$ with a rational point of order N (up to isomorphism). Mazur (in the 1970's) proved more, namely that there are actually no rational points on $Y_1(N)$, for $N > 12$ and $N = 11$.

Theorem 2.4.2 (Manin [**88**]). *If K is a number field and p is a prime number, then there exists a constant $N(p, K)$ so that if E is an elliptic curve over K, then the number of torsion points in $E(K)$ whose order is a power of p is at most $p^{N(p,K)}$.*

Therefore to prove the (weak) Torsion Conjecture for elliptic curves, it suffices to bound the primes p that can occur as orders of torsion points. (Note that Manin's $N(p, K)$ depends on the field K, not just its degree.)

Exercise 2.4.3. *Show that Faltings' Theorem implies Manin's Theorem. Hint: Use that there are only finitely many N for which the genus of $X_1(N)$ is ≤ 1. (In fact, what Manin proved is that for all n sufficiently large, $X_0(p^n)(K)$ is finite. Here $X_0(N)$ is (the compactification of) the moduli space of pairs (E, C) where C is a subgroup of order N on the elliptic curve E.)*

Theorem 2.4.4 (Kamienny [**65**], using Kenku-Momose [**71**]). *If E is an elliptic curve defined over a quadratic number field K, then $E(K)_{\text{tors}}$ is isomorphic to one of the following* 26 *groups:*

$$\begin{array}{lll}
\mathbf{Z}/N\mathbf{Z} & \textit{for} & N = 1, \ldots, 16, \textit{ or } 18, \\
\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2N\mathbf{Z} & \textit{for} & N = 1, \ldots, 6, \\
\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3N\mathbf{Z} & \textit{for} & N = 1 \textit{ or } 2, \\
\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}. & &
\end{array}$$

This proves the Strong Torsion Conjecture for $d = 1$ and $m = 2$, i.e., for elliptic curves over quadratic number fields (uniformly). The result was conjectured by Kenku and Momose in [**71**]. Kamienny proved that, for K quadratic, the order of a torsion point in $E(K)$ must divide $2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$, and in [**71**] it had already been determined exactly which groups can then occur. Note that not all of these groups will occur, for a given quadratic number field.

Kamienny and Mazur proved the Strong Torsion Conjecture for $d = 1$ and $m \leq 8$ (see [**66**] and [**67**]), and Abramovich proved it for $d = 1$ and $m \leq 14$ (see [**1**]). Then Merel proved it for $d = 1$ and all m, that is, he settled it for elliptic curves (see [**99**]).

Theorem 2.4.5 (Merel). *If E is an elliptic curve defined over a number field K of degree m, then $\#E(K)_{\text{tors}}$ is bounded above by a constant depending only on d and m. If $m > 1$ and $E(K)$ has a point of prime order p, then $p < m^{3m^2}$.*

Next we state a strengthening of Merel's result, due to Oesterlé.

Theorem 2.4.6 (Oesterlé). *If E is an elliptic curve defined over a number field K of degree m, and $E(K)$ has a point of prime order p, then*

$$p \leq (1 + 3^{\frac{m}{2}})^2.$$

(Note: To get from this to the Strong Torsion Conjecture for Elliptic Curves, one needs to use Faltings' Theorem....)

The next result gives an effective version of the Strong Torsion Conjecture for Elliptic Curves.

Theorem 2.4.7 (Parent [**121**]). *If E is an elliptic curve defined over a number field K of degree m, and $E(K)$ has a point of order p^n where p is a prime number, then*

$$p^n \leq 129(5^m - 1)(3m)^6.$$

Oesterlé's result (for $m = 3$) shows that if E is an elliptic curve over a number field K of degree 3, and $E(K)$ has a point of prime order p, then $p \leq 37$. In a recent preprint Parent has a result which gives us reason to believe that the correct bound is 17 or 13.

Theorem 2.4.8 (Parent preprint [**122**]). *Suppose E is an elliptic curve defined over a number field K of degree 3, suppose $E(K)$ has a point of prime order p, and assume that a certain condition which would follow from the Birch and Swinnerton-Dyer Conjecture holds*[1]. *Then $p \leq 17$, and there are at most 49 elliptic curves "up to isomorphism" having a point of order 17 over a cubic number field.*

Exercise 2.4.9. *Show that there exists an elliptic curve with a point of order 11 over a cubic number field, by showing that the modular curve $X_1(11)$ has infinitely many points defined over cubic number fields. Hint: Use Hilbert's Irreducibility Theorem and the fact that $X_1(11)$ is an elliptic curve — an equation for it is $y^2 + y = x^3 - x^2$.*

2.5. Abelian varieties over number fields.

For abelian varieties of dimension greater than one, there are no number fields for which the Torsion Conjecture is known to hold. However, one can give explicit bounds for torsion for certain families of abelian varieties.

First, let's consider a result that says that the torsion subgroup is "large". Flynn constructed sequences of curves over $\mathbf{Q}$ whose Jacobian varieties have $\mathbf{Q}$-rational torsion points whose orders grow quadratically in the genus of the curve.

Theorem 2.5.1 (Flynn [**44**]). *If g is even, $t \neq 0$, and $0 \leq r \leq g$, then the curves*

$$y^2 + t(x-1)y = \left(\sum_{i=1}^{g-r+1} x^{r+i}\right)^2 - t(x^{g+2} + x^{r+1})$$

have genus g, and their Jacobian varieties have rational torsion points of exact order $g^2 + 3g + 1 - r$. Moreover, there is a sequence $A(n)$ of abelian varieties over $\mathbf{Q}$ of strictly increasing dimension $d(n)$, each containing a $\mathbf{Q}$-rational torsion point of order $N(n)$, such that

$$N(n) > (1.6)^{(d(n)\log d(n))^{2/3}}.$$

The following result (see Theorem 3.3 of [**154**]) follows from results of Serre-Tate on abelian varieties with potentially good reduction. We will give the definitions and proof below.

[1] Namely, that the winding quotient of $J_1(q)$ has zero rank over $\mathbf{Q}$ for all primes q between 17 and 37 inclusive.

Theorem 2.5.2. *If A is a d-dimensional abelian variety defined over a number field K of degree m, and A has everywhere potentially good reduction, then*

$$\begin{aligned}\#A(K)_{\mathrm{tors}} &\leq [(1 + 2^{\#\mathrm{GL}_{2d}(\mathbf{Z}/3\mathbf{Z})m/2})(1 + 3^{\#\mathrm{GL}_{2d}(\mathbf{Z}/4\mathbf{Z})m/2})]^{2d} \\ &< \left(1 + \frac{1}{10^{11}}\right)(2^{3^{4d^2}} \cdot 3^{4^{4d^2}})^{md} < 6^{md \cdot 4^{4d^2}}.\end{aligned}$$

Definition 2.5.3. An abelian variety A over a number field K has *good reduction* at a prime ideal $\mathfrak{p}$ of the ring of integers $\mathcal{O}$ of K if (for some appropriate defining equations for A over $\mathcal{O}$) the reduction of A modulo $\mathfrak{p}$ is an abelian variety (i.e., is non-singular) over the (finite) field $\mathcal{O}/\mathfrak{p}$. (See [**14**] for a more precise discussion of the requirements on the "defining equations" and a detailed study of their existence.) It has *potentially good reduction* at $\mathfrak{p}$ if it has good reduction at all the primes dividing $\mathfrak{p}$ in some finite extension of the field K. It has *everywhere potentially good reduction* if it has potentially good reduction at all primes of K (in which case there will exist a finite extension of K over which A has good reduction at all prime ideals).

Example 2.5.4. The elliptic curve $y^2 = x^3 - x$ has good reduction at all odd prime numbers (this is easy to see directly from the definition), and has everywhere potentially good reduction (this is less easy).

Example 2.5.5. Let E be the elliptic curve

$$y^2 = x^3 - 35x - 98$$

(this is $X_0(49)$). By the change of variables $x \mapsto 4x - 1$, $y \mapsto 8y + 4x$, we have the equation

$$y^2 + xy = x^3 - x^2 - 2x - 1,$$

which has good reduction at all prime numbers except 7 (in fact, the discriminant is -7^3). However, by the change of variables $x \mapsto \sqrt{-7}x$, $y \mapsto (-7)^{3/4}y$ we have the equation

$$y^2 = x^3 + 5x - 2\sqrt{-7}$$

which has good reduction at all prime ideals of the field $\mathbf{Q}(\sqrt[4]{-7})$ (check that the discriminant is -1). Therefore E has everywhere potentially good reduction.

Definition 2.5.6. If E is an elliptic curve of the form $y^2 = x^3 + ax + b$, then its j-invariant is

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

Fact 2.5.7. If $E : y^2 = x^3 + ax + b$ is an elliptic curve with $a, b \in \mathbf{Q}$, then E has everywhere potentially good reduction if and only if $j(E) \in \mathbf{Z}$.

Fact 2.5.8. Elliptic curves with complex multiplication (see §2.7 below) have everywhere potentially good reduction (and have j-invariants which are algebraic integers). More generally, abelian varieties of CM-type have everywhere potentially good reduction (see [**149**] and [**139**]).

Definition 2.5.9. Suppose A is an abelian variety over a number field K, and N is a positive integer. Let $A[N]$ denote the subgroup of points of $A(\mathbf{C})$ of order dividing N. Let K_N (or in more standard notation, $K(A[N])$) denote the smallest field extension of K over which all the points on A of order dividing N are defined. Also, let

$$A(K)[N] = A[N] \cap A(K).$$

Example 2.5.10. For $E : y^2 = x^3 - x$ we have

$$E[2] = \{O, (0,0), (1,0), (-1,0)\} \quad \text{and} \quad \mathbf{Q}(E[2]) = \mathbf{Q}.$$

Example 2.5.11. For $E : y^2 = x^3 - 2x$ we have

$$E[2] = \{O, (0,0), (\sqrt{2},0), (-\sqrt{2},0)\} \quad \text{and} \quad \mathbf{Q}(E[2]) = \mathbf{Q}(\sqrt{2}).$$

Facts 2.5.12. Suppose A is a d-dimensional abelian variety over a number field K. Then

$$A[N] \cong (\mathbf{Z}/N\mathbf{Z})^{2d},$$

the field K_N is a finite Galois extension of K, and the action of $\mathrm{Gal}(K_N/K)$ on $A[N]$ gives a group homomorphism

$$\mathrm{Gal}(K_N/K) \to \mathrm{GL}_{2d}(\mathbf{Z}/N\mathbf{Z}).$$

This homomorphism is injective by the definition of K_N. Therefore,

$$[K_N : K] \leq \#\mathrm{GL}_{2d}(\mathbf{Z}/N\mathbf{Z}) < N^{4d^2}.$$

Fact 2.5.13 (Serre-Tate [**139**])**.** Suppose A is an abelian variety over a number field K, with everywhere potentially good reduction. If $N \geq 3$, then A has good reduction at all the prime ideals of K_N which do not divide N.

Definition 2.5.14. If A is an abelian variety over a number field M, and p is a prime number, let $A(M)_{p'-\mathrm{tors}}$ denote the subgroup of $A(M)_{\mathrm{tors}}$ of points of order prime to p.

Fact 2.5.15. Suppose A is an abelian variety over a number field M, suppose $\mathfrak{p}$ is a prime ideal of the ring of integers $\mathcal{O}$ of M, and suppose p is the characteristic of the field $\mathcal{O}/\mathfrak{p}$ (so $\mathfrak{p}$ divides p). If A has good reduction at $\mathfrak{p}$, then reduction modulo $\mathfrak{p}$ gives an injective homomorphism

$$A(M)_{p'-\mathrm{tors}} \hookrightarrow A(\mathcal{O}/\mathfrak{p}).$$

Fact 2.5.16 (Weil's bound)**.** If A is a d-dimensional abelian variety over the finite field $\mathbf{F}_q$, then

$$\#A(\mathbf{F}_q) \leq (1+\sqrt{q})^{2d}.$$

Proof of Theorem 2.5.2. With notation as in the statement of Theorem 2.5.2, let $\mathcal{O}$ denote the ring of integers of K_3, let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$ dividing 2, and let

$$q = 2^{\#\mathrm{GL}_{2d}(\mathbf{Z}/3\mathbf{Z})m}.$$

Then $\#(\mathcal{O}/\mathfrak{p})$ divides $2^{[K_3:\mathbf{Q}]}$ which divides q. By Fact 2.5.13, A has good reduction at $\mathfrak{p}$. By Facts 2.5.15 and 2.5.16 we have

$$\begin{aligned}\#A(K_3)_{2'-\mathrm{tors}} &\leq \#A(\mathcal{O}/\mathfrak{p}) \leq \#A(\mathbf{F}_q)\\ &\leq (1+\sqrt{q})^{2d} = (1+2^{\#\mathrm{GL}_{2d}(\mathbf{Z}/3\mathbf{Z})m/2})^{2d}.\end{aligned}$$

Similarly,

$$\#A(K_4)_{3'-\mathrm{tors}} \leq (1+3^{\#\mathrm{GL}_{2d}(\mathbf{Z}/4\mathbf{Z})m/2})^{2d}.$$

Since

$$\#A(K)_{\mathrm{tors}} \leq \#A(K_N)_{\mathrm{tors}} \quad \text{for every } N,$$

we have

$$\#A(K)_{\mathrm{tors}} \le \#A(K_3)_{2'-\mathrm{tors}} \#A(K_4)_{3'-\mathrm{tors}}.$$

The rest of the proof is left as an exercise. □

2.6. Abelian varieties over other fields.

As remarked by Cassels, the Torsion Conjecture would be false if the phrase "number field" were replaced by "local field" (Lemma 17.1 and p. 264 of [**29**]).

However, for abelian varieties (with no constant part) over function fields, one expects a Torsion Conjecture to hold. For a non-constant elliptic curve E defined over a function field in one variable K, Theorem 1 of [**83**] gives an explicit upper bound on the order of the torsion subgroup of $E(K)$, depending only on the genus of K. See also Theorem 7.2 of [**62**], which shows that if K has genus g and characteristic zero, then

$$\#E(K)_{\mathrm{tors}} \le 144(g+1)^{2/3}.$$

For surveys on Torsion Conjectures see [**40**] (for elliptic curves) and [**154**].

2.7. Digression on complex multiplication.

If E is an elliptic curve over $\mathbf{C}$, and $m \in \mathbf{Z}$, then the map on $E(\mathbf{C})$ that takes a point P and sends it to mP defines an endomorphism of E. In this way we can view $\mathbf{Z}$ as a subring of $\mathrm{End}(E)$.

Definition 2.7.1. If E is an elliptic curve over $\mathbf{C}$, we say that E has *complex multiplication* or *CM* if E has endomorphisms that are not multiplication by an integer (i.e., if $\mathrm{End}(E) - \mathbf{Z} \neq \emptyset$).

If E has CM, then $\mathrm{End}(E)$ is an order in an imaginary quadratic field K (so that $\mathrm{End}(E) \otimes_{\mathbf{Z}} \mathbf{Q} = K$), and we say that E has *CM by K*. See [**148**] and [**149**] for more about complex multiplication of elliptic curves and abelian varieties.

Example 2.7.2. Consider

$$E : y^2 = x^3 - x.$$

The map $(x,y) \mapsto (-x, iy)$ is an automorphism of E. It is not multiplication by an integer, since it has order 4. Therefore E has complex multiplication.

Example 2.7.3. More generally, consider

$$E : y^2 = x^3 + ax,$$

with a a non-zero integer. As above, the map $(x,y) \mapsto (-x, iy)$ is in $\mathrm{End}(E) - \mathbf{Z}$. Therefore E has complex multiplication (by $\mathbf{Q}(i)$).

Example 2.7.4. Consider

$$E : y^2 = x^3 + b,$$

with b a non-zero integer. The map $(x,y) \mapsto (\omega x, y)$, where ω is a primitive cube root of unity, is an automorphism of E. It is not multiplication by an integer, since it has order 3. Therefore E has complex multiplication (by $\mathbf{Q}(\omega)$).

See [**149**] for the theory of abelian varieties of CM-type. See [**153**], [**154**], [**179**], and [**2**] for bounds on torsion subgroups of Mordell-Weil groups of abelian varieties of CM-type.

CHAPTER 3
Ranks

Even for elliptic curves, the rank is still very mysterious. We will see in this chapter and the next some deep conjectures about the ranks of abelian varieties and elliptic curves.

3.1. Examples.

By the Mordell-Weil Theorem, if A is an abelian variety over a number field K, then

$$A(K) \cong \mathbf{Z}^r \oplus A(K)_{\mathrm{tors}}$$

for some non-negative integer r. We call r the *rank* of A over K.

Example 3.1.1.

$$E : y^2 = x^3 - x$$
$$E(\mathbf{Q}) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, \quad r = 0$$

Example 3.1.2.

$$E : y^2 = x^3 - 5^2 x$$
$$E(\mathbf{Q}) \cong \mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, \quad r = 1$$

The point $(-4, 6)$ has infinite order (this follows from the Nagell-Lutz Theorem, since $6 \neq 0$ and 36 does not divide $4(25)^3$).

Example 3.1.3.

$$E : y^2 = x^3 - (2 \cdot 7 \cdot 11)^2 x$$
$$E(\mathbf{Q}) \cong \mathbf{Z}^2 \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, \quad r = 2$$

The points $(-98, 1176)$ and $(350, 5880)$ are independent points of infinite order. (This can be shown by computing the determinant of the associated Néron-Tate pairing matrix — see §4.6 below — and showing it is non-zero.)

