The Birch and Swinnerton-Dyer Conjecture, a Computational Approach

William A. Stein

Department of Mathematics, University of Washington
E-mail address: wstein@math.washington.edu

1991 *Mathematics Subject Classification.* Primary 11;
Secondary 11-04

Key words and phrases. abelian varieties, computation, elliptic curves, Hecke operators, modular curves, modular forms, modular symbols, Manin symbols, number theory

Abstract.

Contents

Preface

This is an introductory graduate-level textbook about the Birch and Swinnerton-Dyer conjecture and modern approaches to the arithmetic of elliptic curves.

Other very relevant books: Darmon's *Rational Points on Modular Elliptic Curves*.

Acknowledgements. I would like to acknowledge the partial support of NSF Grant DMS 05-55776.

Notation and Conventions.

Chapter 1

The BSD Rank Conjecture

This chapter explains the conjecture that Birch and Swinnerton-Dyer made about ranks of elliptic curves (the BSD rank conjecture).

1.1. Statement of the BSD Rank Conjecture

An excellent reference for this section is Andrew Wiles's Clay Math Institute paper [**Wil00**]. The reader is also strongly encouraged to look Birch's original paper [**Bir71**] to get a better sense of the excitement surrounding this conjecture, as exemplified in the following quote:

> "I want to describe some computations undertaken by myself and Swinnerton-Dyer on EDSAC by which we have calculated the zeta-functions of certain elliptic curves. As a result of these computations we have found an analogue for an elliptic curve of the Tamagawa number of an algebraic group; and conjectures (due to ourselves, due to Tate, and due to others) have proliferated."

An *elliptic curve* E over a field K is the projective closure of the zero locus of a nonsingular affine curve

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.1.1}$$

where $a_1, a_2, a_3, a_4, a_6 \in K$. There is a simple algebraic condition on the a_i that ensures that (1.1.1) defines a nonsingular curve (see, e.g., [**Sil92**]).

An elliptic curve E has genus 1, and the set of points on E has a natural structure of *abelian group*, with identity element the one extra projective

point at ∞. Again, there are simple algebraic formulas that, given two points P and Q on an elliptic curve, produce a third point $P+Q$ on the elliptic curve. Moreover, if P and Q both have coordinates in K, then so does $P+Q$. The *Mordell-Weil group*

$$E(K) = \{ \text{ points on } E \text{ with coordinates in } K \ \}$$

of E over K plays a central role in this book.

In the 1920s, Mordell proved that if $K = \mathbb{Q}$, then $E(\mathbb{Q})$ is finitely generated, and soon after Weil proved that $E(K)$ is finitely generated for any number field K, so

$$E(K) \approx \mathbb{Z}^r \oplus T, \tag{1.1.2}$$

where T is a finite group. Perhaps the chief invariant of an elliptic curve E over a number field K is the *rank*, which is the number r in (1.1.2).

Fix an elliptic curve E over $\mathbb{Q}$. For all but finitely many prime numbers p, the equation (1.1.1) reduces modulo p to define an elliptic curve over the finite field $\mathbb{F}_p$. The primes that must be excluded are exactly the primes that divide the discriminant Δ of (1.1.1).

As above, the set of points $E(\mathbb{F}_p)$ is an abelian group. This group is finite, because it is contained in the set $\mathbb{P}^2(\mathbb{F}_p)$ of rational points in the projective plane. Moreover, since it is the set of points on a (genus 1) curve, a theorem of Hasse implies that

$$|p + 1 - \#E(\mathbb{F}_p)| \leq 2\sqrt{p}.$$

The error terms

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

play a central role in almost everything in this book. We next gather together the error terms into a single "generating function":

$$\tilde{L}(E, s) = \prod_{p \nmid \Delta} \left(\frac{1}{1 - a_p p^{-s} + p^{1-2s}} \right).$$

The function $\tilde{L}(E, s)$ defines a complex analytic function on some right half plane $\mathrm{Re}(s) > \frac{3}{2}$.

A deep theorem of Wiles et al. [**Wil95, BCDT01**], which many consider the crowning achievement of 1990s number theory, implies that $\tilde{L}(E, s)$ can be analytically continued to an analytic function on all $\mathbb{C}$. This implies that $\tilde{L}(E, s)$ has a Taylor series expansion about $s = 1$:

$$\tilde{L}(E, s) = c_0 + c_1(s-1) + c_2(s-1)^2 + \cdots$$

Define the *analytic rank* r_{an} of E to be the order of vanishing of $\tilde{L}(E, s)$ as $s = 1$, so

$$\tilde{L}(E, s) = c_{r_{\mathrm{an}}}(s-1)^{r_{\mathrm{an}}} + \cdots .$$

The definitions of the analytic and Mordell-Weil ranks could not be more different – one is completely analytic and the other is purely algebraic.

Conjecture 1.1 (Birch and Swinnerton-Dyer Rank Conjecture)**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then the algebraic and analytic ranks of E are the same.*

This problem is extremely difficult. The conjecture was made in the 1960s, and hundreds of people have thought about it for over 4 decades. The work of Wiles et al. on modularity in late 1999, combined with earlier work of Gross, Zagier, and Kolyvagin, and many others proves the following partial result toward the conjecture.

Theorem 1.2. *Suppose E is an elliptic curve over $\mathbb{Q}$ and that $r_{\text{an}} \leq 1$. Then the algebraic and analytic ranks of E are the same.*

In 2000, Conjecture 1.1 was declared a million dollar millenium prize problem by the Clay Mathematics Institute, which motivated even more work, conferences, etc., on the conjecture. Since then, to the best of my knowledge, not a single new result directly about Conjecture 1.1 has been proved[1]. The class of curves for which we know the conjecture is still the set of curves over $\mathbb{Q}$ with $r_{\text{an}} \leq 1$, along with a finite set of individual curves on which further computer calculations have been performed (by Cremona, Watkins, myself, and others).

> *"A new idea is needed."*
> – Nick Katz on BSD, at a 2001 Arizona Winter School

And another quote from Bertolini-Darmon (2001):

> "The following question stands as the ultimate challenge concerning the Birch and Swinnerton-Dyer conjecture for elliptic curves over $\mathbb{Q}$: *Provide evidence for the Birch and Swinnerton-Dyer conjecture in cases where* $\text{ord}_{s=1} L(E, s) > 1$."

1.2. The BSD Rank Conjecture Implies that $E(\mathbb{Q})$ is Computable

Proposition 1.3. *Let E be an elliptic curve over $\mathbb{Q}$. If Conjecture 1.1 is true, then there is an algorithm to compute the rank of E.*

Proof. By naively searching for points in $E(\mathbb{Q})$ we obtain a lower bound on r, which is closer and closer to the true rank r, the longer we run the search. At some point this lower bound will equal r, but without using further information we do not know when that will occur.

[1] Much interesting new work has been done on related conjectures and problems.

As explained, e.g., in [**Cre97**] (see also [**Dok04**]), we can for any k compute $L^{(k)}(E,1)$ to any desired precision. Such computations yield upper bounds on r_{an}. In particular, if we compute $L^{(k)}(E,1)$ and it is nonzero (to the precision of our computation), then $r_{\text{an}} \leq k$. Eventually this method will also converge to give an upper bound on r_{an}, though again without further information we do not know when our computed upper bound on r_{an} equals to the true value of r_{an}.

Since we are assuming that Conjecture 1.1 is true, we know that $r = r_{\text{an}}$, hence at some point the lower bound on r computed using point searches will equal the upper bound on r_{an} computed using the L-series. At this point, by Conjecture 1.1, we know the true value of r. □

Next we show that given the rank r, the full group $E(\mathbb{Q})$ is computable. The issue is that what we did above might have only computed a subgroup of finite index. The argument below follows [**Cre97**, §3.5] closely.

The *naive height* $h(P)$ of a point $P = (x,y) \in E(\mathbb{Q})$ is

$$h(P) = \log(\max(\text{numer}(x), \text{denom}(x))).$$

The *Néron-Tate canonical height* of P is

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

Note that if P has finite order then $\hat{h}(P) = 0$. Also, a standard result is that the *height pairing*

$$\langle P, Q\rangle = \frac{1}{2}\left(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)\right)$$

defines a nondegenerate real-valued quadratic form on $E(\mathbb{Q})/_{\text{tor}}$ with discrete image.

Lemma 1.4. *Let $B > 0$ be a positive real number such that*

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

contains a set of generators for $E(\mathbb{Q})/2E(\mathbb{Q})$. Then S generates $E(\mathbb{Q})$.

Proof. Let A be the subgroup of $E(\mathbb{Q})/_{\text{tor}}$ generated by the points in S. Suppose for the sake of contradiction that A is a proper subgroup. Then there is $Q \in E(\mathbb{Q}) \setminus A$ with $\hat{h}(Q)$ minimal, since $\hat{h}$ takes a discrete set of values. Since S contains generators for $E(\mathbb{Q})/2E(\mathbb{Q})$, there is an element $P \in S$ that is congruent to Q modulo $2E(\mathbb{Q})$, i.e., so that

$$Q = P + 2R,$$

for some $R \in E(\mathbb{Q})$. We have $R \notin A$ (since otherwise Q would be in A), so $\hat{h}(R) \geq \hat{h}(Q)$ by minimality. Finally, since $\hat{h}$ is quadratic and nonnegative,

we have

$$\begin{aligned}\hat{h}(P) &= \frac{1}{2}\left(\hat{h}(Q+P)+\hat{h}(Q-P)-\hat{h}(Q)\right)\\ &\geq \frac{1}{2}\hat{h}(2R)-\hat{h}(Q)\\ &= 2\hat{h}(R)-\hat{h}(Q) \geq \hat{h}(Q) > B.\end{aligned}$$

(Here we use that $\hat{h}(P) = \langle P, P\rangle$ and use properties of a bilinear form.) □

Proposition 1.5. *Let E be an elliptic curve over $\mathbb{Q}$. If Conjecture 1.1 is true, then there is an algorithm to compute $E(\mathbb{Q})$.*

Proof. By Proposition 1.3 we can compute the rank r of $E(\mathbb{Q})$. Note that we can also trivially compute the subgroup $E(\mathbb{Q})[2]$ of elements of order 2 in $E(\mathbb{Q})$, since if E is given by $y^2 = x^3+ax+b$, then this subgroup is generated by points (α, β), where α is a rational root of $x^3 + ax + b$. Thus we can compute $s = \dim_{\mathbb{F}_2} E(\mathbb{Q})/2E(\mathbb{Q})$, since it is equal to $r + \dim E(\mathbb{Q})[2]$.

Run any search for points in $E(\mathbb{Q})$ and use that $\hat{h}$ is a nondegenerate quadratic form to find independent points $P_1, \ldots, P_r$ of infinite order. It is easy to check whether a point P is twice another point (just solve a relatively simple algebraic equation). Run through all subsets of the points P_i, and if any subset of the P_i sums to $2Q$ for some point $Q \in E(\mathbb{Q})$, then we replace one of the P_i by Q and decrease the index of our subgroup in $E(\mathbb{Q})$ by a factor of 2. Because $E(\mathbb{Q})$ is a finitely generated group, after a finite number of steps (and including the 2-torsion points found above) we obtain independent points $P_1, \ldots, P_s$ that generate $E(\mathbb{Q})/2E(\mathbb{Q})$.

Let C the the explicit bound of Cremona-Pricket-Siksek on the difference between the naive and canonical height (i.e., for any $P \in E(\mathbb{Q})$, we have $|h(P) - \hat{h}(P)| < C$). Let

$$B = \max\{\hat{h}(P_1), \ldots, \hat{h}(P_s)\}.$$

Then by a point search up to naive height $B + C$, we compute a set that contains the set S in Lemma 1.4. This set then contains generators for $E(\mathbb{Q})$, hence we have computed $E(\mathbb{Q})$.

□

1.3. The Complex L-series $L(E, s)$

In Section 1.1 we defined a function $\tilde{L}(E, s)$, which encoded information about $E(\mathbb{F}_p)$ for all but finitely many primes p. In this section we define the function $L(E, s)$, which includes information about all primes, and the function $\Lambda(E, s)$ that also includes information "at infinity".

Let E be an elliptic curve over $\mathbb{Q}$ defined by *a minimal Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.3.1}$$

A minimal Weierstrass equation in one for which the a_i are all integers and the discriminant $\Delta \in \mathbb{Z}$ is minimal amongs all discriminants of Weierstrass equations for E (again, see [**Sil92**] for the definition of the discriminant of a Weierstrass equation, and also for an explicit description of the allowed transformations of a Weierstrass equation).

For each prime number $p \nmid \Delta$, the equation (1.3.1) reduces modulo p to define an elliptic $E_{\mathbb{F}_p}$ over the finite field $\mathbb{F}_p$. Let

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

For each prime $p \mid \Delta$, we use the following recipe to define a_p. If the *singular* curve $E_{\mathbb{F}_p}$ has a cuspidal singularity, e.g., is $y^2 = x^3$, then let $a_p = 0$. If it has a a nodal singularity, e.g., like $y^2 = x^3 + x^2$, let $a_p = 1$ if the slope of the tangent line at the singular point is in $\mathbb{F}_p$ and let $a_p = -1$ if the slope is not in $\mathbb{F}_p$. Summarizing:

$$a_p = \begin{cases} 0 & \text{if the reduction is cuspidal (“additive”),} \\ 1 & \text{if the reduction is nodal and tangent line is } \mathbb{F}_p\text{-rational (“split multiplicative”)} \\ -1 & \text{if the reduction is nodal and tangent line is not } \mathbb{F}_p\text{-rational (“non-split multiplicative”} \end{cases}$$

Even in the cases when $p \mid \Delta$, we still have

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

When E has additive reduction, the nonsingular points form a group isomorphic to $(\mathbb{F}_p, +)$, and there is one singular point, hence $p + 1$ points, so

$$a_p = p + 1 - (p + 1))) = 0.$$

When E has split multiplicative reduction, there is 1 singular point plus the number of elements of a group isomorphic to $(\mathbb{F}_p^*, \times)$, so $1 + (p - 1) = p$ points, and

$$a_p = p + 1 - p = 1.$$

When E has non-split multiplicative reduction, there is 1 singular point plus the number of elements of a group isomorphic $(\mathbb{F}_{p^2}^*/\mathbb{F}_p^*, \times)$, i.e., $p+2$ points, and

$$a_p = p + 1 - (p + 2) = -1.$$

The definition of the full L-function of E is then

$$L(E, s) = \prod_{p|\Delta} \frac{1}{1 - a_p p^{-s}} \cdot \prod_{p\nmid\Delta} \frac{1}{1 - a_p p^{-s} + p \cdot p^{-2s}}. = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

If in addition we add in a few more analytic factors to the L-function we obtain a function $\Lambda(E, s)$ that satisfies a remarkably simple functional equation. Let

$$\Gamma(z) = \int_0^\infty t^{z-1} e^{-t} dt$$

be the Γ-*function* (e.g., $\Gamma(n) = (n-1)!$), which defines a meromorphic function on $\mathbb{C}$, with poles at the non-positive integers.

Theorem 1.6 (Hecke, Wiles et al.)**.** *There is a unique positive integer $N = N_E$ and sign $\varepsilon = \varepsilon_E \in \{\pm 1\}$ such that the function*

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

extends to a complex analytic function on all $\mathbb{C}$ that satisfies the functional equation

$$\Lambda(E, 2-s) = \varepsilon \cdot \Lambda(E, s), \tag{1.3.2}$$

for all $s \in \mathbb{C}$.

Proof. Wiles et al. prove that $L(E, s)$ is the L-series attached to a modular form (see Section **??** below), and Hecke proved that the L-series of a modular form analytically continues and satisfies the given functional equation. □

The integer $N = N_E$ is called the *conductor* of E and $\varepsilon = \varepsilon_E$ is called the *sign in the functional equation* for E or the *root number* of E. One can prove that the primes that divide N are the same as the primes that divide Δ. Moreover, for $p \geq 5$, we have that

$$\mathrm{ord}_p(N) = \begin{cases} 0, & \text{if } p \nmid \Delta, \\ 1, & \text{if } E \text{ has multiplicative reduction at } p, \text{ and} \\ 2, & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

There is a geometric algorithm called Tate's algorithm that computes N in all cases and ε.

Example 1.7. Consider the elliptic curve E defined by

$$y^2 + y = x^3 + 50x + 31.$$

The above Weierstrass equation is minimal and has discriminant

$$-1 \cdot 5^6 \cdot 7^2 \cdot 11.$$

```
sage: e = EllipticCurve('1925d'); e
Elliptic Curve defined by y^2 + y = x^3 + 50*x + 31 over Rational Field
sage: e.is_minimal()
True
sage: factor(e.discriminant())
-1 * 5^6 * 7^2 * 11
```

At 5 the curve has additive reduction so $a_5 = 0$. At 7 the curve has split multiplicative reduction so $a_7 = 1$. At 11 the curve has nonsplit multiplicative reduction, so $a_{11} = -1$. Counting points for $p = 2, 3$, we find that

$$L(E,s) = \frac{1}{1^{-s}} + \frac{3}{3^{-s}} + \frac{-2}{4^{-s}} + \frac{1}{7^{-s}} + \frac{6}{9^{-s}} + \frac{-1}{11^{-s}} + \frac{-6}{12^{-s}} + \cdots$$

```
sage: [e.ap(p) for p in primes(14)]
[0, 3, 0, 1, -1, 4]
```

Corollary 1.8. *Let E be an elliptic curve over $\mathbb{Q}$, let $\varepsilon \in \{1, -1\}$ be the sign in the functional equation* (1.3.2)*, and let $r_{E,\mathrm{an}} = \mathrm{ord}_{s=1} L(E,s)$. Then*

$$\varepsilon = (-1)^{r_{E,\mathrm{an}}}.$$

Proof. Because $\Gamma(1) = 1$, we have $\mathrm{ord}_{s=1} L(E,s) = \mathrm{ord}_{s=1} \Lambda(E,s)$. It thus sufficies to prove the corollary with $L(E,s)$ replaced by $\Lambda(E,s)$. Note that $r = r_{E,\mathrm{an}}$ is the minimal integer $r \geq 0$ such that $\Lambda^{(r)}(E,1) \neq 0$. By repeated differentiation, we see that for any integer $k \geq 0$, we have

$$(-1)^k \Lambda^{(k)}(E, 2-s) = \varepsilon \cdot \Lambda^{(k)}(s). \tag{1.3.3}$$

Setting $s = 1$ and $k = r$, and using that $\Lambda^{(r)}(E,1) \neq 0$, shows that $(-1)^r = \varepsilon$, as claimed. □

Conjecture 1.9 (The Parity Conjecture)**.** *Let E be an elliptic curve over $\mathbb{Q}$, let $r_{E,\mathrm{an}}$ be the analytic rank and $r_{E,\mathrm{alg}}$ be the algebraic rank. Then*

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

Jan Nekovar has done a huge amount of work toward Conjecture 1.9; in particular, he proves it under the (as yet unproved) hypothesis that Ш(E) is finite (see Section 2.2 below).

1.4. Computing $L(E,s)$

In this section we briefly describe one way to evaluate $L(E,s)$, for s real. See [**Dok04**] for a more sophisticated analysis of computing $L(E,s)$ and its Taylor expansion for any complex number s.

Theorem 1.10 (Lavrik)**.** *We have the following rapidly-converging series expression for $L(E, s)$, for any complex number s:*

$$L(E,s) = N^{-s/2} \cdot (2\pi)^s \cdot \Gamma(s)^{-1} \cdot \sum_{n=1}^{\infty} a_n \cdot (F_n(s-1) - \varepsilon F_n(1-s))$$

where

$$F_n(t) = \Gamma\left(t+1, \frac{2\pi n}{\sqrt{N}}\right) \cdot \left(\frac{\sqrt{N}}{2\pi n}\right)^{t+1},$$

and

$$\Gamma(z,\alpha) = \int_{\alpha}^{\infty} t^{z-1} e^{-t} dt$$

is the incomplete Γ-function*.*

Theorem 1.10 above is a special case of a more general theorem that gives rapidly converging series that allow computation of any Dirichlet series $\sum a_n n^s$ that meromorphically continues to the whole complex plane and satisfies an appropriate functional equation. For more details, see [**Coh00**, §10.3], especially Exercise 24 on page 521 of [**Coh00**].