Example 3.1.4 (Kramarz [**76**]).

$$E : y^2 = x^3 - (2 \cdot 3 \cdot 11 \cdot 19)^2 x$$
$$E(\mathbf{Q}) \cong \mathbf{Z}^3 \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, \quad r = 3$$

The points $(-98, 12376)$, $(1650, 43560)$, and $(109554, 36258840)$ are independent points of infinite order.

Example 3.1.5.

$$E : y^2 = x^3 - (2 \cdot 3 \cdot 7 \cdot 17 \cdot 41)^2 x$$
$$E(\mathbf{Q}) \cong \mathbf{Z}^4 \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, \quad r = 4$$

Example 3.1.6 (Rogers [**126**])**.**

$$E : y^2 = x^3 - (2 \cdot 3 \cdot 11 \cdot 17 \cdot 19 \cdot 59 \cdot 163)^2 x$$
$$E(\mathbf{Q}) \cong \mathbf{Z}^5 \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, \quad r = 5$$

Example 3.1.7 (Rogers [**126**])**.**

$$E : y^2 = x^3 - (2 \cdot 3 \cdot 5 \cdot 11 \cdot 19 \cdot 41 \cdot 43 \cdot 67 \cdot 83)^2 x$$
$$E(\mathbf{Q}) \cong \mathbf{Z}^6 \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, \quad r = 6$$

Example 3.1.8. Roland Martin and William McMillen [**92**] of NSA found 24 independent points of infinite order on

$$y^2 + xy + y = x^3 - 120039822036992245303534619191166796374x +$$
$$504224992484910670010801799168082726759443756222911415116.$$

They (and a number of other people who have constructed elliptic curves of large rank) used methods of Mestre [**100**]. They had found earlier [**91**] an elliptic curve over $\mathbf{Q}$ with rank at least 23.

Example 3.1.9. Nagao [**109**] found an infinite family of elliptic curves over $\mathbf{Q}$ of rank at least 13, by finding an elliptic curve over $\mathbf{Q}(t)$ of rank at least 13. Kihara [**72**] found an infinite family of elliptic curves over $\mathbf{Q}$ of rank at least 14, by considering Nagao's $\mathbf{Q}(t)$-curve over the function field of a certain elliptic curve of positive rank.

Example 3.1.10. D. Zagier and G. Kramarz [**188**] considered the curves $x^3+y^3 = d$, i.e., the elliptic curves $y^2 = x^3 - 432d^2$. These are the "cubic twists" of $x^3+y^3 = 1$. They performed numerical calculations for d up to $70{,}000$, and found that 23.3% of the even ranks are at least 2, and 2.2% of the odd ranks are at least 3, with these percentages remaining constant as d grows.

Example 3.1.11. Shioda gives $y^2 = x^3 + t^{360} + 1$ as an example of an elliptic curve over $\mathbf{C}(t)$ of rank 68 (see [**151**] and [**30**]; see also [**168**] and [**150**] for examples with rank 56).

3.2. Unboundedness/boundedness.

The following conjecture is part of the folklore.

Conjecture 3.2.1. *Ranks of elliptic curves over* $\mathbf{Q}$ *are unbounded.*

One reason for believing the conjecture is that the analogous result over a function field in one variable over a finite field $\mathbf{F}_q$ is true:

Theorem 3.2.2 (Tate-Shafarevich [**175**])**.** *Ranks of elliptic curves over* $\mathbf{F}_q(t)$ *are unbounded.*

The examples of Tate-Shafarevich are of quadratic twists. In [**175**] it is stated that Lapin ([**81**], [**82**]) constructed analogous examples over $\mathbf{C}(t)$. However, I have been told that this does not seem to be the case.

3.3. Vary the field.

One can fix the elliptic curve or abelian variety, increase the field, and see how the rank behaves. Such questions are considered, for example, in [**6**], [**112**], [**94**], [**57**], and [**120**]. Honda stated a controversial conjecture:

Conjecture 3.3.1 (Honda [**63**], see also Question 3 on p. 162 of [**137**]). *If A is an abelian variety over a number field L, then there exists a constant C_A, depending only on A, such that for all number fields $K \supseteq L$,*

$$\operatorname{rank}(A(K)) \leq C_A[K : \mathbf{Q}].$$

Honda based his conjecture on the following two theorems he proved about ranks of abelian varieties, and an analogy with the Dirichlet unit theorem.

Theorem 3.3.2 (Honda [**63**], Corollary of Theorem 5). *If A is an abelian variety of dimension d over a number field, then there exists a constant C_A, depending only on A, such that for every prime ℓ and every number field K over which A is defined and such that $A[\ell] \subset A(K)$,*

$$\operatorname{rank}(A(K)) \leq C_A[K : \mathbf{Q}] + 2dh_K(\ell),$$

where $h_K(\ell)$ is the ℓ-rank of the ideal class group of K.

Note that the condition $A[\ell] \subset A(K)$ is equivalent to $K(A[\ell]) = K$, which is equivalent to $A(K)[\ell] \cong (\mathbf{Z}/\ell\mathbf{Z})^{2d}$.

Theorem 3.3.3 (Honda [**63**], Theorem 6). *If A is a simple abelian variety over a number field K, and A is of CM-type with reflex CM-field F, then*

$$\operatorname{rank}(A(KF)) = [KF : K]\operatorname{rank}(A(K)).$$

See [**149**] or [**148**] for the definition of the reflex CM-field. In the case of CM elliptic curves, the reflex CM-field is the same as the imaginary quadratic field by which the curve has complex multiplication.

Honda's Conjecture is not widely believed, and would imply statements that many people believe to be false. For example, it would imply that ranks of elliptic curves are bounded in families of quadratic twists (see Exercise 3.4.7 below). However, in [**133**] Schneiders and Zimmer give data which they say provide numerical evidence for Honda's Conjecture.

3.4. Quadratic twists.

From now until the end of the chapter, unless otherwise stated, E is an elliptic curve over $\mathbf{Q}$.

Definition 3.4.1. If $E : y^2 = x^3 + ax + b$ is an elliptic curve over $\mathbf{Q}$ and $0 \neq D \in \mathbf{Z}$, define the *quadratic twist of E by D* to be the elliptic curve

$$E^{(D)} : Dy^2 = x^3 + ax + b.$$

Exercise 3.4.2. *Check that the map $(x, y) \mapsto (Dx, D^2y)$ is an isomorphism from $E^{(D)}$ onto $y^2 = x^3 + D^2ax + D^3b$.*

Exercise 3.4.3. *Show that if $D_1 = n^2D_2$ with $n \in \mathbf{Q}$, then $E^{(D_1)} \cong E^{(D_2)}$.*

Exercise 3.4.4. *Show that $E^{(D)}$ and E are isomorphic over $\mathbf{Q}(\sqrt{D})$.*

Definition 3.4.5. Let
$$r_E(D) = \operatorname{rank}(E^{(D)}(\mathbf{Q})).$$

Exercise 3.4.6. *Show that*
$$\operatorname{rank}(E(\mathbf{Q})) + r_E(D) = \operatorname{rank}(E(\mathbf{Q}(\sqrt{D}))).$$

Exercise 3.4.7. *Use Exercise 3.4.6 to show that (Honda's) Conjecture 3.3.1 implies that there exists a positive constant C_E depending only on E such that $r_E(D) \leq C_E$ for all D.*

Question 3.4.8. *Are ranks unbounded in (all, some) families of quadratic twists?*

Note that the result of Tate and Shafarevich was for a family of quadratic twists (i.e., they found quadratic twists of an elliptic curve over $\mathbf{F}_q(t)$ of unbounded rank). Honda's Conjecture would be false if number fields were replaced by function fields over finite fields.

Write $\omega(n)$ for the number of prime divisors of n.

Fact 3.4.9. (See Exercise 3.4.12 below.) If $E(\mathbf{Q})[2] \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, then
$$\operatorname{rank}(E(\mathbf{Q})) \leq 2\omega(2\Delta(E))$$
where $\Delta(E)$ is the discriminant of E.

Remark 3.4.10. For some positive constant C,
$$\omega(n) \leq C\frac{\log n}{\log\log n}$$
if $n > 2$. Therefore if $E(\mathbf{Q})[2] \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, then
$$\operatorname{rank}(E(\mathbf{Q})) \leq C\frac{\log|\Delta(E)|}{\log\log|\Delta(E)|}.$$

Exercise 3.4.11. *Use Fact 3.4.9 to show that if $E(\mathbf{Q})[2] \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ and $|D| > 2$, then*
$$r_E(D) \leq 2\omega(2D \cdot \Delta(E)) \leq C_E\frac{\log|D|}{\log\log|D|},$$
where C_E is a constant depending only on E.

Therefore, to get large rank, $|D|$ must be large. The bound
$$r_E(D) \leq C_E\frac{\log|D|}{\log\log|D|} \tag{6}$$
is called the "trivial bound".

For $y^2 = x^3 - x$, compare the bounds given by the first inequality of Exercise 3.4.11 with the examples in §3.1.

Exercise 3.4.12 (Advanced exercise)**.** *Suppose E is an elliptic curve over a number field K, suppose ℓ is a prime number, and suppose $E[\ell] \subset E(K)$. Let M denote the maximal Galois extension of K whose Galois group is an elementary abelian ℓ-group and which is unramified at all primes that do not divide $\ell \cdot \Delta(E)$. Define φ by $\varphi(P)(g) = g(Q) - Q$ for $P \in E(K)$ and $g \in \operatorname{Gal}(\bar{K}/K)$, where Q is a point of $E(\bar{K})$ such that $\ell Q = P$. Show that φ induces a well-defined injective group homomorphism*
$$E(K)/\ell E(K) \hookrightarrow \operatorname{Hom}(\operatorname{Gal}(M/K), E[\ell]).$$
Then let $\ell = 2$ and $K = \mathbf{Q}$ and use Class Field Theory to prove Fact 3.4.9, thereby proving the "trivial bound" (6).

The technique of proof in Exercise 3.4.12 can be generalized to lead to a proof of (Honda's) Theorem 3.3.2. The same technique is also used in proving the Mordell-Weil Theorem. We will see more of this later when we define Tate-Shafarevich groups.

3.5. Average ranks.

The average rank will depend on how we define the average. Let's first consider the average rank in a family of quadratic twists, where we order the curves by $|D|$. Goldfeld conjectured that this average is always $\frac{1}{2}$:

Conjecture 3.5.1 (Goldfeld [**51**]).

$$\lim_{X\to\infty} \frac{\sum_{|D|<X} r_E(D)}{\sum_{|D|<X} 1} = \frac{1}{2}$$

(where the D's in the sums are square-free).

Theorem 3.5.2 (Goldfeld [**51**]). *Assuming the Birch and Swinnerton-Dyer Conjecture, the Modularity Conjecture, and a form of the Riemann Hypothesis, then*

$$\limsup_{X\to\infty} \frac{\sum_{|D|<X} r_E(D)}{\sum_{|D|<X} 1} \leq 3.25$$

(where the D's in the sums are square-free).

In [**17**] Brumer pointed out that Goldfeld's 3.25 can be replaced by 2.5. Brumer tells me that Heath-Brown can prove that it can in fact be replaced by 1.5.

Heath-Brown has determined an upper bound for the average rank of the odd quadratic twists of the curve $y^2 = x^3 - x$:

Theorem 3.5.3 (Heath-Brown [**60**]). *If $E : y^2 = x^3 - x$, then*

$$\limsup_{X\to\infty} \frac{\sum_{D\, odd, |D|<X} r_E(D)}{\sum_{D\, odd, |D|<X} 1} \leq 1.2645\ldots$$

(where the D's are square-free).

Exercise 3.5.4. *Show that every elliptic curve over* $\mathbf{Q}$ *has a unique model of the form*

$$E_{r,s} : y^2 = x^3 + rx + s$$

where r and s are integers with the property that if p^4 divides r then p^6 does not divide s.

Rather than looking at families of twists, Brumer looked at all elliptic curves, ordered by the size of the coefficients for a model as in Exercise 3.5.4.

Theorem 3.5.5 (Brumer [**17**]). *Assuming the Birch and Swinnerton-Dyer Conjecture, the Modularity Conjecture, and the Riemann Hypothesis for L-functions of elliptic curves, then*

$$\limsup_{X\to\infty} \frac{1}{\#\mathcal{C}(X)} \sum_{E\in\mathcal{C}(X)} \operatorname{rank}(E(\mathbf{Q})) \leq 2.3,$$

where

$$\mathcal{C}(X) = \{E_{r,s} : |r| \leq X^{1/3}, |s| \leq X^{1/2}\}.$$

Brumer tells me that Heath-Brown can reduce the 2.3 to 2.

In [**17**] Brumer points out that we can't yet prove unconditionally that the average rank is > 0, or that it is bounded.

Brumer and McGuinness [**19**] did numerical calculations for elliptic curves over $\mathbf{Q}$ of prime conductor up to 10^8, for which the average rank seems to increase slowly to around 1.

Brumer proved the following unconditional result over $\mathbf{F}_q(t)$.

Theorem 3.5.6 (Brumer [**17**])**.** *If q is a power of a prime p, and $p \geq 5$, then the average rank of elliptic curves over $\mathbf{F}_q(t)$ is at most 2.3.*

Brumer tells me that he can now reduce this 2.3 to 2, using methods analogous to those Heath-Brown used to obtain the improvements stated above.

3.6. Distribution of ranks.

The following conjecture is a consequence of the Conjecture of Birch and Swinnerton-Dyer, which we will discuss later.

Conjecture 3.6.1 (Weak Parity Conjecture)**.** *For square-free D, the density of D with $r_E(D)$ even is $1/2$.*

Note that the Weak Parity Conjecture implies that the average rank in a family of quadratic twists is at least $1/2$. We will state a stronger Parity Conjecture later, when we discuss the Conjecture of Birch and Swinnerton-Dyer. Most experts believe the Parity Conjecture, since most believe the Conjecture of Birch and Swinnerton-Dyer. Many (but fewer) also believe the following conjecture.

Conjecture 3.6.2 (Density Conjecture)**.** *For square-free D, the density of D with $r_E(D) = 0$ (respectively $= 1$, respectively ≥ 2) is $1/2$ (respectively $1/2$, respectively 0).*

Exercise 3.6.3. *Show that the Weak Parity Conjecture and Goldfeld's Conjecture together imply the Density Conjecture.*

Katz and Sarnak ([**68**], [**69**]) have a philosophy for why the Density Conjecture should be true.

Theorem 3.6.4 (Heath-Brown [**60**])**.** *If $E : y^2 = x^3 - x$, then*

(i) *the density of odd D with $r_E(D) = 0$ is greater than zero, and*

(ii)

$$\limsup_{X\to\infty} \frac{\#\{\text{ odd } D : |D| \leq X, r_E(D) \geq R\}}{\#\{\text{ odd } D : |D| \leq X\}} \leq (1.7313\ldots)2^{-(R^2-R)/2}$$

(where the D's are always square-free).

Part (ii) of Heath-Brown's Theorem implies that the density of odd square-free D with $r_E(D) \geq 2$ is at most .866, the density with $r_E(D) \geq 3$ is at most .213, etc.

Theorem 3.6.5 (Ono-Skinner [**119**])**.** *If E is a (modular) elliptic curve over $\mathbf{Q}$, then*

$$\#\{\text{ square-free } D : |D| \leq X, r_E(D) = 0\} \geq C_E \frac{X}{\log X}.$$

This result does not give a positive density with rank 0 the way Heath-Brown's result did, but it holds for all (modular) elliptic curves over $\mathbf{Q}$.

In Definition 4.3.1 below we will define the analytic rank, which conjecturally is equal to the rank. There are many results in the literature about analytic ranks. For average and density results for analytic ranks in the family of cubic twists $x^3 + y^3 = d$, see [**85**] and [**86**].

Example 3.6.6 (Silverman [**159**])**.** Let E be the elliptic curve $y^2 = x^3 - x$, and for $0 \neq d \in \mathbf{Q}(i)$ let $E^{(d)}$ be the elliptic curve $dy^2 = x^3 - x$. Then $\operatorname{rank}(E^{(d)}(\mathbf{Q}(i)))$ is even (since $\operatorname{End}(E^{(d)}) = \mathbf{Z}[i]$, so $E^{(d)}(\mathbf{Q}(i))$ is a $\mathbf{Z}[i]$-module). Viewing $ty^2 = x^3 - x$ as an elliptic curve over the function field $\mathbf{C}(t)$, it has rank 0 (a Mordell-Weil Theorem holds here). Under the general philosophy that ranks are "no bigger than they have to be", one expects that for $d \in \mathbf{Q}(i)$, the rank of $E^{(d)}(\mathbf{Q}(i))$ is 0 for d in a set of density 1.