1.4.1. Approximating the Rank. Fix an elliptic curve E over $\mathbb{Q}$. The usual method to *approximate* the rank is to find a series that rapidly converges to $L^{(r)}(E, 1)$ for $r = 0, 1, 2, 3, \ldots$, then compute $L(E, 1)$, $L'(E, 1)$, $L^{(2)}(E, 1)$, etc., until one appears to be nonzero. Note that half of the $L^{(k)}(E, 1)$ are automatically 0 because of equation (1.3.3). For more details, see [**Cre97**, §2.13] and [**Dok04**].

In this section, we describe a slightly different method, which only uses Theorem 1.10 and the definition of the derivative.

Proposition 1.11. *Write*

$$L(E,s) = c_r(s-1)^r + c_{r+1}(s-1)^{r+1} + \cdots.$$

with $c_r \neq 0$. Then

$$\lim_{s\to 1} (s-1) \cdot \frac{L'(E,s)}{L(E,s)} = r.$$

Proof. Setting $L(s) = L(E, s)$, we have

$$\begin{aligned}
\lim_{s\to 1} (s-1) \cdot \frac{L'(s)}{L(s)} &= \lim_{s\to 1} (s-1) \cdot \frac{rc_r(s-1)^{r-1} + (r+1)c_{r+1}(s-1)^r + \cdots}{c_r(s-1)^r + c_{r+1}(s-1)^{r+1} + \cdots} \\
&= r \cdot \lim_{s\to 1} \frac{c_r(s-1)^r + \frac{(r+1)}{r}c_{r+1}(s-1)^{r+1} + \cdots}{c_r(s-1)^r + c_{r+1}(s-1)^{r+1} + \cdots} \\
&= r.
\end{aligned}$$

□

Thus the rank r is the limit as $s \to 1$ of a certain (smooth) function. We know this limit is an integer. But, for example, for the rank 4 curve

$$y^2 + xy = x^3 - x^2 - 79x + 289 \tag{1.4.1}$$

of conductor 234446 nobody has succeeded in proving that this integer limit is 4. (We can prove that the limit is either 2 or 4 by using the functionality equation (1.3.2) to show that the order of vanishing is even, then verifying by computation that $L^{(4)}(E, 1) = 214.65233\ldots \neq 0$.)

Using the definition of derivative, we approximate $(s-1)\frac{L'(s)}{L(s)}$ as follows. For $|s-1|$ small, we have

$$\begin{aligned}(s-1)\frac{L'(s)}{L(s)} &= \frac{s-1}{L(s)} \cdot \lim_{h\to 0} \frac{L(s+h) - L(s)}{h} \\ &\approx \frac{s-1}{L(s)} \cdot \frac{L(s+(s-1)^2) - L(s)}{(s-1)^2} \\ &= \frac{L(s^2 - s + 1) - L(s)}{(s-1)L(s)}\end{aligned}$$

In fact, we have

$$\lim_{s\to 1} (s-1) \cdot \frac{L'(s)}{L(s)} = \lim_{s\to 1} \frac{L(s^2 - s + 1) - L(s)}{(s-1)L(s)}.$$

We can use this formula in SAGE to "approximate" r. First we start with a curve of rank 2.

```
sage: e = EllipticCurve('389a'); e.rank()
2
sage: L = e.Lseries_dokchitser()
sage: def r(e,s): L1=L(s); L2=L(s^2-s+1); return (L2-L1)/((s-1)*L1)
sage: r(e,1.01)
2.00413534247395
sage: r(e,1.001)
2.00043133754756
sage: r(e,1.00001)
2.00000433133371
```

Next consider the curve $y^2 + xy = x^3 - x^2 - 79x + 289$ of rank 4:

```
sage: e =  EllipticCurve([1, -1, 0, -79, 289])
sage: e.rank()
4
sage: L = e.Lseries_dokchitser(100)
sage: def r(e,s): L1=L(s); L2=L(s^2-s+1); return (L2-L1)/((s-1)*L1)
sage: R = RealField(100)
sage: r(e,R('1.01'))
4.0212949184444018810727106489
sage: r(e,R('1.001'))
4.0022223745190806421850637523
sage: r(e,R('1.00001'))
4.0000223250026401574120263050
sage: r(e,R('1.000001'))
4.0000022325922257758141597819
```

It certainly looks like $\lim_{s\to 1} r(s) = 4$. We know that $\lim_{s\to 1} r(s) \in \mathbb{Z}$, and if only there were a good way to bound the error we could conclude that the limit is 4. But this has stumped people for years, and probably it is nearly impossible without a deep result that somehow interprets $L''(E, 1)$ in a completely different way.

1.5. The p-adic $\mathcal{L}$-series

Fix[2] an elliptic curve E defined over $\mathbb{Q}$. We say a prime p is a prime of *good ordinary reduction* for E if $p \nmid N_E$ and $a_p \not\equiv 0 \pmod{p}$. The Hasse bound, i.e., that $|a_p| < 2\sqrt{p}$ on implies that if $p \geq 5$ then ordinary at p is the same as $a_p \neq 0$.

In this section, we define for each odd prime number p of good ordinary reduction for E a p-adic L-function $L_p(E, T)$. This is a p-adic analogue of the complex L-function $L(E, s)$ about which there are similar analogue of the BSD conjecture.

1.5.1. Hensel's lemma and the Teichmuller lift. The following standard lemma is proved by Newton iteration.

Lemma 1.12 (Hensel)**.** *If $f \in \mathbb{Z}_p[x]$ is a polynomial and $\beta \in \mathbb{Z}/p\mathbb{Z}$ is a multiplicity one root of $\overline{f}$, then there is a unique lift of β to a root of f.*

For example, consider the polynomial $f(x) = x^{p-1} - 1$. By Fermat's little theorem, it has $p-1$ distinct roots in $\mathbb{Z}/p\mathbb{Z}$, so by Lemma 1.12 there are $p-1$ roots of $f(x)$ in $\mathbb{Z}_p$, i.e., all the $p-1$st roots of unity are elements of $\mathbb{Z}_p$. The *Teichmuller lift* is the map that sends any $\beta \in (\mathbb{Z}/p\mathbb{Z})^*$ to the unique $(p-1)$st root of unity in $\mathbb{Z}_p^*$ that reduces to it.

The *Teichmuller character* is the homomorphism

$$\tau : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$$

obtained by first reducing modulo p, then sending an element to its Teichmuller lift. The 1-*unit projection* character is the homomorphism

$$\langle \bullet \rangle : \mathbb{Z}_p^* \to 1 + p\mathbb{Z}_p$$

given by

$$\langle x \rangle = \frac{x}{\tau(x)}.$$

1.5.2. Modular Symbol and Measures. Let

$$f_E(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z} \in S_2(\Gamma_0(N))$$

be the modular form associated to E, which is a holomorphic function on the extended upper half plane $\mathfrak{h} \cup \mathbb{Q} \cup \{\infty\}$. Let

$$\Omega_E = \int_{E(\mathbb{R})} \frac{dx}{2y + \underline{a}_1 x + \underline{a}_3} \in \mathbb{R}$$

[2]This section is based on correspondence with Robert Pollack and Koopa Koo.

be the real period associated to a minimal Weierstrass equation

$$y^2 + \underline{a}_1 xy + \underline{a}_3 y = x^3 + \underline{a}_2 x^2 + \underline{a}_4 x + \underline{a}_6$$

for E.

The *plus modular symbol map* associated to the elliptic curve E is the map $\mathbb{Q} \to \mathbb{Q}$ given by sending $r \in \mathbb{Q}$ to

$$[r] = [r]_E = \frac{2\pi i}{\Omega_E}\left(\int_r^{i\infty} f_E(z)dz + \int_{-r}^{i\infty} f_E(z)dz\right).$$

Question 1.13. Let E vary over all elliptic curve over $\mathbb{Q}$ and r over all rational numbers. Is the set of denominators of the rational numbers $[r]_E$ bounded? Thoughts: For a given curve E, the denominators are bounded by the order of the image in $E(\overline{\mathbb{Q}})$ of the cuspidal subgroup of $J_0(N)(\overline{\mathbb{Q}})$. It is likely one can show that if a prime ℓ divides the order of the image of this subgroup, then E admits a rational ℓ-isogeny. Mazur's theorem would then prove that the set of such ℓ is bounded, which would imply a "yes" answer to this question. Also, for any particular curve E, one can compute the cuspidal subgroup precisely, and hence bound the denominators of $[r]_E$.

Let a_p be the pth Fourier coefficient of E and note that the polynomial

$$x^2 - a_p x + p \equiv x(x - a_p) \pmod{p}$$

has distinct roots because p is an ordinary prime. Let α be the root of $x^2 - a_p x + p$ with $|\alpha|_p = 1$, i.e., the lift of the root a_p modulo p, which exists by Lemma 1.12.

Define a *measure on* $\mathbb{Z}_p^*$ by

$$\mu_E(a + p^n\mathbb{Z}_p) = \frac{1}{\alpha^n}\left[\frac{a}{p^n}\right] - \frac{1}{\alpha^{n+1}}\left[\frac{a}{p^{n-1}}\right].$$

That μ_E is a measure follows from the formula for the action of Hecke operators on modular symbols and that f_E is a Hecke eigenform. We will not prove this here[3].

1.5.3. The p-Adic L-function. Define the p-adic L-function as a function on characters

$$\chi \in \mathrm{Hom}(\mathbb{Z}_p^*, \mathbb{C}_p^*)$$

as follows. Send a character χ to

$$L_p(E, \chi) = \int_{\mathbb{Z}_p^*} \chi \, d\mu_E.$$

We will later make the integral on the right more precise, as a limit of Riemann sums (see Section 1.6).

[3]Add proof or good reference.