Theorem 3.6.7 (Gouvêa-Mazur [**53**])**.** *If E is an elliptic curve over $\mathbf{Q}$, and the Parity Conjecture holds, then for every $\varepsilon > 0$ there exists a constant $C_{E,\varepsilon} > 0$ such that for every $X > C_{E,\varepsilon}$,*

$$\#\{\textit{square-free } D : |D| \leq X, r_E(D) \geq 2, \textit{ and } r_E(D) \textit{ is even}\} \geq X^{1/2-\varepsilon}.$$

Here is a quick sketch of what Gouvêa and Mazur did. Suppose E is given by the equation $y^2 = x^3 + ax + b$ with $a, b \in \mathbf{Z}$. If n is a non-zero rational number, write $s(n)$ for the square-free part of n, i.e., the unique integer s such that $n = sy^2$ for some $y \in \mathbf{Q}$ (check that this is well-defined). Take a rational number x and compute $x^3 + ax + b$. If it is non-zero, then write $x^3 + ax + b$ as Dy^2 where D is the square-free part and $y \in \mathbf{Q}$. Then (x, y) is a point in $E^{(D)}(\mathbf{Q})$. (For example, if E is $y^2 = x^3 - x$, and $x = 2$, then $D = 6$ and $y = 1$.) For all but finitely many $x \in \mathbf{Q}$, (x, y) is a point of infinite order. This gives a way of (usually) obtaining D's so that $r_E(D) \geq 1$. To deal with integers rather than rational numbers, write x as a fraction in lowest terms, u/v. Then

$$Dy^2 = \left(\frac{u}{v}\right)^3 + a\left(\frac{u}{v}\right) + b.$$

Therefore, $D(yv^2)^2 = u^3v + auv^3 + bv^4$. Let

$$F(u, v) = u^3v + auv^3 + bv^4.$$

Then $D = s(F(u, v))$. Proving Theorem 3.6.7 basically reduces to finding a (sufficiently good) lower bound for

$$\#\{D \in \mathbf{Z} : |D| \leq X, r_E(D) \text{ is even, } D = s(F(u, v)) \text{ for some } u, v \in \mathbf{Z}\}.$$

The Parity Conjecture gives a criterion for when $r_E(D)$ is even. Gouvêa and Mazur show that a positive proportion of $F(u, v)$'s are square-free (this is the hardest part of their proof). If $|u|, |v| \leq X^{1/4}$, then $|F(u, v)| \leq C_E X$. Further, they show that

$$\#\{F(u, v) : |u|, |v| \leq X^{1/4}\} \geq C'_{E,\delta} X^{1/2-\delta}$$

for every $\delta > 0$.

Theorem 3.6.8 (Stewart-Top [**166**])**.** *If $E : y^2 = x^3 + ax + b$ with $a, b \in \mathbf{Q}$ and $ab \neq 0$, then there exist positive constants C_0 and C_1 such that for every $X > C_0$,*

$$\#\{\textit{square-free } D : |D| \leq X, r_E(D) \geq 2\} \geq C_1 \frac{X^{1/7}}{(\log X)^2}.$$

The result of Stewart and Top has a weaker conclusion than that of the theorem of Gouvêa and Mazur, but does not rely on the Parity Conjecture.

Karl Rubin and I [**130**] modified the idea of Gouvêa and Mazur, where instead of counting how many D's occur as square-free parts of $F(u,v)$'s, we count how often each D occurs as the square-free part of an $F(u,v)$. The D's that occur more often tend to correspond to higher rank curves. Using our method, Nick Rogers [**126**] carried out computations which led to the rank 5 and 6 curves in Examples 3.1.6 and 3.1.7.

CHAPTER 4
Conjectures of Birch and Swinnerton-Dyer

Birch and Swinnerton-Dyer based their conjectures ([**10**], [**11**], see also [**7**] and [**25**]) on extensive numerical evidence obtained from computer calculations they did in the 1950's and 1960's. As Birch recalls, "Back in the late 1950's there was a lot of excitement about Tamagawa's work on Siegel's formulae". Birch and Swinnerton-Dyer were trying to generalize Siegel's results on quadratic forms to the setting of elliptic curves, and wanted to understand the analogue of the Tamagawa numbers. Their conjectures remain among the major unsolved problems in number theory. The original conjectures were made for elliptic curves over $\mathbf{Q}$. They have been generalized by Tate (to abelian varieties over global fields) and others. See in particular the conjectures of Beilinson ([**124**], [**111**]) and Bloch-Kato [**12**].

4.1. The L-function of an elliptic curve.

Let E be an elliptic curve over $\mathbf{Q}$.

Let N_E denote the conductor of E (defined in Joe Buhler's lectures). Then N_E divides $\Delta(E)$. Further, if p is a prime, then p divides N_E if and only if E has bad reduction at p.

There exists a generalized Weierstrass equation for E with coefficients in $\mathbf{Z}$ for which $|\Delta(E)|$ is minimal. Call this a *minimal Weierstrass equation* for E. In this chapter from now on we will only consider minimal Weierstrass equations. Then p divides N_E if and only if p divides $\Delta(E)$. Given an elliptic curve over $\mathbf{Q}$, the computer program PARI will tell you how to get a minimal Weierstrass equation for it.

If p is a prime, let

$$a_p = p + 1 - \#E(\mathbf{F}_p).$$

Exercise 4.1.1. *Show that if p divides $\Delta(E)$, then*

$$a_p = \begin{cases} 0 & \text{if } E \text{ has additive reduction at } p, \\ 1 & \text{if } E \text{ has split multiplicative reduction at } p, \\ -1 & \text{if } E \text{ has non-split multiplicative reduction at } p. \end{cases}$$

*(See [**156**] for definitions of additive, split multiplicative, and non-split multiplicative reduction.)*

Example 4.1.2. The equation $E : y^2 = x^3 - x$ is a minimal Weierstrass equation. Here, $\Delta(E) = 2^6$ and $N_E = 2^5$. The point $(1, 0)$ is the singular point on the reduction of E modulo 2. We have (see §2 of [**11**])

$$a_p = \begin{cases} 0 & \text{if } p \equiv 3 \pmod 4 \text{ or } p = 2, \\ 2\alpha & \text{if } p \equiv 1 \pmod 4, \end{cases}$$

where $p = \alpha^2 + \beta^2$ with $\alpha, \beta \in \mathbf{Z}$, normalized so that β is even and 4 divides $\alpha - 1 - \beta$.

Let

$$L(E,s) = \prod_{p \nmid \Delta(E)} \frac{1}{1 - \frac{a_p}{p^s} + \frac{p}{p^{2s}}} \prod_{p \mid \Delta(E)} \frac{1}{1 - \frac{a_p}{p^s}}. \tag{7}$$

The function $L(E, s)$ is called the *Hasse-Weil L-function* for E.

The next result is a special case of Weil's bound (see Fact 2.5.16 above).

Theorem 4.1.3 (Hasse).

$$|a_p| < 2\sqrt{p}.$$

Corollary 4.1.4 (Exercise). *For* $\mathbf{Re}(s) > 3/2$, *the Euler product (7) defining* $L(E, s)$ *converges absolutely.*

Multiplying out the Euler product, we have the Dirichlet series

$$L(E,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

which converges absolutely for $\mathbf{Re}(s) > 3/2$, and defines the a_n's for composite n.

Definition 4.1.5. Suppose A and A' are abelian varieties over a number field K. We say that A *is isogenous to* A' *over* K if there exists a surjective homomorphism $A \to A'$ over K with finite kernel.

Two elliptic curves E and E' are isogenous over K if and only if there exists a non-zero homomorphism $E \to E'$ over K.

Exercise 4.1.6. *Show that if* E *and* E' *are elliptic curves over* $\mathbf{Q}$ *which are isogenous over* $\mathbf{Q}$, *then*

$$\operatorname{rank}(E(\mathbf{Q})) = \operatorname{rank}(E'(\mathbf{Q})) \text{ and } L(E,s) = L(E',s).$$

In other words, the rank and L-function are both isogeny invariants.

Theorem 4.1.7 (Faltings [**43**]). *If* E *and* E' *are elliptic curves over* $\mathbf{Q}$ *and* $L(E, s) = L(E', s)$, *then* E *and* E' *are isogenous over* $\mathbf{Q}$.

Remark 4.1.8. Faltings proved more generally that if two abelian varieties over a number field have isomorphic ℓ-adic representations for some prime ℓ, then they are isogenous. This result was formerly known as Tate's Isogeny Conjecture.

Warning 4.1.9. Tate's Isogeny Conjecture is sometimes incorrectly stated in the literature as saying that two abelian varieties over a number field K are isogenous over K if and only if their L-functions over K are equal. However, this statement is false even for elliptic curves, i.e., Theorem 4.1.7 above is *false* if $\mathbf{Q}$ is replaced by an arbitrary number field (see Remark 3.4 of [**155**] for a counterexample over $\mathbf{Q}(i)$).

4.2. Modularity.

Definition 4.2.2 below is the quickest definition of modularity that I know.

Let $\mathbf{H}$ denote the complex upper half plane, and let

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) : N \text{ divides } c \right\}.$$

Exercise 4.2.1. *Show that if $z \in \mathbf{H}$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$, then $\frac{az+b}{cz+d} \in \mathbf{H}$.*

It follows that the group $\Gamma_0(N)$ acts on $\mathbf{H}$ by linear fractional transformations. For $N \geq 3$, let $Y_0(N)$ denote the moduli space of pairs (E, C) where E is an elliptic curve and C is a cyclic subgroup of E of order N. Then $Y_0(N)(\mathbf{C}) \cong \mathbf{H}/\Gamma_0(N)$. The compactification $X_0(N)$ of $Y_0(N)$ is an algebraic curve over $\mathbf{Q}$. We have

$$X_0(N)(\mathbf{C}) \cong \mathbf{H}/\Gamma_0(N) \cup (\mathbf{Q} \cup i\infty)/\Gamma_0(N),$$

and $X_0(N)(\mathbf{C})$ can be viewed as a compact Riemann surface. The elements of the finite set $(\mathbf{Q} \cup i\infty)/\Gamma_0(N)$ are called the cusps of the modular curve $X_0(N)$.

Definition 4.2.2. If E is an elliptic curve over $\mathbf{Q}$, we say that E is *modular* if there is a non-constant analytic map of Riemann surfaces $X_0(N)(\mathbf{C}) \to E(\mathbf{C})$ for some N.

Example 4.2.3. If E is the elliptic curve $y^2 = x^3 - x$, then there is a non-constant analytic map $X_0(32)(\mathbf{C}) \to E(\mathbf{C})$.

The following result of Shimura (which he proved much more generally, in the setting of abelian varieties; see Chapter 7, especially Proposition 7.19, of [**148**], and [**144**], especially Theorem 1 and Proposition 1) was a groundbreaking result that led to much work on modularity.

Theorem 4.2.4 (Shimura)**.**

(i) *If f is a normalized Hecke eigenform of weight 2 for $\Gamma_0(N)$ with rational Fourier coefficients, then there is an elliptic curve E_f over $\mathbf{Q}$ such that:*
   (a) *there is a non-constant morphism $X_0(N) \to E_f$ defined over $\mathbf{Q}$, and*
   (b) *$L(E_f, s) = L(f, s)$ up to finitely many Euler factors.*

(ii) *If E is an elliptic curve over $\mathbf{Q}$, and for some N there is a non-constant morphism $X_0(N) \to E$ defined over $\mathbf{Q}$, then there is an f as in (i) such that E is isogenous to E_f over $\mathbf{Q}$ (and thus $L(E, s) = L(E_f, s)$).*

(For definitions of modular forms, Hecke eigenforms, etc., see [**148**].) Building on Shimura's work, Carayol (Corollaire on p. 411 of [**24**]) proved:

Theorem 4.2.5 (Carayol)**.** *Under the hypotheses in Theorem 4.2.4(i), if f is a newform, then $L(E_f, s) = L(f, s)$ and $N = N_{E_f}$ (where N_{E_f} is the conductor of E_f).*

Exercise 4.2.6. *Use Theorems 4.2.4 and 4.2.5 (along with Faltings' result, Theorem 4.1.7 above) to deduce Theorem 4.2.7 below (see the appendix to [**97**] for the implication (a) $\Rightarrow$ (b)).*

Theorem 4.2.7. *If E is an elliptic curve over $\mathbf{Q}$, then the following statements are equivalent:*

(a) *E is modular in the sense of Definition 4.2.2;*

(b) *there is a non-constant morphism* $X_0(N) \to E$ *defined over* $\mathbf{Q}$, *for some* N;
(c) *for some* N, $g(z) := \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$ *satisfies*

$$g(\gamma(z)) = (cz+d)^2 g(z)$$

for every $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$;
(d) *for some* N, *there exists a weight two cusp form* f *for* $\Gamma_0(N)$ *such that* $L(E,s) = L(f,s)$ *(if so, then* f *will be a normalized eigenform, and* $f = g$*)*;
(e) *there exists a normalized Hecke eigenform* f *of weight* 2 *for* $\Gamma_0(N)$ *with rational Fourier coefficients such that* E *is isogenous over* $\mathbf{Q}$ *to* E_f;
(f) *the same as any of the above, with* $N = N_E$, *the conductor of* E.

If E is a CM elliptic curve over $\mathbf{Q}$, then E is modular (see [**143**] for the proof, as well as references to relevant papers of Hecke and Deuring).

Taniyama [**147**] conjectured that every elliptic curve is "automorphic", and Shimura conjectured that every elliptic curve over $\mathbf{Q}$ is modular. Breuil, Conrad, Diamond, and Taylor have recently announced that they can complete the work of Wiles to prove Shimura's Modularity Conjecture. (See [**186**] and [**176**] for the work of Wiles and Taylor-Wiles.)

Theorem 4.2.8 (Breuil-Conrad-Diamond-Taylor-Wiles)**.** *Every elliptic curve over* $\mathbf{Q}$ *is modular*[1].

This result implies the following long-standing conjecture of Hasse and Weil (see [**184**] and the Commentary to [1952d] in [**185**]), which had been proved earlier when E is modular (see [**144**] and [**148**]; see also [**41**] and [**141**]).

Theorem 4.2.9. *If* E *is an elliptic curve over* $\mathbf{Q}$, *then* $L(E,s)$ *has an analytic continuation to the complex plane* $\mathbf{C}$, *and has a functional equation:*

$$\Lambda(E,s) = w_E \Lambda(E, 2-s) \tag{8}$$

with $w_E \in \{\pm 1\}$ *and with*

$$\Lambda(E,s) = N_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s).$$

See §2.2 of [**108**] and Theorem 4.1 of [**31**] for the following result of Chandrasekharan and Narasimhan.

Theorem 4.2.10. *If Theorem 4.2.9 holds for* E, *then* $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ *converges (conditionally) to* $L(E,s)$ *for* $\mathbf{Re}(s) > 5/6$.

4.3. BSD I.

If Theorem 4.2.9 holds for E, then taking the Taylor expansion of $L(E,s)$ around $s = 1$ gives

$$L(E,s) = \sum_{i=r}^{\infty} b_i(s-1)^i = b_r(s-1)^r + b_{r+1}(s-1)^{r+1} + \dots \tag{9}$$

for some non-negative integer r, with $b_i \in \mathbf{C}$ and with $b_r \neq 0$.

Definition 4.3.1. This r is called the *analytic rank* of E (over $\mathbf{Q}$).

[1] Since this result is so new, when a result in this text relies on Theorem 4.2.8 or 4.2.9, this dependence is explicitly stated.

We have

$$r = \mathrm{ord}_{s=1} L(E,s).$$

Note that

$$b_r = \lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \frac{L^{(r)}(E,1)}{r!},$$

where $L^{(r)}$ is the r-th derivative of L.

Exercise 4.3.2. *Show that all $b_i \in \mathbf{R}$.*

Birch and Swinnerton-Dyer made the following conjecture (see [**11**]).

Conjecture of BSD I. *If E is an elliptic curve over $\mathbf{Q}$, then*

$$\textit{rank} \;=\; \textit{analytic rank}.$$

A heuristic justification for this conjecture goes as follows. At $s = 1$, the Euler product for $L(E,s)$ is

$$\prod_{p\nmid\Delta(E)} \frac{p}{\#E(\mathbf{F}_p)} \prod_{p\mid\Delta(E)} \left(1 - \frac{a_p}{p}\right)^{-1},$$

where the second (finite) product is a non-zero number. Therefore, $L(E,s)$ should have a high order zero at $s = 1$ if and only if E has "many" points modulo primes, and the latter should be true if and only if E has "many" rational points.

Exercise 4.3.3. *Use the functional equation (8) to show that*

$$w_E = (-1)^r$$

where w_E is the "root number" defined in Theorem 4.2.9 and r is the analytic rank.

It follows that BSD I implies:

Parity Conjecture. *If E is an elliptic curve over $\mathbf{Q}$, then*

$$w_E = (-1)^{\mathrm{rank}(E(\mathbf{Q}))},$$

i.e., $\mathrm{rank}(E(\mathbf{Q}))$ *is even if $w_E = 1$ and is odd if $w_E = -1$.*

Suppose D is a square-free integer. Let ψ_D denote the Dirichlet character associated to $\mathbf{Q}(\sqrt{D})$. Define the conductor

$$N_{\psi_D} = \begin{cases} D & \text{if } D \equiv 1 \pmod 4, \\ 4D & \text{if } D \equiv 2,3 \pmod 4. \end{cases}$$

If $(N_E, N_{\psi_D}) = 1$, then

$$w_{E^{(D)}} = \psi_D(-N_E) w_E. \tag{10}$$

Example 4.3.4. Suppose E is the elliptic curve $y^2 = x^3 - x$. Fermat showed that the rank (over $\mathbf{Q}$) is 0. Since E has complex multiplication, $L(E,s)$ is entire. Using that $L(E,s) = L(f_E, s)$ for an appropriate modular form f_E, one can compute that $L(E,1)$ is approximately $0.655514\ldots \neq 0$. Therefore, the analytic rank $r = 0$, and thus $w_E = 1$ and BSD I holds for this E. Further,

$$w_{E^{(D)}} = \begin{cases} 1 & \text{if } |D| \equiv 1,2,3 \pmod 8, \\ -1 & \text{if } |D| \equiv 5,6,7 \pmod 8. \end{cases} \tag{11}$$

Exercise 4.3.5. *Use (10) to show that (11) holds when D is odd.*

4.4. The Congruent Number Problem.

Definition 4.4.1. A *congruent number* is a positive integer D which is the area of a right triangle with three rational sides.

For example, 6 is a congruent number since the 3–4–5 right triangle has area 6.

The Congruent Number Problem is the problem of determining which positive integers are congruent numbers.

Throughout this section, let E be the elliptic curve $y^2 = x^3 - x$. Then $E^{(D)}$ is the curve $y^2 = x^3 - D^2x$.

Fact 4.4.2 (see [**73**]). A positive integer D is a congruent number if and only if $r_E(D) \geq 1$.

If D is a square-free positive integer, then the Parity Conjecture (or BSD I for all the curves $E^{(D)}$) would imply that $D \equiv 5, 6, 7 \pmod 8$ if and only if $r_E(D)$ is odd. If $r_E(D)$ is odd, then in particular it is non-zero, and therefore D is a congruent number. In any case, if one knew BSD I and computed $L(E^{(D)}, 1)$, then one would know whether D is a congruent number. Thus, the Conjecture of Birch and Swinnerton-Dyer would give an algorithm for answering the Congruent Number Problem, a classical problem in number theory. Writing p_i for primes congruent to $i \pmod 8$, then $1 = r_E(p_5) = r_E(p_7) = r_E(2p_3) = r_E(2p_7)$ (see [**105**], [**61**], [**8**], [**9**]). In particular, if p is a prime and $p \equiv 5$ or $7 \pmod 8$, then p is a congruent number. For more on the Congruent Number Problem, see [**73**], [**177**], and [**135**].

4.5. Evidence for BSD I.

What is known in the direction of BSD I? There is extensive numerical evidence (see especially [**11**] and [**164**]). There is also theoretical evidence. We give below some of the more recent results.

Theorem 4.5.1 (Kolyvagin, et al.). *If E is a (modular) elliptic curve over $\mathbf{Q}$ with analytic rank* 0*, then* $\operatorname{rank}(E(\mathbf{Q})) = 0$.

The result was proved in the case of complex multiplication by Coates-Wiles [**32**]. When E is modular, the result follows from work of Kolyvagin [**74**], combined with the work of Gross-Zagier [**56**] and an analytic number theory result proved independently by Bump-Friedberg-Hoffstein [**21**] and Murty-Murty [**107**].

Theorem 4.5.2 (Gross-Zagier, Kolyvagin, et al.). *If E is a (modular) elliptic curve over $\mathbf{Q}$ with analytic rank* 1*, then* $\operatorname{rank}(E(\mathbf{Q})) = 1$.

Gross and Zagier [**56**] showed that if E is modular, and the analytic rank is 1, then $\operatorname{rank}(E(\mathbf{Q})) \geq 1$. Rubin [**128**] showed that if E has complex multiplication, and the analytic rank is 1, then $\operatorname{rank}(E(\mathbf{Q})) \leq 1$. Work of Kolyvagin [**74**] (when combined with work of Waldspurger [**182**]) shows that if E is modular, and the analytic rank is 1, then $\operatorname{rank}(E(\mathbf{Q})) \leq 1$.

More precisely, suppose that E is a modular elliptic curve over $\mathbf{Q}$. Let $K = \mathbf{Q}(\sqrt{D})$ be an imaginary quadratic field with the property that every prime of bad reduction for E splits into two distinct prime ideals for K.

Exercise 4.5.3. *Use (10) to show that this condition on K implies that $w_{E^{(D)}} = -w_E$.*

The concept of L-function can be defined more generally for elliptic curves (or abelian varieties) over number fields other than $\mathbf{Q}$. In particular, the L-function of E over K satisfies

$$L(E/K, s) = L(E, s)L(E^{(D)}, s)$$

where the L-functions on the right side are the L-functions for E and $E^{(D)}$ over $\mathbf{Q}$ as defined above (this is true for any quadratic number field $K = \mathbf{Q}(\sqrt{D})$, not just those as above). Gross and Zagier [**56**] showed that there is a point $P_K \in E(K)$ (closely related to the Heegner point on E corresponding to K), lying in $E(\mathbf{Q})$ when $w_E = -1$ and lying in $E^{(D)}(\mathbf{Q})$ when $w_E = 1$, with the property that P_K has infinite order if and only if $L'(E/K, 1) \neq 0$. Waldspurger [**182**] showed that if $w_E = -1$, then there exists a field K as above with $L(E^{(D)}, 1) \neq 0$. Bump-Friedberg-Hoffstein [**21**] and Murty-Murty [**107**] showed that if $w_E = 1$, then there exists a field K as above with $L'(E^{(D)}, 1) \neq 0$. Kolyvagin [**74**], [**75**] showed that if P_K has infinite order, then $\operatorname{rank}(E(K)) = 1$.

Exercise 4.5.4. *Use Exercise 3.4.6 above to deduce Theorems 4.5.1 and 4.5.2 from the above information.*

4.6. BSD II.

For the remainder of this chapter, E is an elliptic curve over $\mathbf{Q}$. Assuming BSD I, then Birch and Swinnerton-Dyer made the following conjecture (the new terms are defined below; note that they assumed the "folklore conjecture" that the group Ш is finite).

Conjecture of BSD II.

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \frac{\Omega R \# \text{Ш} \prod_{p|\Delta(E)} c_p}{\#(E(\mathbf{Q})_{\text{tors}})^2}.$$

Note that the left side is just b_r defined in (9).

John Tate (p. 198 of [**174**]) wrote "This remarkable conjecture relates the behavior of a function L at a point where it is not at present known to be defined to the order of a group Ш which is not known to be finite!" Thanks to Theorem 4.2.9, $L(E, s)$ is now known to be defined at $s = 1$.

Tate generalized the conjecture to abelian varieties over global fields [**173**].

Definition 4.6.1. Let

$$\Omega = \int_{E(\mathbf{R})} \frac{dx}{|2y + a_1x + a_3|} \in \mathbf{R},$$

where a_1 and a_3 are coefficients of a generalized Weierstrass model for E as in (2) in Chapter 1.

Like b_r, Ω is transcendental. The expression $\frac{dx}{2y+a_1x+a_3}$ is a holomorphic differential on E, and is invariant (under translation on E). All others are multiples of this one.

Tate found that the "fudge factors" c_p of Birch and Swinnerton-Dyer were the same as the following:

Definition 4.6.2. Let

$$c_p = \#(E(\mathbf{Q}_p)/E_0(\mathbf{Q}_p))$$

where $\mathbf{Q}_p$ is the field of p-adic numbers, and

$$E_0(\mathbf{Q}_p) = \{P \in E(\mathbf{Q}_p) : P \text{ reduces to a non-singular point on the reduction of } E \bmod p\}.$$

Note that $c_p = 1$ if E has good reduction at p.

Exercise 4.6.3. *Show that $E_0(\mathbf{Q}_p)$ is a subgroup of $E(\mathbf{Q}_p)$.*

Theorem 4.6.4 (Theorem 3 of [**183**]). *There exists an absolute constant κ such that if E is an elliptic curve over $\mathbf{Q}$, then*

$$\prod_{p \mid \Delta(E)} c_p < \Delta(E)^{\kappa / \log\log \Delta(E)}.$$

Next we define a height function on $E(\mathbf{Q})$, in order to define the regulator R. For $P = (x, y) \in E(\mathbf{Q})$, write $x = \frac{u}{v}$ with $u, v \in \mathbf{Z}$ in lowest terms, and define the *naive height*

$$h(P) = \log \max(|u|, |v|).$$

Define the *height*

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

(and define $\hat{h}(O) = 0$). (For the existence of the limit, see for example Proposition 9.1 in Chapter VIII of [**156**].) Note that $\hat{h}$ is a function from $E(\mathbf{Q})$ to the set of non-negative real numbers, and $\hat{h}(P) = 0$ if and only if P is a point of finite order. Further, for $m \in \mathbf{Z}$,

$$\hat{h}(mP) = m^2 \hat{h}(P).$$

Other properties of $\hat{h}$ were given in Joe Buhler's lectures (see also §9 in Chapter VIII of [**156**]). Define the *Néron-Tate pairing*, a bilinear form on $E(\mathbf{Q})$, by

$$< P, Q > = \hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q).$$

Let $\{P_1, \dots, P_r\}$ be a $\mathbf{Z}$-basis for $E(\mathbf{Q})/E(\mathbf{Q})_{\mathrm{tors}}$.

Definition 4.6.5. Define the *regulator*

$$R = \det(< P_i, P_j >)_{1 \le i \le r, 1 \le j \le r}$$

if the rank $r \ge 1$, and let $R = 1$ if $r = 0$.

Note that $R = 2\hat{h}(P_1)$ if $r = 1$.

Exercise 4.6.6. *Show that R is independent of the choice of basis $\{P_1, \dots, P_r\}$.*

Warning 4.6.7. Be careful to use correct definitions for the "period" Ω and the height $\hat{h}$. They can be normalized differently, and this can lead to confusion. BSD II is sometimes misstated in the literature, due to incompatible normalizations of the period and height. A good rule to follow is to use the papers of Tate [**173**], [**174**], especially for BSD II for abelian varieties over number fields or, more generally, global fields.

If v is a prime number p (respectively, is ∞), then write $\mathbf{Q}_v$ for $\mathbf{Q}_p$ (respectively, $\mathbf{R}$), and write $\bar{\mathbf{Q}}_v$ for $\bar{\mathbf{Q}}_p$ (respectively, $\mathbf{C}$).

Definition 4.6.8. Define the *Tate-Shafarevich group*

$$Ш = Ш(E/\mathbf{Q}) = \ker \left[H^1(\mathbf{Q}, E(\bar{\mathbf{Q}})) \to \prod_v H^1(\mathbf{Q}_v, E(\bar{\mathbf{Q}}_v)) \right]$$

where $H^1(K, E(\bar{K})) = H^1(\mathrm{Gal}(\bar{K}/K), E(\bar{K}))$, and where the map is induced from the inclusions $\mathrm{Gal}(\bar{\mathbf{Q}}_v/\mathbf{Q}_v) \hookrightarrow \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$.

The group Ш consists of the global cohomology classes which are locally trivial everywhere.

BSD II assumes:

Conjecture 4.6.9 (see pp. 239–240 of [**25**])**.** Ш *is finite.*

Theorem 4.6.10 (Cassels [**26**])**.** *If* Ш *is finite, then* #Ш *is a square.*

The Tate-Shafarevich group Ш for an abelian variety can be defined similarly.

Theorem 4.6.11 (Tate, [**173**])**.** *For principally polarized abelian varieties, if* Ш *is finite, then* #Ш *is a square or twice a square.*

In [**123**] Poonen and Stoll constructed interesting examples, including an example of a principally polarized abelian surface over $\mathbf{Q}$ where $\#Ш = 2$.

Note that Tate-Shafarevich groups for abelian varieties over function fields can be infinite (see [**118**], [**140**]).

4.7. Evidence for BSD II.

The first examples of elliptic curves for which Ш could be proved to be finite were obtained by Rubin [**128**].

If Ш is finite, then both sides of the equation in BSD II are isogeny invariant (although the individual factors on the right side are not). Cassels [**28**] showed this for elliptic curves over number fields, and Tate [**173**] showed it for abelian varieties over global fields, if the degree of the isogeny is relatively prime to the characteristic of the field.

For the function field case, Tate wrote (p. 199 of [**174**]): "The situation is encouraging." He proved that for abelian varieties over a function field over a finite field of characteristic p, the rank is bounded above by the analytic rank. Further, in the same setting, he showed that the prime-to-p part of Ш is finite if and only if the rank equals the analytic rank (i.e., if and only if BSD I holds), and that BSD I holds if and only if BSD II holds up to a power of p. Milne [**103**] (see also [**102**], [**104**], [**3**], [**132**], and [**5**] for related results) showed that in fact everything is also OK at p, if p is odd.

We return to the case of elliptic curves over $\mathbf{Q}$.

Theorem 4.7.1.

$$\frac{L(E,1)}{\Omega} \in \mathbf{Q}$$

and the denominator of this rational number can be effectively bounded.

For the family $y^2 = x^3 - Dx$ this was proved by Birch and Swinnerton-Dyer [**11**]. See [**37**] for the general CM case. In the modular case it follows from work of Shimura [**142**], [**145**], [**146**] and Manin [**89**], [**90**] (by writing the expression in terms of modular symbols that live in rational homology).

Theorem 4.7.2. *If the analytic rank is* 1*, then* $E(\mathbf{Q})$ *has a point* P *of infinite order such that*

$$\frac{L'(E,1)}{\Omega\hat{h}(P)} \in \mathbf{Q}.$$

When E is modular, this was proved by Gross-Zagier (see Theorem 7.3 of [**56**]).

If K is an imaginary quadratic field, let $w(K)$ denote the number of roots of unity in K. Then $w(K) = 2$, 4, or 6, with $w(K) = 4$ if and only if $K = \mathbf{Q}(i)$, and $w(K) = 6$ if and only if $K = \mathbf{Q}(\sqrt{-3})$.

Theorem 4.7.3 (Rubin [**129**])**.** *If* E *is an elliptic curve over* $\mathbf{Q}$ *with CM by* K*, and* $L(E,1) \neq 0$ *(i.e., the analytic rank is* 0*), then*

(i) Ш *is finite,*
(ii) $\#Ш = \frac{L(E,1)}{\Omega}$ *up to powers of primes that divide* $w(K)$*,*
(iii) *BSD II is true up to powers of primes that divide* $w(K)$*.*

Theorem 4.7.4 ([**55**], [**127**], [**129**])**.** *Suppose* E *is an elliptic curve over* $\mathbf{Q}$ *with CM, and the analytic rank is greater than* 0*. Then either the rank is greater than* 0*, or the* p*-primary part of* Ш *is infinite for all primes* $p > 3$*.*

When E has CM and odd analytic rank, Greenberg [**55**] (respectively, Rubin [**127**]) showed that either $\mathrm{rank}(E(\mathbf{Q})) > 0$ or the p-primary part of Ш is infinite for all odd primes p of good ordinary (respectively, good supersingular) reduction. For the full Theorem 4.7.4, see the Theorem on p. 25 of [**129**].

Theorem 4.7.5 (Kolyvagin [**74**])**.** *Suppose* E *is a modular elliptic curve over* $\mathbf{Q}$*, and the analytic rank is* 0 *or* 1*. Then* Ш *is finite.*

4.8. Selmer groups.

To compute Mordell-Weil groups, we need to define Selmer groups.

If X is an abelian group, and m is a positive integer, let $X[m]$ denote the group of elements in X of order dividing m. As before, if E is an elliptic curve over $\mathbf{Q}$ we write $E[m]$ for $E(\mathbf{C})[m]$ $(= E(\bar{\mathbf{Q}})[m])$.

The short exact sequence given by multiplication by m on E

$$0 \to E[m] \to E(\bar{\mathbf{Q}}) \xrightarrow{m} E(\bar{\mathbf{Q}}) \to 0$$

induces cohomology sequences

$$\begin{tikzcd}
0 \arrow[r] & E(\mathbf{Q})/mE(\mathbf{Q}) \arrow[r, "\kappa"] \arrow[d] & H^1(\mathbf{Q}, E[m]) \arrow[r, "\lambda"] \arrow[d, "\mathrm{res}_v"] & H^1(\mathbf{Q}, E(\bar{\mathbf{Q}}))[m] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & E(\mathbf{Q}_v)/mE(\mathbf{Q}_v) \arrow[r, "\kappa_v"] & H^1(\mathbf{Q}_v, E[m]) \arrow[r, "\lambda_v"] & H^1(\mathbf{Q}_v, E(\bar{\mathbf{Q}}_v))[m] \arrow[r] & 0
\end{tikzcd}$$

where the first vertical map is induced by inclusion, and the other two are restriction maps (restricting from $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ to its subgroup $\mathrm{Gal}(\bar{\mathbf{Q}}_v/\mathbf{Q}_v)$). The map κ is defined to take a point P (mod $mE(\mathbf{Q})$) and send it to the cocycle that takes $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ to $\sigma Q - Q$ where $Q \in E(\bar{\mathbf{Q}})$ and $mQ = P$. Note that $E(\mathbf{Q})/mE(\mathbf{Q})$ and $E(\mathbf{Q}_v)/mE(\mathbf{Q}_v)$ are finite groups.