Remark 1.14. For any Dirichlet character $\chi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$, let $L(E, \chi, s)$ be the entire L-function defined by the Dirichlet series

$$\sum_{n=1}^{\infty} \frac{\chi(n) a_n}{n^s}.$$

The standard *interpolation property* of L_p is that for any primitive Dirichlet character χ of conductor p^n (for any n), we have[4]

$$L_p(E, \chi) = \begin{cases} p^n \cdot g(\chi) \cdot L(E, \bar{\chi}, 1)/\Omega_E & \text{for } \chi \neq 1, \\ (1 - \alpha^{-1})^2 L(E, 1)/\Omega_E & \text{if } \chi = 1, \end{cases} \tag{1.5.1}$$

where $g(\chi)$ is the Gauss sum:

$$g(\chi) = \sum_{a \mod p^n} \chi(a) e^{\frac{2\pi i a}{p^n}}.$$

Note, in particular, that $L(E, 1) \neq 0$ if and only if $L_p(E, 1) \neq 0$.

In order to obtain a Taylor series attached to L_p, we view L_p as a p-adic analytic function on the open disk

$$D = \{u \in \mathbb{C}_p \,:\, |u - 1|_p < 1\},$$

as follows. We have that $\gamma = 1 + p$ is a topological generator for $1 + p\mathbb{Z}_p$. For any $u \in D$, let $\psi_u : 1 + p\mathbb{Z}_p \to \mathbb{C}_p^*$ be the character given by sending γ to u and extending by using the group law and continuity. Extend ψ_u to a character $\chi_u : \mathbb{Z}_p^* \to \mathbb{C}_p^*$ by letting $\chi_u(x) = \psi_u(\langle x \rangle)$. Finally, overloading notation, let

$$L_p(E, u) = L_p(E, \chi_u).$$

Theorem 1.15. *The function $L_p(E, u)$ is a p-adic analytic function on D with Taylor series about $u = 1$ in the variable T*

$$\mathcal{L}_p(E, T) \in \mathbb{Q}_p[[T]].$$

that converges on $\{z \in \mathbb{C}_p \,:\, |z|_p < 1\}$. (Note that $L_p(E, u) = \mathcal{L}_p(E, u - 1)$.)

It is $\mathcal{L}_p(E, T)$ that we will compute explicitly.

Conjecture 1.16 (Mazur, Tate, Teitelbaum)**.**

$$\operatorname{ord}_T \mathcal{L}_p(E, T) = \operatorname{rank} E(\mathbb{Q}).$$

Proposition 1.17. *Conjecture 1.16 is true if* $\operatorname{ord}_T \mathcal{L}_p(E, T) \leq 1$.

[4] I copied this from Bertolini-Darmon, and I don't trust it exactly yet, especially because the line from Bertolini-Darmon for $\chi = 1$ was wrong.

Sketch of Proof. By Remark 1.14, we have $\operatorname{ord}_T(\mathcal{L}_p(E,T)) = 0$ if and only if

$$r_{E,\mathrm{an}} = \operatorname{ord}_{s=1} L(E,s) = 0.$$

Since the BSD rank conjecture (Conjecture 1.1) is a theorem when $r_{E,\mathrm{an}} = 0$, Conjecture 1.16 is also known under the hypothesis that $\operatorname{ord}_T(\mathcal{L}_p(E,T)) = 0$.

Recall that the BSD rank conjecture is also a theorem when $r_{E,\mathrm{an}} = 1$. It turns out that the same is true of Conjecture 1.16 above. If $\operatorname{ord}_T(\mathcal{L}_p(E,T)) = 1$, then a theorem of Perrin-Riou implies that a certain Heegner point has nonzero p-adic height, hence is non-torsion, so by the Gross-Zagier theorem $r_{E,\mathrm{an}} = 1$. Kolyvagin's theorem then implies that $\operatorname{rank} E(\mathbb{Q}) = 1$. □

Remark 1.18. Mazur, Tate, and Teitelbaum also define an analogue of $\mathcal{L}_p(E,T)$ for primes of bad multiplicative reduction and make a conjecture. A prime p is *supersingular* for E if $a_p \equiv 0 \pmod{p}$; it is a theorem of Elkies [**Elk87**] that for any elliptic curve E there are infinitely many supersingular primes p. Perrin-Riou, Pollack, Greenberg and others have studied $\mathcal{L}_p(E,T)$ at good supersingular primes. More works needs to be done on finding a definition of $\mathcal{L}_p(E,T)$ when p is a prime of bad additive reduction for E.

Remark 1.19. A theorem of Rohrlich implies that there is some character as in (1.5.1) such that $L(E,\chi,1) \neq 0$, so $\mathcal{L}_p(E,T)$ is not identically zero. Thus $\operatorname{ord}_T \mathcal{L}_p(T) < \infty$.

1.6. Computing $\mathcal{L}_p(E,T)$

Fix notation as in Section 1.5. In particular, E is an elliptic curve over $\mathbb{Q}$, p is an odd prime of good ordinary reduction for E, and α is the root of $x^2 - a_p x + p$ with $|\alpha|_p = 1$.

For each integer $n \geq 1$, define a polynomial

$$P_n(T) = \sum_{a=1}^{p-1} \left(\sum_{j=0}^{p^{n-1}-1} \mu_E\left(\tau(a)(1+p)^j + p^n\mathbb{Z}_p\right) \cdot (1+T)^j \right) \in \mathbb{Q}_p[T].$$

Recall that $\tau(a) \in \mathbb{Z}_p^*$ is the Teichmuller lift of a.

Proposition 1.20. *We have that the p-adic limit of these polynomials is the p-adic L-series:*

$$\lim_{n\to\infty} P_n(T) = \mathcal{L}_p(E,T).$$

This convergence is coefficient-by-coefficient, in the sense that if $P_n(T) = \sum_j a_{n,j} T^j$ and $\mathcal{L}_p(E,T) = \sum_j a_j T^j$, then

$$\lim_{n\to\infty} a_{n,j} = a_j.$$

We now give a proof of this convergence and in doing so obtain an upper bound for $|a_j - a_{n,j}|$.

For any choice ζ_r of p^r-th root of unity in $\mathbb{C}_p$, let χ_r be the $\mathbb{C}_p$-valued character of $\mathbb{Z}_p^\times$ of order p^r which factors through $1+p\mathbb{Z}_p$ and sends $1+p$ to ζ_r. Note that the conductor of χ_r is p^{r+1}.

Lemma 1.21. *Let ζ_r be a p^r-th root of unity with $1 \le r \le n-1$, and let χ_r be the corresponding character of order p^{r+1}, as above. Then*

$$P_n(\zeta_r - 1) = \int_{\mathbb{Z}_p^\times} \chi_r \, d\mu_E$$

In particular, note that the right hand side does not depend on n.

Proof. Writing $\chi = \chi_r$, we have

$$\begin{aligned} P_n(\zeta_r - 1) &= \sum_{a=1}^{p-1} \sum_{j=0}^{p^{n-1}-1} \mu_E\left(\tau(a)(1+p)^j + p^n\mathbb{Z}_p\right) \cdot \zeta_r^j \\ &= \sum_{a=1}^{p-1} \sum_{j=0}^{p^{n-1}-1} \mu_E\left(\tau(a)(1+p)^j + p^n\mathbb{Z}_p\right) \cdot \chi\left((1+p)^j\right) \\ &= \sum_{b \in (\mathbb{Z}/p^n\mathbb{Z})^*} \mu_E\left(b + p^n\mathbb{Z}_p\right) \cdot \chi(b) \\ &= \int_{\mathbb{Z}_p^\times} \chi \, d\mu_E. \end{aligned}$$

In the second to the last equality, we use that

$$(\mathbb{Z}/p^n\mathbb{Z})^* \cong (\mathbb{Z}/p\mathbb{Z})^* \times (1 + p(\mathbb{Z}/p^n\mathbb{Z}))^*$$

to sum over lifts of $b \in (\mathbb{Z}/p^n\mathbb{Z})^*$ of the form $\tau(a)(1+p)^j$, i.e., a Teichmuller lift times a power of $(1+p)^j$. In the last equality, we use that χ has conductor p^n, so is constant on the residue classes modulo p^n, i.e., the last equality is just the Riemann sums definition of the given integral.

□

For each positive integer n, let $w_n(T) = (1+T)^{p^n} - 1$.

Corollary 1.22. *We have that*

$$w_{n-1}(T) \text{ divides } P_{n+1}(T) - P_n(T).$$

Proof. By Lemma 1.21, $P_{n+1}(T)$ and $P_n(T)$ agree on $\zeta_j - 1$ for $0 \le j \le n-1$ and any choice ζ_j of p^j-th root of unity, so their difference vanishes on every root of the polynomial $w_{n-1}(T) = (1+T)^{p^{n-1}} - 1$. The claimed divisibility follows, since $w_{n-1}(T)$ has distinct roots. □

Lemma 1.23. *Let $f(T) = \sum_j b_j T^j$ and $g(T) = \sum_j c_j T^j$ be in $\mathcal{O}[T]$ with $\mathcal{O}$ a finite extension of $\mathbb{Z}_p$. If $f(T)$ divides $g(T)$, then*

$$\mathrm{ord}_p(c_j) \geq \min_{0\leq i\leq j} \mathrm{ord}_p(b_i).$$

Proof. We have $f(T)k(T) = g(T)$. The lemma follows by using the definition of polynomial multiplication and the non-archimedean property of ord_p on each coefficient of $g(T)$. □

As above, let $a_{n,j}$ be the jth coefficient of the polynomial $P_n(T)$. Let

$$c_n = \max(0, -\min_j \mathrm{ord}_p(a_{n,j}))$$

so that $p^{c_n} P_n(T) \in \mathbb{Z}_p[T]$, i.e., c_n is the smallest power of p that clears the denominator. Note that c_n is an integer since $a_{n,j} \in \mathbb{Q}$. *Probably if $E[p]$ is irreducible then $c_n = 0$ – see Question 1.13.* Also, for any $j > 0$, let

$$e_{n,j} = \min_{1\leq i\leq j} \mathrm{ord}_p \binom{p^n}{i}.$$

be the min of the valuations of the coefficients of $w_n(T)$, as in Lemma 1.23.

Proposition 1.24. *For all $n \geq 0$, we have $a_{n+1,0} = a_{n,0}$, and for $j > 0$,*

$$\mathrm{ord}_p(a_{n+1,j} - a_{n,j}) \geq e_{n-1,j} - \max(c_n, c_{n+1}).$$

Proof. Let $c = \max(c_n, c_{n+1})$. The divisibility of Corollary 1.8 implies that there is a polynomial $h(T) \in \mathbb{Z}_p[T]$ with

$$w_{n-1}(T) \cdot p^c h(T) = p^c P_{n+1}(T) - p^c P_n(T)$$

and thus (by Gauss' lemma) $p^c h(T) \in \mathbb{Z}_p[T]$ since the right hand side of the equation is integral and $w_{n-1}(T)$ is a primitive polynomial. Applying Lemma 1.23 and renormalizing by p^c gives the result. □

For j fixed, $e_{n-1,j} - \max(c_{n+1}, c_n)$ goes to infinity as n grows since the c_k are uniformly bounded (they are bounded by the power of p that divides the order of the cuspidal subgroup of E). Thus, $\{a_{n,j}\}$ is a Cauchy and Proposition 1.24 implies that that

$$\mathrm{ord}_p(a_j - a_{n,j}) \geq e_{n-1,j} - \max(c_{n+1}, c_n).$$

Remark 1.25. Recall that presently there is not a single example where we can provably show that $\mathrm{ord}_{s=1} L(E,s) \geq 4$. Amazingly $\mathrm{ord}_T \mathcal{L}_p(E,T)$ is "computable in practice" because Kato has proved, using his Euler system in K_2, that $\mathrm{rank}\, E(\mathbb{Q}) \leq \mathrm{ord}_T \mathcal{L}_p(E,T)$ by proving a divisibility predicted by Iwasawa Theory. Thus computing elements of $E(\mathbb{Q})$ gives a provable lower bound, and approximating $\mathcal{L}_p(E,T)$ using Riemann sums gives a provable upper bound – in practice these meet.

Chapter 2

The Birch and Swinnerton-Dyer Formula

2.1. Galois Cohomology

Galois cohomology is the basic language used for much research into algebraic aspects of the BSD conjecture. It was introduced by Lang and Tate in 1958 in [**LT58**]. This section contains a survey of the basic facts we will need in order to define Shafarevich-Tate groups, discuss descent, and construct Kolyvagin's cohomology classes.

The best basic reference on Galois cohomology is chapters VII and X of Serre's *Local Fields* [**Ser79**] or the (very similar!) article by Atiyah and Wall in Cassels-Frohlich [**Cp86**, Ch. IV]. See also the article by Gruenberg in [**Cp86**, Ch. V] for an introduction to profinite groups such as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Since this section is only a survey, you should read one of the above two references in detail, if you haven't already. You might also want to read Chapter 1 of [**CS00**] by Coates and Sujatha, which contains an excellent summary of more advanced topics in Galois cohomology, and Serre's book *Galois Cohomology* [**Ser97**] discusses many general advanced topics in depth. The original article [**LT58**] is also well worth reading.

2.1.1. Group Cohomology. If G is a multiplicative group, the *group ring* $\mathbb{Z}[G]$ is the ring of all finite formal sums of elements of G, with multiplication defined using distributivity and extending linearly. Let A be an additive

group. We say that A is a *G-module* if A is equipped with a module structure over the group ring $\mathbb{Z}[G]$.

Let A^G be the submodule of elements of A that are fixed by G. Notice that if $A \to B$ is a homomorphism of G-modules, then restriction defines a homomorphism $A^G \to B^G$, so $A \mapsto A^G$ is a *functor*. In fact, it is a *left-exact* functor:

Proposition 2.1. *If $0 \to A \to B \to C$ is an exact sequence of G modules, then $0 \to A^G \to B^G \to C^G$ is also exact.*

Definition 2.2 (Group Cohomology)**.** The *group cohomology* $H^n(G, A)$ is by definition the *right derived functors* of the left exact functor $A \to A^G$. These are the unique, up to canonical equivalence, functors H^n such that

- The sequence

$$0 \to A^G \to B^G \to C^G \xrightarrow{\delta} H^1(G, A) \to \cdots \to H^n(G, A) \to H^n(G, B) \to H^n(G, C) \xrightarrow{\delta} H^{n+1}(G, A) \to$$

  is exact.
- If A is *coinduced*, i.e., $A = \mathrm{Hom}(\mathbb{Z}[G], X)$ for X an abelian group, then
$$\mathrm{H}^n(G, A) = 0 \text{ for all } n \geq 1.$$

Remark 2.3. For those familiar with the Ext functor, we have

$$\mathrm{H}^n(G, A) = \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A).$$

We construct $\mathrm{H}^n(G, A)$ explicitly as follows. Consider $\mathbb{Z}$ as a G-module, equipped with the trivial G-action. Consider the following free resolution of $\mathbb{Z}$. Let P_i be the free $\mathbb{Z}$-module with basis the set of $i+1$ tuples $(g_0, \ldots, g_i) \in G^{i+1}$, and with G acting on P_i componentwise:

$$s(g_0, \ldots, g_i) = (sg_0, \ldots, sg_i).$$

The homomorphism $d : P_i \to P_{i+1}$ is given by

$$d(g_0, \ldots, g_i) = \sum_{j=0}^{i} (-1)^j (g_0, \ldots, g_{j-1}, g_{j+1}, \ldots g_i),$$

and $P_0 \to \mathbb{Z}$ is given by sending every element (g_0) to $1 \in \mathbb{Z}$.

The cohomology groups $\mathrm{H}^i(G, A)$ are then the cohomology groups of the complex $K_i = \mathrm{Hom}_{\mathbb{Z}[G]}(P_i, A)$. We identify an element of K_i with a function $f : G^{i+1} \to A$ such that the condition

$$f(sg_0, \ldots, sg_i) = sf(g_0, \ldots, g_i)$$

holds. Notice that such an $f \in K_i$ is uniquely determined by the function (of i inputs)

$$\varphi(g_1, \ldots, g_i) = f(1, g_1, g_1g_2, \ldots, g_1 \cdots g_i).$$

The boundary map $d : K_i \to K_{i+1}$ on such functions $\varphi \in K_i$ is then given explicitly by the formula

$$(d\varphi)(g_1, \ldots, g_{i+1}) = g_1\varphi(g_2, \ldots, g_{i+1}) + \sum_{j=1}^{i}(-1)^j\varphi(g_2, \ldots, g_jg_{j+1}, \ldots, g_{i+1}) + (-1)^{i+1}\varphi(g_1, \ldots, g_i).$$

The group of *n-cocycles* is the group of $\varphi \in K_n$, as above are functions of n variables such that $d\varphi = 0$. The subgroup of *n-coboundaries* is the image of K_{n+1} under d. Explicitly, the cohomology group $H^n(G, A)$ is the quotient of the group group of n-cocycles modulo the subgroup of n-coboundaries.

When $n = 1$, the 1-cocycles are the maps $G \to A$ such that

$$\varphi(gg') = g\varphi(g') + \varphi(g),$$

and φ is a coboundary if there exists $a \in A$ such that $\varphi(g) = ga - a$ for all $g \in G$. Notice that if G acts trivially on A, then

$$\mathrm{H}^1(G, A) = \mathrm{Hom}(G, A).$$

2.1.2. The inf-res Sequence. Suppose G is a group and H is a normal subgroup of G, and A is a G-module. Then for any $n \geq 0$, there are natural homomorphisms

$$\mathrm{res} : \mathrm{H}^n(G, A) \to \mathrm{H}^n(H, A)$$

and

$$\mathrm{inf} : \mathrm{H}^n(G/H, A^H) \to \mathrm{H}^n(G, A)$$

Require that we view n-cocycles as certain maps on the n-fold product of the group. On cocycles, the map res is obtained by simply restricting a cocycle, which is a map $G^i \to A$, to a map $H^i \to A$. The second map inf is obtained by precomposing a cocycle $(G/H)^i \to A^H$ with the natural map $G^i \to (G/H)^i$.

Proposition 2.4. *The* inf-res sequence

$$0 \to \mathrm{H}^1(G/H, A^H) \xrightarrow{\mathrm{inf}} \mathrm{H}^1(G, A) \xrightarrow{\mathrm{res}} \mathrm{H}^1(H, A)$$

is exact.

Proof. See [**Ser79**, §VII.6]. □

2.1.3. Galois Cohomology. Let K be a field and L a finite *Galois extension* of K, so the set of field automorphisms of L that fix K equals the dimension of L viewed as a K-vector space.

For any $\mathrm{Gal}(L/K)$-module A and any $n \geq 0$, let

$$\mathrm{H}^n(L/K, A) = \mathrm{H}^n(\mathrm{Gal}(L/K), A).$$

If $M/L/K$ is a tower of Galois extensions of K and suppose $\mathrm{Gal}(M/K)$ acts on A. Then inf defines a map

$$\mathrm{H}^n(L/K, A^L) \to \mathrm{H}^n(M/K, A). \tag{2.1.1}$$

Let K^{sep} denote a separable closure of K and suppose A is a (continuous) $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-module. (Note – if K has characteristic 0, then a separable closure is the same thing as an algebraic closure.) For any subfield $L \subset K^{\mathrm{sep}}$ that contains K, let $A(L) = A^L$. Let

$$\mathrm{H}^n(K, A) = \varinjlim_{L/K \text{ finite Galois}} \mathrm{H}^n(L/K, A(L)),$$

where the direct limit is with respect to the maps (2.1.1). We can think of this direct limit as simply the union of all the groups, where we identify two elements if they are eventually equal under some map (2.1.1).

One can prove (see [**Cp86**, Ch. V]) that changing the choice of separable closure K^{sep} only changes $\mathrm{H}^n(K, A)$ by unique isomorphism, i.e., the construction is essentially independent of the choice of seperable closure.

2.2. The Shafarevich-Tate Group

In this section we discuss Galois cohomology of elliptic curves, introduce the Kummmer sequence, define the Selmer group, the Shafarevich-Tate group and dicuss descent and the Mordell-Weil theorem.