Definition 4.8.1. Define the *m-Selmer group*

$$S_m = \bigcap_v \mathrm{res}_v^{-1}\left(\kappa_v(E(\mathbf{Q}_v)/mE(\mathbf{Q}_v))\right) \subseteq H^1(\mathbf{Q}, E[m]).$$

The "local condition at v" that S_m satisfies is

$$\mathrm{res}_v(S_m) \subseteq \kappa_v(E(\mathbf{Q}_v)/mE(\mathbf{Q}_v)).$$

The Selmer group consists of global cohomology classes that everywhere locally come from local points. We want to understand the Mordell-Weil group by understanding the image of κ, i.e., the global cohomology classes that come from global points. But we don't know how to do that, so we study the cohomology classes that everywhere locally come from local points.

Note that what Ralph Greenberg calls $\mathrm{Sel}_E(\mathbf{Q})_p$ in his lectures is the direct limit of the S_{p^n}'s. (The maps might not be injective, so Ralph's $\mathrm{Sel}_E(\mathbf{Q})_p[p^n]$ is not necessarily my S_{p^n}. They're the same if and only if there is no p-torsion in $E(\mathbf{Q})$.)

Exercise 4.8.2. *Show that S_m is finite. (Hint: This is very similar to the proof in Exercise 3.4.12. Show that the image of S_m in $H^1(\mathbf{Q}(E[m]), E[m])$ is contained in* $\mathrm{Hom}(\mathrm{Gal}(M/\mathbf{Q}(E[m]), E[m])$*, where M is the maximal abelian extension of $\mathbf{Q}(E[m])$ of exponent m unramified outside the primes dividing $m\Delta(E)$.)*

Exercise 4.8.3. *Show that we have a short exact sequence:*

$$0 \to E(\mathbf{Q})/mE(\mathbf{Q}) \xrightarrow{\kappa} S_m \xrightarrow{\lambda} Ш[m] \to 0.$$

Therefore, Ш can be viewed as the obstruction to knowing the Mordell-Weil group, once you know the Selmer group. The Tate-Shafarevich group can therefore be viewed as an "error term".

It follows from Exercises 4.8.2 and 4.8.3 that Ш$[m]$ is finite.

Birch points out that the Parity Conjecture is very close to an earlier conjecture of Selmer [**134**] that for primes p, the p-rank of Ш ($= \dim_{\mathbf{F}_p} Ш[p]$) is even (see [**106**]). By Theorem 4.6.10, Selmer's Conjecture would follow from the finiteness of Ш.

Tate (p. 193 of [**174**]) quotes Barry Mazur as saying that to compute $E(\mathbf{Q})$, by day one makes descents, calculating Selmer groups. By night one computes points in the Mordell-Weil group. If, some happy day or night, this process converges, then one has computed $E(\mathbf{Q})$. On the other hand, if Ш is infinite, then we are doomed to continue computing through all eternity.

Let's start computing.

4.9. Examples — descents.

Example 4.9.1. Let E be the elliptic curve $y^2 = x^3 - x$. This equation is minimal, and we have $N_E = 2^5$, $\Delta(E) = 2^6$. One can compute that $L(E,1) \approx 0.655514\ldots$. Further,

$$\Omega = \int_{E(\mathbf{R})} \frac{dx}{2|y|} = \int_{-1}^{0} + \int_{1}^{\infty} \frac{dx}{\sqrt{x^3 - x}} \approx 5.2441\ldots.$$

Therefore, $L(E,1)/\Omega \approx \frac{1}{8}$. In fact, Birch and Swinnerton-Dyer [**11**] proved that $L(E,1)/\Omega = \frac{1}{8}$. Further, we have $c_p = 1$ if $p \neq 2$. To compute

$$c_2 = \#(E(\mathbf{Q}_2)/E_0(\mathbf{Q}_2)),$$

note that $(1,0) \in E(\mathbf{Q}_2) - E_0(\mathbf{Q}_2)$, since $(1,0)$ is the singular point modulo 2. Suppose $P = (x,y) \in E(\mathbf{Q}_2) - E_0(\mathbf{Q}_2)$. We will show that $P \in (1,0) + E_0(\mathbf{Q}_2)$, thereby proving that $c_2 = 2$. Letting $\tilde{P}$ denote the reduction of P modulo 2, we have $\tilde{P} = (1,0)$, so that $x \equiv 1 \pmod 2$. Thus,

$$P + (1,0) = (x,y) + (1,0) = \left(\frac{x+1}{x-1}, \frac{-2y}{(x-1)^2}\right).$$

If $x \equiv 1 \pmod 4$ then $\widetilde{P + (1,0)} = O$. If $x \equiv 3 \pmod 4$ then $\widetilde{P + (1,0)} = (0,0)$. In both cases, we can conclude that $P + (1,0) \in E_0(\mathbf{Q}_2)$, and therefore $P \in (1,0) + E_0(\mathbf{Q}_2)$. We will consider this curve again in Example 4.9.3 below.

Exercise 4.9.2. *For $E^{(D)} : y^2 = x^3 - D^2x$, show that*

$$\Omega_{E^{(D)}} = \frac{\Omega_{E^{(1)}}}{\sqrt{D}}.$$

To perform additional computations in some examples, we need to do some more work. Suppose that E is an elliptic curve over $\mathbf{Q}$, and

$$E[2] \subseteq E(\mathbf{Q}).$$

Then $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ and $\mathrm{Gal}(\bar{\mathbf{Q}}_v/\mathbf{Q}_v)$ act as the identity on $E[2]$. Therefore,

$$H^1(\mathbf{Q}, E[2]) = \mathrm{Hom}(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), E[2]),$$
$$H^1(\mathbf{Q}_v, E[2]) = \mathrm{Hom}(\mathrm{Gal}(\bar{\mathbf{Q}}_v/\mathbf{Q}_v), E[2]).$$

Let M be the maximal Galois extension of $\mathbf{Q}$ unramified at all primes not dividing $2\Delta(E)$ and with $\mathrm{Gal}(M/\mathbf{Q}) \cong (\mathbf{Z}/2\mathbf{Z})^n$ for some n. Using the hint in Exercise 4.8.2, we have

$$\begin{aligned} E(\mathbf{Q})/2E(\mathbf{Q}) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times (\mathbf{Z}/2\mathbf{Z})^{\mathrm{rank}} &\overset{\kappa}{\hookrightarrow} S_2 \\ \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(M/\mathbf{Q}), E[2]) &\hookrightarrow \mathrm{Hom}(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), E[2]). \end{aligned}$$

Further,

$$\mathrm{Hom}(\mathrm{Gal}(M/\mathbf{Q}), E[2]) \cong \mathrm{Hom}((\mathbf{Z}/2\mathbf{Z})^n, (\mathbf{Z}/2\mathbf{Z})^2) \cong (\mathbf{Z}/2\mathbf{Z})^{2n}.$$

As Ralph Greenberg told us in his lectures,

$$E(\mathbf{Q}_p) \cong \mathbf{Z}_p \times H$$

where H is a finite subgroup of $(\mathbf{Q}/\mathbf{Z})^2$. For $p = 2$, we have

$$E(\mathbf{Q}_2)/2E(\mathbf{Q}_2) \cong (\mathbf{Z}/2\mathbf{Z})^3$$

since $E[2] \subseteq E(\mathbf{Q})$. We therefore have

$$\begin{array}{ccc} (\mathbf{Z}/2\mathbf{Z})^{\mathrm{rank}+2} & \overset{\kappa}{\hookrightarrow} & S_2 \subset \mathrm{Hom}(\mathrm{Gal}(M/\mathbf{Q}), E[2]) \cong (\mathbf{Z}/2\mathbf{Z})^{2n} \\ & & \downarrow \\ & & \mathrm{Hom}(\mathrm{Gal}(M_{\mathfrak{p}}/\mathbf{Q}_2), E[2]) \\ & & \big\downarrow \\ (\mathbf{Z}/2\mathbf{Z})^3 \cong E(\mathbf{Q}_2)/2E(\mathbf{Q}_2) & \overset{\kappa_2}{\hookrightarrow} & \mathrm{Hom}(\mathrm{Gal}(\bar{\mathbf{Q}}_2/\mathbf{Q}_2), E[2]) \cong (\mathbf{Z}/2\mathbf{Z})^6 \end{array}$$

where $\mathfrak{p}$ is a prime ideal of M dividing 2, and $M_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic completion of M. Note that

$$\mathrm{Hom}(\mathrm{Gal}(\bar{\mathbf{Q}}_2/\mathbf{Q}_2), E[2]) \cong (\mathbf{Z}/2\mathbf{Z})^6$$

since the inertia subgroup of $\mathrm{Gal}(\mathbf{Q}_2{}^{\mathrm{ab}}/\mathbf{Q}_2)$ is $\mathbf{Z}_2^\times$, and thus

$$\mathrm{Gal}(\mathbf{Q}_2{}^{\mathrm{ab}}/\mathbf{Q}_2) \cong \mathbf{Z}_2^\times \times \mathrm{Gal}(\bar{\mathbf{F}}_2/\mathbf{F}_2) \cong \mathbf{Z}_2 \times \mathbf{Z}/2\mathbf{Z} \times \hat{\mathbf{Z}},$$

where $\hat{\mathbf{Z}} = \prod \mathbf{Z}_p \cong \mathrm{Gal}(\bar{\mathbf{F}}_2/\mathbf{F}_2)$.

Example 4.9.3. Let E be the elliptic curve $y^2 = x^3 - x$. Then one can check that M is now $\mathbf{Q}(\sqrt{2}, i)$ and that $\mathfrak{p}$ is totally ramified. The above diagram now is:

$$\begin{tikzcd}
(\mathbf{Z}/2\mathbf{Z})^{\mathrm{rank}+2} \arrow[r, hook] & S_2 \arrow[r, phantom, "\subset"] \arrow[ddr, bend right, "\mathrm{res}_2"'] & \mathrm{Hom}(\mathrm{Gal}(M/\mathbf{Q}), E[2]) \cong (\mathbf{Z}/2\mathbf{Z})^4 \arrow[d, equal] \\
 & & \mathrm{Hom}(\mathrm{Gal}(M_{\mathfrak{p}}/\mathbf{Q}_2), E[2]) \arrow[d, hook] \\
(\mathbf{Z}/2\mathbf{Z})^3 \cong E(\mathbf{Q}_2)/2E(\mathbf{Q}_2) \arrow[rr, hook, "\kappa_2"] & & \mathrm{Hom}(\mathrm{Gal}(\bar{\mathbf{Q}}_2/\mathbf{Q}_2), E[2])
\end{tikzcd}$$

Let $P = (\frac{1}{4}, \frac{\sqrt{-15}}{8}) \in E(\mathbf{Q}_2)$ and let $Q = (\alpha, \alpha^2 + 1)$ where α satisfies $x^4 - x^3 + 2x^2 + x + 1$, a $\mathbf{Q}$-irreducible polynomial of discriminant $(15)^2$. Then $2Q = P$, and thus for every $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}_2/\mathbf{Q}_2)$ we have $\kappa_2(P)(\sigma) = \sigma(Q) - Q$. The field $\mathbf{Q}(Q)$ $(= \mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{-3}, \sqrt{5}))$ has degree 4 over $\mathbf{Q}$, with quadratic subfield $\mathbf{Q}(\sqrt{-15})$, while the field $\mathbf{Q}_2(Q)$ $(= \mathbf{Q}_2(\alpha) = \mathbf{Q}_2(\sqrt{-3}) = \mathbf{Q}_2(\sqrt{5}))$ is an unramified quadratic extension of $\mathbf{Q}_2$ $(= \mathbf{Q}_2(\sqrt{-15}))$. Since $M_{\mathfrak{p}}$ is a totally ramified extension of $\mathbf{Q}_2$, it does not contain $\mathbf{Q}_2(Q)$. Therefore, $\kappa_2(P) \notin \mathrm{Hom}(\mathrm{Gal}(M_{\mathfrak{p}}/\mathbf{Q}_2), E[2])$, and thus $\kappa_2(P) \notin \mathrm{res}_2(S_2)$. We have

$$(\mathbf{Z}/2\mathbf{Z})^{\mathrm{rank}+2} \hookrightarrow S_2 \hookrightarrow \mathrm{res}_2(S_2) \subsetneq \kappa_2(E(\mathbf{Q}_2)/2E(\mathbf{Q}_2)) \cong (\mathbf{Z}/2\mathbf{Z})^3.$$

Therefore, $\mathrm{rank}(E(\mathbf{Q})) + 2 \leq 2$, so $\mathrm{rank}(E(\mathbf{Q})) = 0$ (proving what Fermat knew),

$$S_2 \cong (\mathbf{Z}/2\mathbf{Z})^2 \cong E(\mathbf{Q})/2E(\mathbf{Q}), \quad Ш[2] = 0, \quad \text{and} \quad R = 1.$$

The curve E has CM by $K = \mathbf{Q}(i)$. We have $w(K) = 4$, and Rubin [**128**] showed that

$$\#Ш = \frac{L(E,1)}{\Omega}(\text{power of } 2) = \frac{1}{8}(\text{power of } 2).$$

Therefore, $Ш = Ш[2] = 0$. Recalling that by Example 4.9.1 we have $\prod c_p = 2$, therefore

$$\frac{\#Ш R \prod c_p}{\#(E(\mathbf{Q})_{\mathrm{tors}})^2} = \frac{1}{8} = \frac{L(E,1)}{\Omega}.$$

Thus, BSD I and II are true for $y^2 = x^3 - x$.

Example 4.9.4. Let E be the elliptic curve $y^2 = x^3 - 25x$. This is a minimal equation, with discriminant $\Delta(E) = 2^6 5^6$ and conductor $N_E = 2^5 5^2$. We have $c_2 = 2$, $c_5 = 4$, $\Omega_5 = \frac{1}{\sqrt{5}}\Omega_1 \approx 2.3452\ldots$. "By night" we compute that $P = (-4, 6)$ has infinite order (one can apply Theorem 1.5.1 above), so $\mathrm{rank}(E(\mathbf{Q})) \geq 1$. By (11), we have $w_{E^{(5)}} = -1$, so $L(E,1) = 0$. Computing $\frac{L(E,1+t)}{\varepsilon}$ in PARI for $\varepsilon \approx 10^{-10}$ shows that $L'(E,1) \approx 2.227\ldots$, and so the analytic rank is 1. Again,

$E[2] \subset E(\mathbf{Q})$. Here, $M = \mathbf{Q}(\sqrt{2}, i, \sqrt{5})$. There is a unique prime $\mathfrak{p}$ of M above 2, but it is no longer totally ramified. As above, we now have

$$\begin{tikzcd}
(\mathbf{Z}/2\mathbf{Z})^{\mathrm{rank}+2} \arrow[r, hook, "\kappa"] & S_2 & \subset & \mathrm{Hom}(\mathrm{Gal}(M_{\mathfrak{p}}/\mathbf{Q}_2), E[2]) \arrow[d, hook] \\
(\mathbf{Z}/2\mathbf{Z})^3 \arrow[rrr, hook, "\kappa_2"] & & & \mathrm{Hom}(\mathrm{Gal}(\bar{\mathbf{Q}}_2/\mathbf{Q}_2), E[2])
\end{tikzcd}$$

We have

$$(\mathbf{Z}/2\mathbf{Z})^{\mathrm{rank}+2} \subseteq S_2 \subseteq \kappa_2(E(\mathbf{Q}_2)/2E(\mathbf{Q}_2)) \cong (\mathbf{Z}/2\mathbf{Z})^3,$$

so $\mathrm{rank}(E(\mathbf{Q})) \leq 1$. Thus, $\mathrm{rank}(E(\mathbf{Q})) = 1$, and

$$S_2 \cong (\mathbf{Z}/2\mathbf{Z})^3 \cong E(\mathbf{Q}_2)/2E(\mathbf{Q}_2), \quad Ш[2] = 0.$$

By Kolyvagin [**74**], $Ш[p] = 0$ for all odd primes p (Kolyvagin rules out the CM case, but his proof also works in the case we are in). Thus, $Ш = 0$. One computes that $\hat{h}(P) \approx 0.94974\ldots$. As an exercise, show that P and the torsion points $(5,0)$ and $(0,0)$ together generate $E(\mathbf{Q})$. (Hint: Use Exercise 9.12 in [**156**], which implies that if an integral point on an elliptic curve (in generalized Weierstrass form with integer coefficients) is a multiple of another point Q, then Q is also integral.) Therefore,

$$R = 2\hat{h}(P) \approx 1.89948\ldots,$$

and $\frac{L'(E,1)}{\Omega R} \approx \frac{1}{2}$. By Gross-Zagier [**56**], $\frac{L'(E,1)}{\Omega R} = \frac{1}{2}$. Now

$$\frac{\#Ш \prod c_p}{\#(E(\mathbf{Q})_{\mathrm{tors}})^2} = \frac{1}{2},$$

and BSD I and II are true for $y^2 = x^3 - 25x$.