2.2.1. The Elliptic Curve Kummer Sequence. Let E be an elliptic curve over a number field K. Consider the abelian group $E(\overline{\mathbb{Q}})$ of all points on E defined over a fixed choice $\overline{\mathbb{Q}}$ of algebraic closure of $\mathbb{Q}$. Then A is a module over $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, and we may consider the Galois cohomology groups

$$\mathrm{H}^n(K, E), \qquad \text{for } n = 0, 1, 2, \ldots$$

which are of great interest in the study of elliptic curves, especially for $n = 0, 1$.

If L is a finite Galois extension of K, then the inf-res sequence, written in terms of Galois chomology, is

$$0 \to \mathrm{H}^1(L/K, E(L)) \to \mathrm{H}^1(K, E) \to \mathrm{H}^1(L, E).$$

For any positive integer n consider the homomorphism

$$[n] : E(\overline{\mathbb{Q}}) \to E(\overline{\mathbb{Q}}).$$

This is a surjective homomorphism of abelian groups, so we have an exact sequence

$$0 \to E[n] \to E \xrightarrow{[n]} E \to 0.$$

The associated long exact sequence of Galois cohomology is

$$0 \to E(K)[n] \to E(K) \xrightarrow{[n]} E(K) \to \mathrm{H}^1(K, E[n]) \to \mathrm{H}^1(K, E) \xrightarrow{[n]} \mathrm{H}^1(K, E) \to \cdots.$$

An interesting way to rewrite the begining part of this sequence is as

$$0 \to E(K)/nE(K) \to \mathrm{H}^1(K, E[n]) \to H^1(K, E)[n] \to 0. \tag{2.2.1}$$

The sequence (2.2.1) is called the *Kummer sequence* associated to the elliptic curve.

2.2.2. The Global-to-Local Restriction Maps. Let $\wp$ be a prime ideal of the ring $\mathcal{O}_K$ of integers of the number field K, and let $K_\wp$ be the completion of K with respect to $\wp$. Thus $K_\wp$ is a finite extension the field $\mathbb{Q}_p$ of p-adic numbers.

More explicitly, if $K = \mathbb{Q}(\alpha)$, with α a root of the irreducible polynomial $f(x)$, then the prime ideals $\wp$ correspond to the irreducible factors of $f(x)$ in $\mathbb{Z}_p[x]$. The fields $K_\wp$ then correspond to adjoing roots of each of these irreducible factors of $f(x)$ in $\mathbb{Z}_p[x]$. Note that for most p, a generalization of Hensel's lemma (see Section 1.5.1) asserts that we can factor $f(x)$ by factoring $f(x)$ modulo p and iteratively lifting the factorization.

We have a natural map $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K_\wp) \to \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ got by restriction; implicit in this is a *choice* of embedding of $\overline{\mathbb{Q}}$ in $\overline{\mathbb{Q}}_p$ that sends K into K_v. We may thus view $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K_\wp)$ as a subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$.

Let A be any $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ module. Then this restriction map induces a restriction map on Galois cohomology

$$\mathrm{res}_\wp : \mathrm{H}^1(K, A) \to \mathrm{H}^1(K_\wp, A).$$

Recall that in terms of 1-cocycles this sends a set-theoretic map (a crossed-homomorphism) $f : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to A$ to a map $\mathrm{res}_\wp(f) : \mathrm{Gal}(\overline{\mathbb{Q}}_p/K_\wp) \to A$.

Likewise there is a restriction map for each real Archimedian prime v, i.e., for each embedding $K \to \mathbb{R}$ we have a map

$$\mathrm{res}_v : \mathrm{H}^1(K, A) \to \mathrm{H}^1(\mathbb{R}, A).$$

Exercise 2.5. Let $A = E(\mathbb{C})$ be the group of points on an elliptic curve over $\mathbb{R}$. Prove that $\mathrm{H}^1(\mathbb{R}, E) = \mathrm{H}^1(\mathbb{C}/\mathbb{R}, E(\mathbb{C}))$ is a group of order 1 or 2.

Exercise 2.6. Prove that for any Galois moduloe A and for all primes $\wp$ the kernel of $\mathrm{res}_\wp$ does not depend on the choice of embedding of $\overline{\mathbb{Q}}$ in $\overline{\mathbb{Q}}_p$. (See [**Cp86**, Ch. V]).

2.2.3. The Selmer Group. Let E be an elliptic curve over a number field K. Let v be either a prime $\wp$ of K or a real Archimedian place (i.e., embedding $K \to \mathbb{R}$). As in Section 2.2.1 we also obtain a local Kummer sequence

$$0 \to E(K_v)/nE(K_v) \to \mathrm{H}^1(K_v, E[n]) \to H^1(K_v, E)[n] \to 0.$$

Putting these together for all v we obtain a commutative diagram:
(2.2.2)

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(K)/nE(K) & \longrightarrow & \mathrm{H}^1(K, E[n]) & \longrightarrow & H^1(K, E)[n] \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \to & \prod_v E(K_v)/nE(K_v) & \to & \prod_v \mathrm{H}^1(K_v, E[n]) & \to & \prod_v H^1(K_v, E)[n] \to 0. \end{array}$$

Definition 2.7. The *n-Selmer group* of an elliptic curve E over a number field K is

$$\mathrm{Sel}^{(n)}(E/K) = \ker\left(\mathrm{H}^1(K, E[n]) \to \prod_v \mathrm{H}^1(K_v, E)[n]\right).$$

2.2.4. The Shafarevich-Tate Group and the Mordell-Weil Theorem.

Definition 2.8 (Shafarevich-Tate Group)**.** The *Shafarevich-Tate group* of an elliptic curve E over a number field K is

$$Ш(E/K) = \ker\left(\mathrm{H}^1(K,E) \to \prod_v \mathrm{H}^1(K_v,E)\right).$$

For any positive integer n, we may thus add in a row to (2.2.2):

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(K)/nE(K) & \longrightarrow & \mathrm{Sel}^{(n)}(E/K) & \longrightarrow & Ш(E/K)[n] & \longrightarrow & 0 \\
 & & \| & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E(K)/nE(K) & \longrightarrow & \mathrm{H}^1(K,E[n]) & \longrightarrow & H^1(K,E)[n] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \prod_v E(K_v)/nE(K_v) & \to & \prod_v \mathrm{H}^1(K_v,E[n]) & \to & \prod_v H^1(K_v,E)[n] & \to & 0.
\end{array}$$

The *n-descent sequence* for E is the short exact sequence

$$0 \to E(K)/nE(K) \to \mathrm{Sel}^{(n)}(E/K) \to Ш(E/K)[n] \to 0. \tag{2.2.3}$$

Theorem 2.9. *For every integer n the group $\mathrm{Sel}^{(n)}(E/K)$ is finite.*

Sketch of Proof. Let $K(E[n])$ denote the finite Galois extension of K obtained by adjoining to K all x and y coordinates of elements of $E(\overline{\mathbb{Q}})$ of order dividing n. The inf-res sequence for $K(E[n])/K$ is

$$0 \to \mathrm{H}^1(K(E[n])/K, E[n]) \to \mathrm{H}^1(K,E[n]) \to \mathrm{H}^1(K(E[n]),E[n]). \tag{2.2.4}$$

Because $\mathrm{Gal}(K(E[n])/K)$ and $E[n]$ are both finite groups, the cohomology group $\mathrm{H}^1(K(E[n])/K, E[n])$ is also finite.

Since $\mathrm{Sel}^{(n)}(E/K) \subset \mathrm{H}^1(K,E[n])$, restriction defines a map

$$\mathrm{Sel}^{(n)}(E/K) \to \mathrm{Sel}^{(n)}(E/K[n]). \tag{2.2.5}$$

The kernel of (2.2.5) is finite since it is contained in the first term of (2.2.4), which is finite. It thus suffices to prove that $\mathrm{Sel}^{(n)}(E/K[n])$ is finite.

But

$$\mathrm{Sel}^{(n)}(E/K[n]) \subset \mathrm{H}^1(K[n],E[n]) \cong \mathrm{Hom}(\mathrm{Gal}(\overline{\mathbb{Q}}/K[n]),E[n])).$$

So each element of $\mathrm{Sel}^{(n)}(E/K[n])$ determines (and is determined by) a homomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}/K[n]) \to (\mathbb{Z}/n\mathbb{Z})^2$. That that the fixed field of such a homomorphism is a Galois extension of $K[n]$ with Galois group contained in $(\mathbb{Z}/n\mathbb{Z})^2$.

To complete the proof, one uses the theory of elliptic curves over local fields to show that there is a finite set S of primes such that any such homomorphism corresponding to an element of the Selmer group corresponds to an extension of $K[n]$ ramified only at primes in S. Then the two main theorems of algebraic number theory — that class groups are finite and unit

groups are finitely generated — together imply that there are only finitely many such extensions of $K[n]$.

□

Exercise 2.10. Prove the that $E[n]$ is a finite Galois extension of K.

Theorem 2.11 (Mordell-Weil)**.** *The group $E(\mathbb{Q})$ is finitely generated.*

Proof. The exact sequence (2.2.3) with $n = 2$ and Theorem 2.9 imply that $E(\mathbb{Q})/2E(\mathbb{Q})$ is a finite group. Recall Lemma 1.4 which asserted that if B is a positive real number such that

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

contains a set of generators for $E(\mathbb{Q})/2E(\mathbb{Q})$, then S generates $E(\mathbb{Q})$. Since $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite, it makes sense to define B to be the maximum of the heights of arbitrary lifts of all the elements of $E(\mathbb{Q})/2E(\mathbb{Q})$. Then the corresponding set S generates $E(\mathbb{Q})$. A basic fact about heights is that the set of points of bounded height is finite, i.e., S is finite, so $E(\mathbb{Q})$ is finitely generated. □

2.2.5. Some Conjectures and Theorems about the Shafarevich-Tate Group.

Conjecture 2.12 (Shafarevich-Tate)**.** *Let E be an elliptic curve over a number field K. Then the group $Ш(E/K)$ is finite.*

Theorem 2.13 (Rubin)**.** *If E is a CM elliptic curve over $\mathbb{Q}$ with $L(E, 1) \neq 0$, then $Ш(E/\mathbb{Q})$ is finite. (He proved more than just this.)*

Thus Rubin's theorem proves that the Shafarevich-Tate group of the CM elliptic curve $y^2 + y = x^3 - 7$ of conductor 27 is finite.