Example 4.9.5. Let E be the elliptic curve $y^2 = x^3 - (17)^2 x$. This is a minimal equation, with discriminant $\Delta(E) = 2^6(17)^6$ and conductor $N_E = 2^5(17)^2$. We have $c_2 = 2$, $c_{17} = 4$, $\Omega_{17} = \frac{1}{\sqrt{17}}\Omega_1 \approx 1.27188\ldots$, $L(E,1) \approx 2.54377\ldots \neq 0$. Therefore, the analytic rank is 0. We have $\frac{L(E,1)}{\Omega_{17}} = 2$. Now, $M = \mathbf{Q}(\sqrt{2}, i, \sqrt{17})$. Taking $\mathfrak{p}$ to be a prime ideal of M above 2, then $M_{\mathfrak{p}}$ $(= \mathbf{Q}_2(i, \sqrt{2}))$ is a totally ramified degree 4 extension of $\mathbf{Q}_2$ $(= \mathbf{Q}_2(\sqrt{17}))$. As above, we have:

$$\begin{tikzcd}
(\mathbf{Z}/2\mathbf{Z})^{\mathrm{rank}+2} \arrow[r, hook, "\kappa"] & S_2 \subset \arrow[ddr, bend right, "\mathrm{res}_2"'] & \mathrm{Hom}(\mathrm{Gal}(M/\mathbf{Q}), E[2]) \cong (\mathbf{Z}/2\mathbf{Z})^6 \arrow[d] \\
& & \mathrm{Hom}(\mathrm{Gal}(M_{\mathfrak{p}}/\mathbf{Q}_2), E[2]) \cong (\mathbf{Z}/2\mathbf{Z})^4 \arrow[d, hook] \\
(\mathbf{Z}/2\mathbf{Z})^3 \cong E(\mathbf{Q}_2)/2E(\mathbf{Q}_2) \arrow[rr, hook, "\kappa_2"] & & \mathrm{Hom}(\mathrm{Gal}(\bar{\mathbf{Q}}_2/\mathbf{Q}_2), E[2]) \cong (\mathbf{Z}/2\mathbf{Z})^6
\end{tikzcd}$$

Let

$$P = \left(\frac{1}{4}, \frac{\sqrt{-4623}}{8}\right) \in E(\mathbf{Q}_2).$$

Then for every $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}_2/\mathbf{Q}_2)$ we have $\kappa_2(P)(\sigma) = \sigma(Q) - Q$ with $Q = (\alpha, \beta)$ and $2Q = P$, where α and β are roots of irreducible polynomials of degree 4 over

$\mathbf{Q}$. The field $\mathbf{Q}_2(Q)$ is an unramified extension of $\mathbf{Q}_2$ of discriminant $(4623)^2$. Since $M_{\mathfrak{p}}$ is a totally ramified extension of $\mathbf{Q}_2$, it does not contain $\mathbf{Q}_2(Q)$. Therefore,

$$\kappa_2(P) \notin \mathrm{res}_2(S_2) \subsetneq \mathrm{im}(\kappa_2) \cong (\mathbf{Z}/2\mathbf{Z})^3.$$

Therefore, $\#\mathrm{res}_2(S_2) \leq 4$. Since $\# \ker(\mathrm{res}_2) \leq 4$, we have $\#S_2 \leq 16$. Since

$$(\mathbf{Z}/2\mathbf{Z})^2 \subseteq S_2 \subseteq (\mathbf{Z}/2\mathbf{Z})^4,$$

we have $Ш[2] \subseteq (\mathbf{Z}/2\mathbf{Z})^2$. It is possible to show that $S_2 \cong (\mathbf{Z}/2\mathbf{Z})^4$ (we have

$$S_2 \subset \mathrm{res}_2^{-1}(\mathrm{im}\kappa_2) \cap \mathrm{Hom}(\mathrm{Gal}(M/\mathbf{Q}), E[2]),$$

and one can show equality by checking the right side for the local conditions at 17 and ∞) and/or that $Ш[2] \cong (\mathbf{Z}/2\mathbf{Z})^2$ (by constructing elements). Therefore, $\#Ш \geq 4$. Rubin [**128**] showed that $Ш[p] = 0$ for all odd prime numbers p, and Ш is finite. One could do a "second descent" to compute that $S_4 \cong (\mathbf{Z}/2\mathbf{Z})^4 \cong S_2$, and therefore that $\mathrm{rank}(E(\mathbf{Q})) = 0$, the 2-primary part of Ш is $(\mathbf{Z}/2\mathbf{Z})^2$ (since there are no elements of order 4), and $Ш \cong (\mathbf{Z}/2\mathbf{Z})^2$. Alternatively, the theorem of Coates-Wiles [**32**] implies that the rank is 0 (since the analytic rank is 0). It follows that BSD I and II are true for $y^2 = x^3 - (17)^2 x$.

CHAPTER 5
ABC and related conjectures

The ABC Conjecture and its variants, although not explicitly stated in terms of elliptic curves, are closely connected with conjectures about elliptic curves, as we shall see below. This chapter relies heavily on [**183**].

When we write $X \ll_\varepsilon Y$ we mean that there exists a positive constant C_ε, depending only on ε, such that $X \leq C_\varepsilon Y$. Further, $\prod_{p|N}$ means that the product is taken over all prime divisors p of N.

5.1. ABC Conjectures.

The ABC Conjecture was conjectured (independently) by Masser and Oesterlé.

ABC Conjecture. *Suppose A, B, and C are positive integers, suppose*

$$\gcd(A, B, C) = 1,$$

and suppose

$$A + B = C.$$

Then

$$C \ll_\varepsilon \left(\prod_{p|ABC} p \right)^{1+\varepsilon}.$$

ABC Conjecture Variant 1. *Suppose $A, B, C \in \mathbf{Z}$, $\gcd(A, B, C) = 1$, and $A + B = C$. Then*

$$\max(|A|, |B|, |C|) \ll_\varepsilon \left(\prod_{p|ABC} p \right)^{1+\varepsilon}.$$

Exercise 5.1.1. *Show that the ABC Conjecture is equivalent to ABC Conjecture Variant 1.*

ABC Conjecture Variant 2.

$$\limsup \frac{\log C}{\log \prod_{p|ABC} p} = 1,$$

where the lim sup *is taken over all positive integers A, B, and C with $A + B = C$ and* $\gcd(A, B, C) = 1$.

Browkin et al. [**16**] proved that the set of limit points is equal to $\left[\frac{1}{3}, 1\right]$ if one assumes the ABC Conjecture. Greaves and Nitaj [**54**] proved that the set of limit points contains $\left[\frac{1}{3}, \frac{36}{37}\right]$.

Exercise 5.1.2. *Show that the ABC Conjecture is equivalent to ABC Conjecture Variant 2. Also, show that*

$$\limsup \frac{\log C}{\log \prod_{p|ABC} p} \geq 1.$$

Hint: Show that letting $A = 1$ and $B = 9^k - 1$ gives infinitely many triples (A, B, C) such that

$$\frac{\log C}{\log \prod_{p|ABC} p} > 1.$$

Weak ABC Conjecture. *Suppose A, B, and C are integers, suppose*

$$\gcd(A, B, C) = 1,$$

and suppose $A + B = C$. Then

$$|ABC|^{1/3} \ll_\varepsilon \left(\prod_{p|ABC} p \right)^{1+\varepsilon}.$$

Clearly, the Weak ABC Conjecture follows from the ABC Conjecture.

Exercise 5.1.3. *Show that the Weak ABC Conjecture implies that Fermat's Last Theorem is true for all sufficiently large exponents.*

Conjecture 5.1.4 (Generalized ABC or n-conjecture)**.** *Fix $n \geq 3$. Suppose*

$$a_1, \ldots, a_n \in \mathbf{Z}, \quad a_1 + \cdots + a_n = 0,$$

and no proper subsum is 0. Then

$$\limsup \frac{\log \max |a_i|}{\log \prod_{p|a_1 \cdots a_n} p} = 2n - 5.$$

Browkin and and Brzezinski [**15**] showed that

$$\limsup \frac{\log \max |a_i|}{\log \prod_{p|a_1 \cdots a_n} p} \geq 2n - 5.$$

A conjecture of Vojta (in analogy with Nevanlinna Theory), applied to the hyperplane $x_1 + \cdots x_n = 0$ in $\mathbf{P}^{n-1}$, implies the following conjecture.

Conjecture 5.1.5 (Vojta's n-conjecture, see [**181**])**.** *Fix $n \geq 3$. Suppose*

$$a_1, \ldots, a_n \in \mathbf{Z} - 0, \quad \gcd(a_1, \ldots, a_n) = 1, \quad \textit{and} \quad a_1 + \cdots + a_n = 0.$$

Then

$$\limsup \frac{\log \max |a_i|}{\log \prod_{p|a_1 \cdots a_n} p} = 1$$

for all such $(a_1, \ldots, a_n)$ outside a proper Zariski-closed subset.

Exercise 5.1.6 ([**181**])**.** *Show that one cannot remove the phrase "outside a proper Zariski-closed subset" in Vojta's n-conjecture. (Hint: Either see [**181**], or use*[1] *$a_1 = 2^a$, $a_2 = -2^a$, $a_3 = 3^b$, $a_4 = -3^b$.)*

[1] I thank Noam Elkies for pointing out this example to me.

Theorem 5.1.7 (Elkies [**42**]). *An effective version of the ABC Conjecture over a number field K implies an effective version of the Mordell Conjecture (Faltings' Theorem) over K.*

See [**165**], [**167**], [**114**], and [**113**] for some additional results on the ABC Conjecture.

5.2. ABC Conjectures for function fields.

Even before the ABC Conjecture was stated for number fields, it had been proved for function fields.

Theorem 5.2.1 (Mason [**93**], see also [**79**]). *Suppose K is an integral domain of characteristic 0. For $f \in K[t]$, let $\mathrm{rad}(f)$ denote the product of the distinct irreducible factors of f. Suppose f, g, $h \in K[t]$, suppose $\gcd(f,g,h) = 1$, and suppose $f + g = h$. Then*

$$\limsup \frac{\max(\deg(f), \deg(g), \deg(h))}{\deg \mathrm{rad}(fgh)} = 1.$$

Conjecture 5.2.2 (Generalized ABC or n-conjecture: function fields). *Fix $n \geq 3$. If*

$$f_1, \dots, f_n \in K[t], \quad \gcd(f_1, \dots, f_n) = 1, \quad \text{and} \quad f_1 + \cdots + f_{n-1} = f_n,$$

then

$$\limsup \frac{\max \deg f_i}{\deg(\mathrm{rad}(f_1 \cdots f_n))} = 2n - 5.$$

This conjecture has been proved for $n = 3$ by Mason's Theorem above, and for $n = 4$ by Browkin and Brzezinski [**15**]. Browkin showed that when $n = 3$ the set of limit points is $\left[\frac{1}{3}, 1\right]$. Davies [**38**] proved that for $n \geq 3$ the set of limit points contains $\left[\frac{1}{n}, 2n - 5\right]$.

5.3. Szpiro Conjecture.

Let E be an elliptic curve over $\mathbf{Q}$. Let N_E denote the conductor of E and let $\Delta_{\min}(E)$ denote the minimal discriminant (i.e., the discriminant of a minimal Weierstrass equation for E).

Szpiro Conjecture. *If E is an elliptic curve over $\mathbf{Q}$, then*

$$|\Delta_{\min}(E)| \ll_\varepsilon N_E^{6+\varepsilon}.$$

Exercise 5.3.1. *Show that Szpiro's Conjecture implies the Weak ABC Conjecture. Hint: Use that, under the hypotheses of the Weak ABC Conjecture, the conductor of the elliptic curve*

$$y^2 = x(x - A)(x + B)$$

is $\left(\prod_{p|ABC} p\right)$ (up to a bounded power of 2), and the minimal discriminant is $(ABC)^2$ (up to a bounded power of 2).

The following theorem was conjectured in [**18**].

Theorem 5.3.2 (see [**136**]; see also [**101**], [**46**], [**98**]). *Suppose E is an elliptic curve over $\mathbf{Q}$ with prime conductor p. Then either $|\Delta_{\min}(E)| = p$ or p^2, or else $p = 11$ and $|\Delta_{\min}(E)| = 11^5$, or $p = 17$ and $|\Delta_{\min}(E)| = 17^4$, or $p = 19$ and $|\Delta_{\min}(E)| = 19^3$, or $p = 37$ and $|\Delta_{\min}(E)| = 37^3$. (Therefore $\Delta_{\min}(E)$ divides p^5.)*

This result implies that Szpiro's Conjecture would be true if one restricted to elliptic curves of prime conductor.

In [**115**], Nitaj gives an example (of a curve of conductor $2526810 = 2\cdot 3\cdot 5\cdot 11\cdot 13\cdot 19\cdot 31$) with "large Szpiro ratio":

$$\frac{\log|\Delta_{\min}(E)|}{\log N_E} \approx 8.812.$$

As a corollary of Theorem 4.6.4 above, de Weger proves:

Theorem 5.3.3 (see Corollary on p. 113 of [**183**]). *If Szpiro's Conjecture is true, then there exists an absolute constant C so that*

$$\prod_{p|\Delta(E)} c_p \ll N_E^{C/\log\log(N_E)}.$$

According to de Weger, an interesting open question is to improve his bounds on the product of the "fudge factors" c_p.

Generalized Szpiro Conjecture. *If E is an elliptic curve over $\mathbf{Q}$, then*

$$\max(|\Delta_{\min}(E)|, |g_2^3|) \ll_\varepsilon N_E^{6+\varepsilon},$$

where $|g_2|$ is minimal with the property that E has a model of the form $y^2 = 4x^3 - g_2x - g_3$ with g_2, $g_3 \in \mathbf{Z}$.

The ABC Conjecture is equivalent to the Generalized Szpiro Conjecture.

A function field analogue of Szpiro's Conjecture (with $\varepsilon = 0$ and an explicit constant) is true (and was proved by Kodaira; see Exercise 3.36 on p. 287 of [**158**]).

For some additional results relating to Szpiro's Conjecture, see [**45**].

5.4. Goldfeld-Szpiro Conjecture.

If E is an elliptic curve over $\mathbf{Q}$, let $Ш_E$ denote the Tate-Shafarevich group $Ш(E/\mathbf{Q})$.

Goldfeld-Szpiro Conjecture [**52**]. *If E is an elliptic curve over $\mathbf{Q}$, then*

$$\#Ш_E \ll_\varepsilon N_E^{1/2+\varepsilon}.$$

Modulo the Conjecture of Birch and Swinnerton-Dyer (and the Modularity Conjecture) for E, the Goldfeld-Szpiro Conjecture is equivalent to the Szpiro Conjecture (see [**52**]).

Theorem 5.4.1 (Cassels [**27**], see also [**13**], [**77**], [**87**]). *$\#Ш_E$ is unbounded, as E varies over elliptic curves over $\mathbf{Q}$.*

Cassels showed the 3-rank of $Ш_E$ is unbounded (i.e., $Ш_E$ contains $(\mathbf{Z}/3\mathbf{Z})^k$ with k arbitrarily large) in the family of cubic twists $x^3 + y^3 = d$. Bölling [**13**] showed that the 2-rank of the Tate-Shafarevich group is unbounded for elliptic curves (over a fixed number field) with a fixed j-invariant.

Definition 5.4.2. An elliptic curve E over $\mathbf{Q}$ is *semistable* if its conductor N_E is square-free.

Conjecture 5.4.3 (Mazur, [**98**]). *There exist semistable elliptic curves over $\mathbf{Q}$ of arbitrarily high conductor N_E with $Ш_E = 0$.*

In particular, Mazur predicts that

$$\liminf \frac{\#Ш_E}{\sqrt{N_E}} = 0.$$

5.5. de Weger Conjectures.

It was conjectured by de Weger that the bound in the Goldfeld-Szpiro Conjecture is best possible. In other words:

de Weger N_E Conjecture. *For every $\varepsilon > 0$ there exist infinitely many elliptic curves E over $\mathbf{Q}$ with*

$$\#\text{Ш}_E \geq N_E^{1/2-\varepsilon}.$$

Exercise 5.5.1. *Show this is equivalent to:*

For every $\varepsilon > 0$ and every $C > 0$, there exist infinitely many elliptic curves E over $\mathbf{Q}$ with

$$\#\text{Ш}_E > CN_E^{1/2-\varepsilon}.$$

and to:

For every $\varepsilon > 0$ there exist infinitely many elliptic curves E over $\mathbf{Q}$ with

$$\#\text{Ш}_E \gg_\varepsilon N_E^{1/2-\varepsilon}.$$

de Weger $\Delta_{\min}(E)$ Conjecture. *For every $\varepsilon > 0$ there exist infinitely many elliptic curves E over $\mathbf{Q}$ with*

$$\#\text{Ш}_E \geq \Delta_{\min}(E)^{1/12-\varepsilon}.$$

In de Weger's paper [**183**] he says that the methods of Cassels, Bölling, and Kramer would at best show that there are infinitely many elliptic curves E over $\mathbf{Q}$ with

$$\#\text{Ш}_E \gg N_E^{C/\log\log N}$$

for some $C > 0$. Cassels and Bölling consider twists, adding one prime p at a time. This multiplies the conductor by p^2, but at best multiplies $\#\text{Ш}_E$ by a constant. The prime number theorem would then give the desired result. Mai and Murty [**87**] show that if the Conjecture of Birch and Swinnerton-Dyer is true, then there are infinitely many elliptic curves E over $\mathbf{Q}$ (of rank and analytic rank 1, all quadratic twists of each other) with

$$\#\text{Ш}_E \geq N_E^{1/4-\varepsilon}.$$

Theorem 5.5.2 (de Weger [**183**]). *The de Weger N_E Conjecture follows by combining BSD II in the rank 0 case, the Szpiro Conjecture, and a generalization of the Riemann Hypothesis (for the Rankin-Selberg zeta-function associated to the weight 3/2 modular form associated to E by the Shintani-Shimura lift).*

Theorem 5.5.3 (de Weger [**183**]). *The de Weger $\Delta_{\min}(E)$ Conjecture follows from BSD II in the rank 0 case.*

The largest value I know of that has been found so far for (the conjectured value of) $\#\text{Ш}_E/\sqrt{N_E}$ was found by Nitaj [**116**] and is approximately 42.265. In that example

$$N_E = 6305720190 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 \cdot 37 \cdot 353$$

and the conjectured order of Ш_E is $(2^3 \cdot 229)^2$.

5.6. Additional remarks.

Frey [**46**] has conjectured bounds on the degrees of the modular parametrizations of elliptic curves (in terms of the conductor), which implies a conjecture he has on the heights of elliptic curves, which in turn implies the ABC Conjecture.

See also [**117**], [**79**], [**80**], [**114**], and pp. 84–88 of [**180**] for surveys of some of these conjectures, and for relationships between these conjectures and others.

CHAPTER 6
Some other conjectures

We close with some additional comments and conjectures.

6.1. Integral points on elliptic curves.

The starting point for any work on integral points on elliptic curves is the following theorem of Siegel.

Theorem 6.1.1 (Siegel). *Every affine model of an elliptic curve over* $\mathbf{Q}$ *has only finitely many points over* $\mathbf{Z}$.

For more recent results on integral points on elliptic curves, see for example [**170**], [**171**], [**48**], [**163**], [**178**], [**169**], [**47**], [**161**], and [**187**].

I learned from [**159**] the statement of the following question:

Question 6.1.2. *Is there is a uniform bound on the number of integral points on minimal (affine) Weierstrass equations for elliptic curves over* $\mathbf{Q}$*?*

The following conjecture of Lang (see Conjecture IX.3.5 of [**156**] and p. 140 of [**78**]) predicts a bound on the number of integral points in terms of the rank of the Mordell-Weil group.

Conjecture 6.1.3 (Lang). *There is an absolute constant* C *such that if* E *is an elliptic curve over* $\mathbf{Q}$ *given by a minimal (affine) Weierstrass equation, then the number of integral points on* E *is at most* $C^{1+\operatorname{rank}(E(\mathbf{Q}))}$.

Silverman [**157**] proved Lang's Conjecture for elliptic curves over $\mathbf{Q}$ with everywhere potentially good reduction (i.e., with integral j-invariant).

See [**137**] for a good discussion of integral points on curves.

6.2. Bounds on numbers of rational points on curves.

Faltings [**43**] proved Mordell's Conjecture that if C is a smooth curve of genus $g \geq 2$ defined over a number field K, then $C(K)$ is finite. The following conjectures predict bounds on the number of points.

Caporaso-Harris-Mazur Conjecture ([**22**]). *If* K *is a number field and* $2 \leq g \in \mathbf{Z}$*, then there exists a constant* $B(K,g)$ *such that no smooth curve of genus* g *defined over* K *has more than* $B(K,g)$ K*-rational points.*

Strong Caporaso-Harris-Mazur Conjecture ([**22**]). *If $2 \leq g \in \mathbf{Z}$, then there exists a constant $N(g)$ such that for every number field K there are only finitely many smooth curves of genus g defined over K with more than $N(g)$ K-rational points.*

See also [**23**], where they show that a conjecture of Lang implies the Caporaso-Harris-Mazur Conjecture.

Theorem 6.2.1 (Brumer and Mestre). *For all g,*

$$N(g) \geq 16(g+1).$$

Theorem 6.2.2 (Shioda [**152**]). *For all g,*

$$B(\mathbf{Q}, g) \geq 8g + 16.$$

Theorem 6.2.3 (Keller-Kulesz [**70**]).

$$B(\mathbf{Q}, 2) \geq 588, \qquad B(\mathbf{Q}, 3) \geq 176.$$

Keller and Kulesz showed that the genus 2 curve

$$y^2 = 278,271,081x^2(x^2-9)^2 - 229,833,600(x^2-1)^2$$

has at least 588 rational points, and the genus 3 curve

$$y^2 = 7,920,000(x^2+1)^4 - 136,782,591x^2(x^2-1)^2$$

has at least 176 rational points.

6.3. Conductors of elliptic curves.

Let $M(N)$ denote the number of ($\mathbf{Q}$-isomorphism classes of) elliptic curves over $\mathbf{Q}$ of conductor N.

Conjecture 6.3.1 (Brumer-Silverman [**20**]). *With p prime, $M(p)$ is unbounded.*

Brumer and Silverman point out that their conjecture implies the unboundedness of both ranks of elliptic curves over $\mathbf{Q}$ (using Silverman's result bounding the number of integral points in terms of the rank, for elliptic curves with integral j-invariant, and Serre's Theorem 5.3.2 above that if N_E is prime then $\Delta_{\min}(E)$ divides p^5) and 3-ranks of ideal class groups of quadratic fields. Conjecture 6.3.1 would contradict an affirmative answer to Question 6.1.2.

6.4. Abelian varieties, Shimura varieties, and open questions.

Abelian varieties are parametrized by Shimura varieties, the way elliptic curves are parametrized by modular curves. As can be seen from the work of Faltings (the Mordell Conjecture) and Wiles (Fermat's Last Theorem), one often cannot remain within the realm of elliptic curves and modular curves, and must use and understand higher dimensional abelian varieties and Shimura varieties. Many results that are known for elliptic curves are still interesting conjectures for abelian varieties. This leaves open wide areas of research for the years to come.

The Mumford-Tate Conjecture (see [**138**], [**39**]) deals with the images of ℓ-adic representations associated to varieties, and is related to the Tate Conjectures [**172**] (which in turn are related to the conjectures of Birch and Swinnerton-Dyer).

As mentioned earlier, see for example [**124**], [**111**], and [**12**] for the conjectures of Beilinson and of Bloch-Kato, which generalize the conjectures of Birch and Swinnerton-Dyer.

There are Modularity Conjectures for elliptic curves over number fields other than $\mathbf{Q}$, and for abelian varieties with real multiplication (or more generally, for abelian varieties of GL_2-type). See for example [**125**], [**58**], and [**59**] (see [**50**] and [**49**] for analogues over function fields). See also Ken Ribet's lectures on Serre's Conjectures [**136**], in this volume.

BIBLIOGRAPHY

1. D. Abramovich, *Formal finiteness and the torsion conjecture on elliptic curves. A footnote to a paper "Rational torsion of prime order in elliptic curves over number fields"*, Columbia University Number Theory Seminar (New York, 1992), Astérisque **228** (1995), 3, 5–17.
2. N. Aoki, *Torsion points on abelian varieties with complex multiplication*, in Algebraic cycles and related topics (Kitasakado, 1994), 1–22, World Sci. Publishing, River Edge, NJ, 1995.
3. M. Artin, H. P. F. Swinnerton-Dyer, *The Shafarevich-Tate conjecture for pencils of elliptic curves on $K3$ surfaces*, Invent. Math. **20** (1973), 249–266.
4. C. Batut, K. Belabas, D. Bernardi, H. Cohen, M. Olivier, *PARI-GP*, `ftp://megrez.math.u-bordeaux.fr/pub/pari/` .
5. W. Bauer, *On the conjecture of Birch and Swinnerton-Dyer for abelian varieties over function fields in characteristic $p > 0$*, Invent. Math. **108** (1992), no. 2, 263–287.
6. G. Billing, *Vom Range kubischer Kurven vom Geschlecht Eins in algebraischen Rationalitätsbereichen* (Helsingfors, 23.–26. VIII. 1938), 146–150, IX Congress of Scandinavian Mathematicians, 1939.
7. B. J. Birch, *Conjectures concerning elliptic curves*, in Proc. Sympos. Pure Math. **VIII**, 106–112, Amer. Math. Soc., Providence, R.I., 1965.
8. B. J. Birch, *Diophantine analysis and modular functions*, in Algebraic Geometry (Internat. Colloq., Tata Inst. Fund. Res., Bombay, 1968), 35–42, Oxford Univ. Press, London, 1969.
9. B. J. Birch, *Elliptic curves and modular functions*, in Symposia Mathematica, Vol. IV (INDAM, Rome, 1968/69), 27–32 Academic Press, London, 1970.
10. B. Birch, H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. I*, J. Reine Angew. Math. **212** (1963), 7–25.
11. B. Birch, H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. II*, J. Reine Angew. Math. **218** (1965), 79–108.
12. S. Bloch, K. Kato, *L-functions and Tamagawa numbers of motives*, in The Grothendieck Festschrift, Vol. I, 333–400, Progr. Math. **86**, Birkhäuser Boston, Boston, MA, 1990.
13. R. Bölling, *Die Ordnung der Schafarewitsch-Tate Gruppe kann beliebig gross werden*, Math. Nachr. **67** (1975), 157–179.

14. S. Bosch, W. Lütkebohmert, M. Raynaud, Néron models, Springer, Berlin-Heidelberg-New York, 1990.
15. J. Browkin, J. Brzezinski, *Some remarks on the abc-conjecture*, Math. Comp. **62** (1994), 931–939.
16. J. Browkin, M. Filaseta, G. Greaves, A. Schinzel, *Squarefree values of polynomials and the abc-conjecture*, in Sieve methods, exponential sums, and their applications in number theory (Cardiff, 1995), 65–85, London Math. Soc. Lecture Note Ser., **237**, Cambridge Univ. Press, Cambridge, 1997.
17. A. Brumer, *The average rank of elliptic curves. I*, Invent. Math. **109** (1992), no. 3, 445–472.
18. A. Brumer, K. Kramer, *The rank of elliptic curves*, Duke Math. J. **44** (1977), no. 4, 715–743.
19. A. Brumer, O. McGuinness, *The behavior of the Mordell-Weil group of elliptic curves*, Bull. Amer. Math. Soc. **23** (1990), no. 2, 375–382.
20. A. Brumer, J. H. Silverman, *The number of elliptic curves over* $\mathbf{Q}$ *with conductor* N, Manuscripta Math. **91** (1996), no. 1, 95–102.
21. D. Bump, S. Friedberg, J. Hoffstein, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Invent. Math. **102** (1990), no. 3, 543–618.
22. L. Caporaso, J. Harris, B. Mazur, *How many rational points can a curve have?*, in The moduli space of curves (Texel Island, 1994), 13–31, Progr. Math., **129**, Birkhäuser Boston, Boston, MA, 1995.
23. L. Caporaso, J. Harris, B. Mazur, *Uniformity of rational points*, J. Amer. Math. Soc. **10** (1997), no. 1, 1–35.
24. H. Carayol, *Sur les représentations* ℓ*-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. École Norm. Sup. (4) **19** (1986), no. 3, 409–468.
25. J. W. S. Cassels, *Arithmetic on an elliptic curve*, in Proc. Internat. Congr. Mathematicians (Stockholm, 1962), 234–246, Inst. Mittag-Leffler, Djursholm, 1963.
26. J. W. S. Cassels, *Arithmetic on curves of genus* 1 *(IV). Proof of the Hauptvermutung*, J. reine angew. Math. **211** (1962), 95–112.
27. J. W. S. Cassels, *Arithmetic on curves of genus* 1 *(VI). The Tate-Safarevic group can be arbitrarily large*, J. reine angew. Math. **214/215** (1964), 65–70.
28. J. W. S. Cassels, *Arithmetic on curves of genus* 1 *(VIII). On conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. **217** (1965), 180–199.
29. J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193–291.
30. J. Chahal, M. Meijer, J. Top, *Sections on certain* $j = 0$ *elliptic surfaces*, `http://www.math.uiuc.edu/Algebraic-Number-Theory/0214/index.html` .
31. K. Chandrasekharan, R. Narasimhan, *Functional equations with multiple Gamma factors and the average order of arithmetical functions*, Ann. of Math. **76** (1962), 93–136.
32. J. Coates, A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), no. 3, 223–251.
33. H. Cohen, A course in computational algebraic number theory, Graduate Texts in Mathematics **138**, Springer-Verlag, Berlin, 1993.
34. Ian Connell, *Apecs*, `ftp://ftp.math.mcgill.ca/pub/apecs/` .
35. J. E. Cremona, Algorithms for modular elliptic curves, Second edition, Cambridge Univ. Press, Cambridge, 1997.

36. J. E. Cremona, *mwrank and related programs*, `http://www.maths.nott.ac.uk/personal/jec/packages.html` .
37. R. M. Damerell, *L-functions of elliptic curves with complex multiplication. I, II*, Acta Arith. **17** (1970), 287–301; **19** (1971), 311–317.
38. D. Davies, *A note on the limit points associated with the generalized abc-conjecture for* $\mathbf{Z}[t]$, Colloq. Math. **71** (1996), no. 2, 329–333.
39. P. Deligne, J. S. Milne, A. Ogus, K-y. Shih, Hodge cycles, motives, and Shimura varieties, Lecture Notes in Math. **900**, Springer-Verlag, Berlin-New York, 1982.
40. B. Edixhoven, *Rational torsion points on elliptic curves over number fields (after Kamienny and Mazur)*, Sém. Bourbaki, Exp. No. 782, Astérisque **227** (1995), 4, 209–227.
41. M. Eichler, *Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion*, Arch. Math. **5** (1954), 355–366.
42. N. Elkies, *ABC implies Mordell*, Internat. Math. Res. Notices **7** (1991), 99–109.
43. G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.
44. E. V. Flynn, *Sequences of rational torsions on abelian varieties*, Invent. math. **106** (1991), 433–442.
45. E. Fouvry, M. Nair, G. Tenenbaum, *L'ensemble exceptionnel dans la conjecture de Szpiro*, Bull. Soc. Math. France **120** (1992), no. 4, 485–506.
46. G. Frey, *Links between solutions of* $A - B = C$ *and elliptic curves*, in Number theory (Ulm, 1987), 31–62, Lecture Notes in Math. **1380**, Springer, New York-Berlin, 1989.
47. J. Gebel, A. Pethö, H. G. Zimmer, *Computing integral points on elliptic curves*, Acta Arith. **68** (1994), no. 2, 171–192.
48. J. Gebel, A. Pethö, H. G. Zimmer, *On Mordell's equation*, Compositio Math. **110** (1998), no. 3, 335–367.
49. E-U. Gekeler, *Jacquet-Langlands theory over* K *and relations with elliptic curves*, in Drinfeld modules, modular schemes and applications (Alden-Biesen, 1996), 224–257, World Sci. Publishing, River Edge, NJ, 1997.
50. E-U. Gekeler, M. Reversat, *Jacobians of Drinfeld modular curves*, J. Reine Angew. Math. **476** (1996), 27–93.
51. D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, in Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), 108–118, Lecture Notes in Math. **751**, Springer-Verlag, Berlin, 1979.
52. D. Goldfeld, L. Szpiro, *Bounds for the order of the Tate-Shafarevich group*, Compositio Math. **97** (1995), 71–87.
53. F. Gouvêa, B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), 1–23.
54. G. Greaves, A. Nitaj, *Some polynomial identities related to the abc-conjecture*, in Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997), 229–236, de Gruyter, Berlin, 1999.
55. R. Greenberg, *On the Birch and Swinnerton-Dyer conjecture*, Invent. Math. **72** (1983), 241–265.
56. B. H. Gross, D. B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.

57. M. Harris, *Systematic growth of Mordell-Weil groups of abelian varieties in towers of number fields*, Invent. Math. **51** (1979), no. 2, 123–141.
58. Y. Hasegawa, **Q**-*curves over quadratic fields*, Manuscripta Math. **94** (1997), no. 3, 347–364.
59. Y. Hasegawa, K. Hashimoto, F. Momose, *Modularity conjecture for* **Q**-*curves and* QM-*curves*, preprint.
60. D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem. II*, Invent. Math. **118** (1994), no. 2, 331–370.
61. K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z. **56** (1952), 227–253.
62. M. Hindry, J. Silverman, *The canonical height and integral points on elliptic curves*, Invent. math. **93** (1988), 419–450.
63. T. Honda, *Isogenies, rational points and section points of group varieties*, Japan. J. Math. **30** (1960), 84–101.
64. Dale Husemöller, Elliptic curves, Graduate Texts in Mathematics **111**, Springer-Verlag, New York-Berlin, 1987.
65. S. Kamienny, *Torsion points on elliptic curves and* q-*coefficients of modular forms*, Invent. Math. **109** (1992), 221–229.
66. S. Kamienny, *Torsion points on elliptic curves over fields of higher degree*, Internat. Math. Res. Notices (1992), 129–133.
67. S. Kamienny, B. Mazur, *Rational torsion of prime order in elliptic curves over number fields*, Columbia University Number Theory Seminar (New York, 1992), Astérisque **228** (1995), 3, 81–100.
68. N. Katz, P. Sarnak, *Zeroes of zeta functions and symmetry*, Bull. Amer. Math. Soc. **36** (1999), 1–26.
69. N. Katz, P. Sarnak, Random matrices, Frobenius eigenvalues and monodromy, AMS Colloquium Publications **45**, Amer. Math. Soc., Providence, RI, 1999.
70. W. Keller, L. Kulesz, *Courbes algébriques de genre* 2 *et* 3 *possédant de nombreux points rationnels*, C. R. Acad. Sci. Paris Sér. I Math. **321** (1995), no. 11, 1469–1472.
71. M. Kenku, F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149.
72. S. Kihara, *On an infinite family of elliptic curves with rank* ≥ 14 *over* **Q**, Proc. Japan Acad. Ser. A Math. Sci. **73** (1997), no. 2, 32.
73. Neal Koblitz, Introduction to elliptic curves and modular forms, Graduate Texts in Mathematics **97**, Springer-Verlag, New York, 1993.
74. V. A. Kolyvagin, *Finiteness of* $E(\mathbf{Q})$ *and* $\text{Ш}(E, \mathbf{Q})$ *for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540, 670–671 (= Math. USSR – Izvestija **32** (1989), no. 3, 523–541).
75. V. A. Kolyvagin, *The Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 6, 1154–1180, 1327; (= Math. USSR – Izvestija **33** (1989), no. 3, 473–499).
76. G. Kramarz, *All congruent numbers less than* 2000, Math. Ann. **273** (1986), 337–340.
77. K. Kramer, *A family of semistable elliptic curves with large Tate-Shafarevitch groups*, Proc. Amer. Math. Soc. **89** (1983), 379–386.
78. S. Lang, Elliptic curves: Diophantine analysis, Grundlehren der Mathematischen Wissenschaften **231**, Springer-Verlag, Berlin-New York, 1978.