Theorem 2.14 (Kolyvagin et al.)**.** *If E is an elliptic curve over $\mathbb{Q}$ with $\operatorname{ord}_{s=1} L(E, s) \leq 1$, then $Ш(E/\mathbb{Q})$ is finite.*

Kolyvagin's theorem is proved in a completely different way than Rubin's theorem. It combines the Gross-Zagier theorem, the modularity theorem that there is a map $X_0(N) \to E$, a nonvanishing result about the special values $L(E^D, 1)$ of quadratic twists of E, and a highly original explicit study of the structure of the images of certain points on $X_0(N)(\overline{\mathbb{Q}})$ in $E(\overline{\mathbb{Q}})$.

Theorem 2.15 (Cassels)**.** *Let E be an elliptic curve over a number field K. There is an alternating pairing on $Ш(E/K)$, which is nondegenerate on the quotient of $Ш(E/K)$ by its maximal divisible subgroup. Moreover, if $Ш(E/K)$ is finite then $\#Ш(E/K)$ is a perfect square.*

For an abelian group A and a prime p, let $A(p)$ denote the subgroup of elements of p power order in A.

The following problem remains open. It helps illustrate our ignorance about Conjecture 2.12 in any cases beyond those mentioned above.

Problem 2.16. Show that there is an elliptic curve E over $\mathbb{Q}$ with rank ≥ 2 such that $Ш(E/\mathbb{Q})(p)$ is finite for infinitely many primes p.

2.3. The Birch and Swinnerton-Dyer Formula

> "The subject of this lecture is rather a special one. I want to describe some computations undertaken by myself and Swinnerton-Dyer on EDSAC, by which we have calculated the zeta-functions of certain elliptic curves. As a result of these computations we have found an analogue for an elliptic curve of the Tamagawa number of an algebraic group; and conjectures have proliferated. [...] I would like to stress that though the associated theory is both abstract and technically complicated, the objects about which I intend to talk are usually simply defined and often machine computable; experimentally we have detected certain relations between different invariants, but we have been unable to approach proofs of these relations, which must lie very deep."
>
> – Bryan Birch

Conjecture 2.17 (Birch and Swinnerton-Dyer)**.** *Let E be an elliptic curve over $\mathbb{Q}$ of rank r. Then $r = \operatorname{ord}_{s=1} L(E, s)$ and*

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\Omega_E \cdot \operatorname{Reg}(E) \cdot \#Ш(E/\mathbb{Q}) \cdot \prod_p c_p}{\#E(\mathbb{Q})^2_{\mathrm{tor}}}. \tag{2.3.1}$$

Let

$$y^2 + \underline{a}_1 xy + \underline{a}_3 y = x^3 + \underline{a}_2 x^2 + \underline{a}_4 x + \underline{a}_6 \tag{2.3.2}$$

be a minimal Weierstrass equation for E.

Recall from Section 1.5.2 that the *real period* Ω_E is the integral

$$\Omega_E = \int_{E(\mathbb{R})} \frac{dx}{2y + \underline{a}_1 x + \underline{a}_3}.$$

See [**Cre97**, §3.7] for an explanation about how to use the Gauss arithmetic-geometry mean to efficiently compute Ω_E.

To define the *regulator* $\operatorname{Reg}(E)$ let $P_1, \ldots, P_n$ be a basis for $E(\mathbb{Q})$ modulo torsion and recall the Néron-Tate canonical height pairing $\langle\, , \,\rangle$ from

Section 1.2. The real number $\mathrm{Reg}(E)$ is the absolute value of the determinant of the $n \times n$ matrix whose (i, j) entry is $\langle P_i, P_j \rangle$. See [**Cre97**, §3.4] for a discussion of how to compute $\mathrm{Reg}(E)$.

We defined the group $Ш(E/\mathbb{Q})$ in Section 2.2.4. In general it is not known to be finite, which led to Tate's famous assertion that the above conjecture "relates the value of a function at a point at which it is not known to be defined[1] to the order of a group that is not known to be finite." The paper [**GJP+05**] discusses methods for computing $\#Ш(E/\mathbb{Q})$ in practice, though no general algorithm for computing $\#Ш(E/\mathbb{Q})$ is known. In fact, in general even if we assume truth of the BSD rank conjecture (Conjecture 1.1) and assume that $Ш(E/\mathbb{Q})$ is finite, there is still no known way to compute $\#Ш(E/\mathbb{Q})$, i.e., there is no analogue of Proposition 1.3. Given finiteness of $Ш(E/\mathbb{Q})$ we can compute the p-part $Ш(E/\mathbb{Q})(p)$ of $Ш(E/\mathbb{Q})$ for any prime p, but we don't know when to stop considering new primes p. (Note that when $r_{E,\mathrm{an}} \leq 1$, Kolyvagin's work provides an explicit upper bound on $\#Ш(E/\mathbb{Q})$, so in that case $Ш(E/\mathbb{Q})$ is computable.)

The *Tamagawa numbers* c_p are 1 for all primes $p \nmid \Delta_E$, where Δ_E is the discriminant of (2.3.2). When $p \mid \Delta_E$, the number c_p is a more refined measure of the structure of the E locally at p. If p is a prime of *additive reduction* (see Section 1.3), then one can prove that $c_p \leq 4$. The other alternatives are that p is a prime of split or nonsplit multiplicative reduction. If p is a *nonsplit prime*, then

$$c_p = \begin{cases} 1 & \text{if } \mathrm{ord}_p(\Delta) \text{ is odd} \\ 2 & \text{otherwise} \end{cases}$$

If p is a prime of *split multiplicative* reduction then

$$c_p = \mathrm{ord}_p(\Delta)$$

can be arbitrarily large. The above discussion completely determines c_p except when p is an additive prime – see [**Cre97**, §3.2] for a discussion of how to compute c_p in general.

For those that are very familiar with elliptic curves over local fields,

$$c_p = [E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p)],$$

where $E^0(\mathbb{Q}_p)$ is the subgroup of $E(\mathbb{Q}_p)$ of points that have nonsingular reduction modulo p.

For those with more geometric background, we offer the following conceptual definition of c_p. Let $\mathcal{E}$ be the *Néron model* of E. This is the unique, up to unique isomorphism, smooth commutative (but not proper!) group

[1] When E is defined over $\mathbb{Q}$ it is now known that $L(E, s)$ is defined overwhere.

scheme over $\mathbb{Z}$ that has generic fiber E and satisfies the Néron mapping property:

> for any smooth group scheme X over $\mathbb{Z}$ the natural map
>
> $$\mathrm{Hom}(X, \mathcal{E}) \to \mathrm{Hom}(X_{\mathbb{Q}}, E)$$
>
> is an isomorphism.

In particular, note that $\mathcal{E}(\mathbb{Z}) \cong E(\mathbb{Q})$. For each prime p, the reduction $\mathcal{E}_{\mathbb{F}_p}$ of the Néron model modulo p is a smooth commutative group scheme over $\mathbb{F}_p$ (smoothness is a property of morphisms that is closed under base extension). Let $\mathcal{E}^0_{\mathbb{F}_p}$ be the identity component of the group scheme $\mathcal{E}_{\mathbb{F}_p}$, i.e., the connected component of $\mathcal{E}^0_{\mathbb{F}_p}$ that contains the 0 section. The *component group* of E at p is the quotient group scheme

$$\Phi_{E,p} = \mathcal{E}_{\mathbb{F}_p}/\mathcal{E}^0_{\mathbb{F}_p},$$

which is a finite étale group scheme over $\mathbb{F}_p$. Finally

$$c_p = \#\Phi_{E,p}(\mathbb{F}_p).$$

2.4. Examples: The Birch and Swinnerton-Dyer Formula

In each example below we use SAGE to compute the conjectural order of $Ш(E/\mathbb{Q})$ and find that it appears to be the square of an integer as predicted by Theorem 2.15.

2.4.1. Example: A Curve of Rank 0. Consider the elliptic curve E with Cremona label 11a, which is one the 3 curves of smallest conductor. We now compute each of the quantities in Conjecture 2.17. First we define the curve E in SAGE and compute its rank:

```
sage: E = EllipticCurve('11a'); E
Elliptic Curve defined by y^2 + y = x^3 - x^2 - 10*x - 20
over Rational Field
sage: E.rank()
0
```

Next we compute the number $L(E, 1)$ to double precision (as an element of the real double field `RDF`):

```
sage: L = RDF(E.Lseries(1)); L
0.253841860856
```

We next compute the real period:

```
sage: Om = RDF(E.omega()); Om
1.26920930428
```

To compute $\prod c_p$ we factor the discriminant of E. It turns at that only 11 divides the discriminant, and since the reduction at 11 is split multiplicative the Tamagawa number is $5 = \mathrm{ord}_{11}(\Delta_E)$.

```
sage: factor(discriminant(E))
-1 * 11^5
sage: c11 = E.tamagawa_number(11); c11
5
```

Next we compute the regulator, which is 1 since E rank 0.

```
sage: Reg = RDF(E.regulator()); Reg
1.0
```

The torsion subgroup has order 5.

```
sage: T = E.torsion_order(); T
5
```

Putting everything together in (2.3.1) and solving for the conjectural order of $Ш(E/\mathbb{Q})$, we see that Conjecture 2.17 for E is equivalent to the assertion that $Ш(E/\mathbb{Q})$ has order 1.

```
sage: Sha_conj = L * T^2 / (Om * Reg * c11); Sha_conj
1.0
```

2.4.2. Example: A Rank 0 curve with nontrivial Sha. Consider the curve E with label 681b. This curve has rank 0, and we compute the conjectural order of $\#Ш(E/\mathbb{Q})$ as in the previous section:

```
sage: E = EllipticCurve('681b'); E
Elliptic Curve defined by y^2 + x*y  = x^3 + x^2 - 1154*x - 15345
over Rational Field
sage: E.rank()
0
sage: L = RDF(E.Lseries(1)); L
1.84481520613
sage: Om = RDF(E.omega()); Om
0.81991786939
```