79. S. Lang, *Old and new conjectured Diophantine inequalities*, Bull. Amer. Math. Soc. **23** (1990), 37–75.
80. S. Lang, *Die abc-Vermutung*, Elem. Math. **48** (1993), no. 3, 89–99.
81. A. I. Lapin, *Subfields of hyperelliptic fields. I*, Izv. Akad. Nauk SSSR Ser. Mat. **28** (1964), 953–988 (= Amer. Math. Soc. Transl. (2) **69** (1968), 204–240).
82. A. I. Lapin, *On the rational points of an elliptic curve*, Izv. Akad. Nauk SSSR Ser. Mat. **29** (1965), 701–716 (= Amer. Math. Soc. Transl. (2) **66** (1968), 231–245).
83. M. Levin, *On the group of rational points on elliptic curves over function fields*, Amer. J. Math. **90** (1968), 456–462.
84. E. Lutz, *Sur l'equation $y^2 = x^3 - Ax - B$ dans les corps p-adic*, J. Reine Angew. Math. **177** (1937), 238–247.
85. L. Mai, *The average analytic rank of a family of elliptic curves*, J. Number Theory **45** (1993), no. 1, 45–60.
86. L. Mai, *The analytic rank of a family of elliptic curves*, Canad. J. Math. **45** (1993), no. 4, 847–862.
87. L. Mai, M. R. Murty, *A note on quadratic twists of an elliptic curve*, in Elliptic curves and related topics, 121–124, CRM Proc. Lecture Notes **4**, Amer. Math. Soc., Providence, RI, 1994.
88. Y. Manin, *The p-torsion of elliptic curves is uniformly bounded*, Izv. Akad. Nauk SSSR Ser. Mat. **33** (1969), 459–465 (= Math. USSR – Izvestija **3** (1969), 433–438).
89. Y. Manin, *Cyclotomic fields and modular curves*, Uspehi Mat. Nauk **26** (1971), no. 6 (162), 7–71.
90. Y. Manin, *Parabolic points and ζ-functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat. **6** (1972), 19–66 (= Math. USSR – Izvestija **6** (1972), no. 1, 19–64).
91. R. Martin, W. McMillen, posting to Number Theory server, March 16, 1998.
92. R. Martin, W. McMillen, posting to Number Theory server, May 2, 2000.
93. R. C. Mason, Diophantine equations over function fields, London Math. Soc. Lecture Note Ser. **96**, Cambridge Univ. Press, Cambridge-New York, 1984.
94. B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.
95. B. Mazur, *Rational points on modular curves*, in Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), 107–148, Lecture Notes in Math. **601**, Springer, Berlin, 1977.
96. B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. math. IHES **47** (1977), 33–186.
97. B. Mazur, *Number theory as Gadfly*, Amer. Math. Monthly **98** (1991), no. 7, 593–610.
98. B. Mazur, *Three lectures about the arithmetic of elliptic curves*, lecture notes for the Arizona Winter School Workshop on Diophantine Geometry Related to the ABC Conjecture, 1998.
99. L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. math. **124** (1996), 437–449.
100. J-F. Mestre, *Courbes elliptiques de rang ≥ 11 sur $\mathbf{Q}(t)$*, C. R. Acad. Sci. Paris, **313** (1991), no. 3, 139–142.
101. J-F. Mestre, J. Oesterlé, *Courbes de Weil semi-stables de discriminant une puissance m-iéme*, J. Reine Angew. Math. **400** (1989), 173–184.

102. J. S. Milne, *The Tate-Safarevič group of a constant abelian variety*, Invent. Math. **6** (1968), 91–105.
103. J. S. Milne, *On a conjecture of Artin and Tate*, Ann. of Math. (2) **102** (1975), no. 3, 517–533.
104. J. S. Milne, *Comparison of the Brauer group with the Tate-Safarevič group*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1982), no. 3, 735–743.
105. P. Monsky, *Mock Heegner points and congruent numbers*, Math. Z. **204** (1990), no. 1, 45–67.
106. P. Monsky, *Generalizing the Birch-Stephens theorem. I. Modular curves*, Math. Z. **221** (1996), no. 3, 415–420.
107. M. R. Murty, V. K. Murty, *Mean values of derivatives of modular L-series*, Ann. of Math. (2) **133** (1991), no. 3, 447–475.
108. V. K. Murty, Modular elliptic curves, in Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994), 1–38, CMS Conf. Proc. **17**, Amer. Math. Soc., Providence, RI, 1995.
109. K. Nagao, *An example of elliptic curve over $\mathbf{Q}(T)$ with rank ≥ 13*, Proc. Japan Acad. Ser. A Math. Sci. **70** (1994), no. 5, 152–153.
110. T. Nagell, *Solution de quelque problèmes dans la théorie arithmétique des cubiques planes du premier genre*, Wid. Akad. Skrifter Oslo I (1935), No. 1, 1–25.
111. J. Nekovář, *Beĭlinson's conjectures*, in Motives (Seattle, WA, 1991), 377–400, Proc. Sympos. Pure Math. **55**, Part 1, Amer. Math. Soc., Providence, RI, 1994.
112. A. Néron, *Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps*, Bull. Soc. Math. France **80**, (1952), 101–166.
113. A. Nitaj, *Aspects expérimentaux de la conjecture abc*, in Number theory (Paris, 1993–1994), 145–156, London Math. Soc. Lecture Note Ser. **235**, Cambridge Univ. Press, Cambridge, 1996.
114. A. Nitaj, *La conjecture abc*, Enseign. Math. (2) **42** (1996), no. 1-2, 3–24.
115. A. Nitaj, *Détermination de courbes elliptiques pour la conjecture de Szpiro*, Acta Arith. **85** (1998), no. 4, 351–376.
116. A. Nitaj, *Invariants des courbes de Frey-Hellegouarch et grandes groupes de Tate-Shafarevich*, to appear in Acta Arith., `http://www.math.uiuc.edu/Algebraic-Number-Theory/0190/index.html` .
117. J. Oesterlé, *Nouvelles approches du "théorème" de Fermat*, Séminaire Bourbaki, Vol. 1987/88, Exp. No. 694, Astérisque **161-162** (1988), 4, 165–186.
118. A. P. Ogg, *Cohomology of abelian varieties over function fields*, Ann. of Math. **76** (1962), 185–212.
119. K. Ono, C. Skinner, *Non-vanishing of quadratic twists of modular L-functions*, Invent. math. **134** (1998), no. 3, 651–660.
120. T. Ooe, J. Top, *On the Mordell-Weil rank of an abelian variety over a number field*, J. Pure Appl. Algebra **58** (1989), no. 3, 261–265.
121. P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, J. Reine Angew. Math. **506** (1999), 85–116.
122. P. Parent, *Torsion des courbes elliptiques sur les corps cubiques*, preprint, 28 janvier, 1999.
123. B. Poonen, M. Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. **150** (1999), no. 3, 1109–1149.

124. M. Rapoport, N. Schappacher, P. Schneider (eds.), Beilinson's conjectures on special values of L-functions, Perspectives in Mathematics **4**, Academic Press, Inc., Boston, MA, 1988.
125. K. Ribet, *Abelian varieties over* $\mathbf{Q}$ *and modular forms*, in Algebra and topology 1992 (Taejon), 53–79, Korea Adv. Inst. Sci. Tech., Taejon, 1992.
126. N. F. Rogers, *Rank computations for the congruent number elliptic curves*, to appear in Experiment. Math.
127. K. Rubin, *Local units, elliptic units, Heegner points and elliptic curves*, Invent. Math. **88** (1987), no. 2, 405–422.
128. K. Rubin, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. **89** (1987), no. 3, 527–559.
129. K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), 25–68.
130. K. Rubin, A. Silverberg, *Ranks of elliptic curves in families of quadratic twists*, to appear in Experiment. Math.
131. N. Schappacher, R. Schoof, *Beppo Levi and the arithmetic of elliptic curves*, Math. Intelligencer **18** (1996), no. 1, 57–69.
132. P. Schneider, *Zur Vermutung von Birch und Swinnerton-Dyer über globalen Funktionenkörpern*, Math. Ann. **260** (1982), no. 4, 495–510.
133. U. Schneiders, H. G. Zimmer, *The rank of elliptic curves upon quadratic extension*, in Computational number theory (Debrecen, 1989), 239–260, de Gruyter, Berlin, 1991.
134. E. S. Selmer, *A conjecture concerning rational points on cubic curves*, Math. Scand. **2** (1954), 49–54.
135. P. Serf, *Congruent numbers and elliptic curves*, in Computational number theory (Debrecen, 1989), 227–238, de Gruyter, Berlin, 1991.
136. J-P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230.
137. J-P. Serre, Lectures on the Mordell-Weil Theorem, Friedr. Vieweg & Sohn, Braunschweig, 1989.
138. J-P. Serre, *Propriétés conjecturales des groupes de Galois motiviques et des reprsentations* ℓ*-adiques*, in Motives (Seattle, WA, 1991), 377–400, Proc. Sympos. Pure Math. **55**, Part 1, Amer. Math. Soc., Providence, RI, 1994.
139. J-P. Serre, J. Tate, *Good reduction of abelian varieties*, Ann. of Math. **88** (1968), 492–517.
140. I. R. Šafarevič, *Principal homogeneous spaces defined over a function field*, Trudy Mat. Inst. Steklov. **64** (1961), 316–346 (= Amer. Math. Soc. Transl. (2) **37** (1964), 85–114).
141. G. Shimura, *Correspondances modulaires et les fonctions* ζ *de courbes algébriques*, J. Math. Soc. Japan **10** (1958), 1–28.
142. G. Shimura, *Sur les intégrales attachées aux formes automorphes*, J. Math. Soc. Japan **11** (1959), 291–311.
143. G. Shimura, *On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields*, Nagoya Math. J. **43** (1971), 199–208.
144. G. Shimura, *On the factors of the jacobian variety of a modular function field*, J. Math. Soc. Japan **25** (1973), 523–544.
145. G. Shimura, *The special values of the zeta functions associated with cusp forms*, Comm. Pure Appl. Math. **29** (1976), no. 6, 783–804.

146. G. Shimura, *On the periods of modular forms*, Math. Ann. **229** (1977), no. 3, 211–221.
147. G. Shimura, *Yutaka Taniyama and his time. Very personal recollections*, Bull. London Math. Soc. **21** (1989), no. 2, 186–196.
148. G. Shimura, Introduction to the arithmetic theory of automorphic functions, Reprint of the 1971 original, Publications of the Math. Soc. Japan **11**, Kanô Memorial Lectures **1**, Princeton Univ. Press, Princeton, NJ, 1994.
149. G. Shimura, Abelian varieties with complex multiplication and modular functions, Princeton Mathematical Series **46**, Princeton Univ. Press, Princeton, NJ, 1998.
150. T. Shioda, *An explicit algorithm for computing the Picard number of certain algebraic surfaces*, Amer. J. Math. **108** (1986), no. 2, 415–432.
151. T. Shioda, *Some remarks on elliptic curves over function fields*, Journées Arithmétiques, 1991 (Geneva), Astérisque **209** (1992), 99–114.
152. T. Shioda, *Genus two curves over* $\mathbf{Q}(t)$ *with high rank*, Comment. Math. Univ. St. Paul. **46** (1997), no. 1, 15–21.
153. A. Silverberg, *Torsion points on abelian varieties of CM-type*, Compositio Math. **68** (1988), no. 3, 241–249.
154. A. Silverberg, *Points of finite order on abelian varieties*, in p-adic methods in number theory and algebraic geometry, 175–193, Contemp. Math. **133**, Amer. Math. Soc., Providence, RI, 1992.
155. A. Silverberg, *Galois representations attached to points on Shimura varieties*, in Séminaire de Théorie des Nombres, Paris 1990–91, 221–240, Progress in Mathematics **108**, Birkhäuser, Boston, 1993.
156. Joseph H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 1986.
157. J. H. Silverman, *A quantitative version of Siegel's theorem: integral points on elliptic curves and Catalan curves*, J. Reine Angew. Math. **378** (1987), 60–100.
158. J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Springer-Verlag, New York, 1994.
159. J. Silverman, *On the rank of elliptic curves*, notes from a talk (see his web page: `http://www.math.brown.edu/~jhs/`).
160. Joseph H. Silverman, John Tate, Rational points on elliptic curves, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.
161. N. P. Smart, *S-integral points on elliptic curves*, Math. Proc. Cambridge Philos. Soc. **116** (1994), no. 3, 391–399.
162. N. P. Smart, The algorithmic resolution of Diophantine equations, LMS Student Texts **41**, Cambridge Univ. Press, Cambridge, 1998.
163. N. P. Smart, N. M. Stephens, *Integral points on elliptic curves over number fields*, Math. Proc. Cambridge Philos. Soc. **122** (1997), no. 1, 9–16.
164. N. M. Stephens, *The diophantine equation* $X^3 + Y^3 = DZ^3$ *and the conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. **231** (1968), 121–162.
165. C. L. Stewart, R. Tijdeman, *On the Oesterlé-Masser conjecture*, Monatsh. Math. **102** (1986), no. 3, 251–257.
166. C. L. Stewart, J. Top, *On ranks of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc. **8** (1995), 943–973.

167. C. L. Stewart, K. R. Yu, *On the abc conjecture*, Math. Ann. **291** (1991), no. 2, 225–230.
168. P. F. Stiller, *The Picard numbers of elliptic surfaces with many symmetries*, Pacific J. Math. **128** (1987), no. 1, 157–189.
169. R. J. Stroeker, N. Tzanakis, *Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arith. **67** (1994), no. 2, 177–196.
170. R. J. Stroeker, N. Tzanakis, *On the elliptic logarithm method for elliptic Diophantine equations: reflections and an improvement*, Experiment. Math. **8** (1999), no. 2, 135–149.
171. R. J. Stroeker, B. M. M. de Weger, *Solving elliptic Diophantine equations: the general cubic case*, Acta Arith. **87** (1999), no. 4, 339–365.
172. J. Tate, *Algebraic cycles and poles of zeta functions*, in Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963), 93–110, Harper & Row, New York, 1965.
173. J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 1965/1966, Exp. No. 306 (1966), 26 pp.
174. J. T. Tate, *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206.
175. J. T. Tate, I. R. Šafarevič, *The rank of elliptic curves*, Dokl. Akad. Nauk SSSR **175** (1967), no. 4, 770–773 (= Soviet Math. Dokl. **8** (1967), no. 4, 917–920).
176. R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. **141** (1995), no. 3, 553–572.
177. J. B. Tunnell, *A classical Diophantine problem and modular forms of weight* 3/2, Invent. Math. **72** (1983), no. 2, 323–334.
178. N. Tzanakis, *Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations*, Acta Arith. **75** (1996), no. 2, 165–190.
179. P. Van Mulbregt, *Torsion-points on low-dimensional abelian varieties with complex multiplication*, in p-adic methods in number theory and algebraic geometry, 205–210, Contemp. Math. **133**, Amer. Math. Soc., Providence, RI, 1992.
180. P. Vojta, Diophantine approximations and value distribution theory, Lecture Notes in Math. **1239**, Springer-Verlag, Berlin, 1987.
181. P. Vojta, *A more general ABC conjecture*, lecture notes for the Arizona Winter School Workshop on Diophantine Geometry Related to the ABC Conjecture, 1998.
182. J-L. Waldspurger, *Correspondances de Shimura et quaternions*, Forum Math. **3** (1991), no. 3, 219–307.
183. B. M. M. de Weger, *$A + B = C$ and big Ш's*, Quart. J. Math. Oxford **49** (1998), 105–128.
184. A. Weil, *Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen*, Math. Ann. **168** (1967), 149–156.
185. A. Weil, Œuvres scientifiques, Vol. II (1951–1964), Springer-Verlag, New York-Heidelberg, 1979.
186. A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. **141** (1995), no. 3, 443–551.

187. D. Zagier, *Large integral points on elliptic curves*, Math. Comp. **48** (1987), no. 177, 425–436.
188. D. Zagier, G. Kramarz, *Numerical investigations related to the L-series of certain elliptic curves*, J. Indian Math. Soc. **52** (1987), 51–69.