There are two primes of bad reduction this time.

```
sage: factor(681)
3 * 227
sage: factor(discriminant(E))
3^10 * 227^2
sage: c3 = E.tamagawa_number(3); c227 = E.tamagawa_number(227)
sage: c3, c227
(2, 2)
sage: Reg = RDF(E.regulator()); Reg
1.0
sage: T = E.torsion_order(); T
4
```

In this case it turns out that $\#Ш(E/\mathbb{Q})$ is conjecturally 9.

```
sage: Sha_conj = L * T^2 / (Om * Reg * c3*c227); Sha_conj
9.0
```

2.4.3. Example: A Curve of Rank 1. Let E be the elliptic curve with label 37a, which is the curve of rank 1 with smallest conductor. We define E and compute its rank, which is 1.

```
sage: E = EllipticCurve('37a'); E
Elliptic Curve defined by y^2 + y = x^3 - x over
Rational Field
sage: E.rank()
1
```

We next compute the value $L'(E,1)$. The corresponding function in SAGE takes a bound on the number of terms of the L-series to use, and returns an approximate to $L'(E,1)$ along with a bound on the error (coming from the tail end of the series).

```
sage: L, error = E.Lseries_deriv_at1(200); L, error
(0.305999773834879, 2.10219814818300e-90)
sage: L = RDF(L); L
0.305999773835
```

We compute Ω_E and the Tamagawa number, regulator, and torsion as above.

```
sage: Om = RDF(E.omega()); Om
5.98691729246
sage: factor(discriminant(E))
37
sage: c37 = 1
sage: Reg = RDF(E.regulator()); Reg
0.05111140824
sage: T = E.torsion_order(); T
1
```

Finally, we solve and find that the conjectural order of $Ш(E/\mathbb{Q})$ is 1.

```
sage: Sha_conj = L * T^2 / (Om * Reg * c37); Sha_conj
1.0
```

2.4.4. Example: A curve of rank 2. Let E be the elliptic curve 389a of rank 2, which is the curve of rank 2 with smallest conductor.

```
sage: E = EllipticCurve('389a'); E
Elliptic Curve defined by y^2 + y = x^3 + x^2 - 2*x
over Rational Field
sage: E.rank()
2
```

Because the curve has rank 2, we use Dokchitser's L-function package to approximate $L^{(2)}(E,1)$ to high precision:

```
sage: Lser = E.Lseries_dokchitser()
sage: L = RDF(abs(Lser.derivative(1,2))); L
1.51863300058
```

We compute the regulator, Tamagawa numbers, and torsion as usual:

```
sage: Om = RDF(E.omega()); Om
4.98042512171
sage: factor(discriminant(E))
389
sage: c389 = 1
sage: Reg = RDF(E.regulator()); Reg
0.152460177943
sage: T = E.torsion_order(); T
1
```

Finally we solve for the conjectural order of $\#Ш(E/\mathbb{Q})$.

```
sage: Sha_conj = (L/2) * T^2 / (Om * Reg * c389)
sage: Sha_conj
1.0
```

We pause to emphasize that just getting something that looks like an integer by computing

$$\frac{L^{(r)}(E,1)}{r!} \cdot \#E(\mathbb{Q})^2_{\mathrm{tor}}/(\Omega_E \cdot \mathrm{Reg}(E) \cdot \prod c_P) \tag{2.4.1}$$

is already excellent evidence for Conjecture 2.17. There is also a subtle and deep open problem here:

Open Problem 2.18. Let E be the elliptic curve 389a above. Prove that the quantity (2.4.1) is a rational number.

For curves E of analytic rank 0 it is easy to prove using modular symbols that the conjectural order of $Ш(E/\mathbb{Q})$ is a rational number. For curves with analytic rank 1, this rationality follows from the very deep Gross-Zagier theorem. For curves of analytic rank ≥ 2 there is not a single example in which the conjectural order of $Ш(E/\mathbb{Q})$ is known to be a rational number.

2.4.5. Example: A Rank 3 curve. The curve E with label 5077a has rank 3. This is the curve with smallest conductor and rank 3.

```
sage: E = EllipticCurve('5077a'); E
Elliptic Curve defined by y^2 + y = x^3 - 7*x + 6
over Rational Field
sage: E.rank()
3
```

We compute $L(E, s)$ using Dokchitser's algorithm. Note that the order of vanishing appears to be 3.

```
sage: E.root_number()
-1
sage: Lser = E.Lseries_dokchitser()
sage: Lser.derivative(1,1)
-5.63436295355925e-22
sage: Lser.derivative(1,2)
2.08600476044634e-21
sage: L = RDF(abs(Lser.derivative(1,3))); L
10.3910994007
```

That the order of vanishing is really 3 follows from the Gross-Zagier theorem, which asserts that $L'(E, 1)$ is a nonzero multiple of the Néron-Tate canonical height of a certain point on E called a Heegner point. One can explicitly construct this point[2] on E and find that it is torsion, hence has height 0, so $L'(E, 1) = 0$. That $L''(E, 1) = 0$ then follows from the functional equation (see Section 1.3). Finally we compute the other BSD invariants:

```
sage: Om = RDF(E.omega()); Om
4.15168798309
sage: factor(discriminant(E))
5077
sage: c5077 = 1
sage: Reg = RDF(E.regulator()); Reg
0.417143558758
sage: T = E.torsion_order(); T
1
```

Putting everything together we see that the conjectural order of $Ш(E/\mathbb{Q})$ is 1.

[2]This is not yet implemented in SAGE; if it were, there would be an example right here.

```
sage: Sha_conj = (L/6) * T^2 / (Om * Reg * c5077)
sage: Sha_conj
1.0
```

Note that just as was the case with the curve 389a above, we do not know that the above conjectural order of $Ш(E/\mathbb{Q})$ is a rational number, since there are no know theoretical results that relate any of the three real numbers $L^{(3)}(E,1)$, $\mathrm{Reg}(E/\mathbb{Q})$, and $\Omega_{E/\mathbb{Q}}$.

2.4.6. Example: A Rank 4 curve. Let E be the curve of rank 4 with label 234446b. It is likely that this is the curve with smallest conductor and rank 4 (a big calculation of the author et al. shows that there are no rank 4 curves with smaller *prime* conductor).

```
sage: E = EllipticCurve([1, -1, 0, -79, 289]); E
Elliptic Curve defined by y^2 + x*y  = x^3 - x^2 - 79*x + 289
over Rational Field
sage: E.rank()
4
```

We next compute $L(E,1)$, $L'(E,1)$, $L^{(2)}(E,1)$, $L^{(3)}(E,1)$, and $L^{(4)}(E,1)$. All these special values *look* like they are 0, except for $L^{(4)}(E,1)$ which is about 214, hence clearly nonzero. One can prove that $L(E,1) = 0$ (e.g., using denominator bounds coming from modular symbols), hence since the root number is $+1$, we have either $r_{E,\mathrm{an}} = 2$ or $r_{E,\mathrm{an}} = 4$, and of course suspect (but cannot prove yet) that $r_{E,\mathrm{an}} = 4$.

```
sage: E.root_number()
1
sage: Lser = E.Lseries_dokchitser()
sage: Lser(1)
1.43930352980778e-18
sage: Lser.derivative(1,1)
-4.59277879927938e-24
sage: Lser.derivative(1,2)
-8.85707917856308e-22
sage: Lser.derivative(1,3)
1.01437455701212e-20
sage: L = RDF(abs(Lser.derivative(1,4))); L
214.652337502
```

As above, we compute the other BSD invariants of E.

```
sage: Om = RDF(E.omega()); Om
2.97267184726
sage: factor(discriminant(E))
2^2 * 117223
sage: c2 = 2
sage: c117223 = 1
sage: Reg = RDF(E.regulator()); Reg
1.50434488828
sage: T = E.torsion_order(); T
1
```

Finally, putting everything together, we see that the conjectural order of $Ш(E/\mathbb{Q})$ is 1.

```
sage: Sha_conj = (L/24) * T^2 / (Om * Reg * c2 * c117223)
sage: Sha_conj
1.0
```

Again we emphasize that we do not even know that the conjectural order computed above is a rational number.

It seems almost a miracle that $L^{(4)}(E,1) = 214.65\ldots$, $\Omega_E = 2.97\ldots$, and $\mathrm{Reg}(E) = 1.50\ldots$ have anything to do with each other, but indeed they do:

```
sage: L/24, 2*Om*Reg
(8.9438473959, 8.9438473959)
```

That these two numbers are the same to several decimal places is a fact, independent of any conjectures.

2.5. The p-adic BSD Conjectural Formula

Let E be an elliptic curve over $\mathbb{Q}$ and let p be a prime of good ordinary reduction for E.

In Chapter 1 (see Theorem 1.15) we defined a p-adic L-series

$$\mathcal{L}_p(E,T) \in \mathbb{Q}_p[[T]].$$

Conjecture 1.16 asserted that $\operatorname{ord}_T \mathcal{L}_p(E,T) = \operatorname{rank} E(\mathbb{Q})$. Just as is the cases for $L(E,s)$, there is a conjectural formula for the leading coefficient of the power series $\mathcal{L}_p(E,T)$. This formula is due to Mazur, Tate, and Teitelbaum [**MTT86**].

First, suppose $\operatorname{ord}_T \mathcal{L}_p(E,T) = 0$, i.e., $\mathcal{L}_p(E,0) \neq 0$. Recall that the interpolation property (1.5.1) for $\mathcal{L}_p(E,T)$ implies that

$$\mathcal{L}_p(E,0) = \varepsilon_p \cdot L(E,1)/\Omega_E,$$

where

$$\varepsilon_p = (1-\alpha^{-1})^2, \tag{2.5.1}$$

and $\alpha \in \mathbb{Z}_p$ is the unit root of $x^2 - a_p x + p = 0$. Thus the usual BSD conjecture predicts that if the rank is 1, then

$$\mathcal{L}_p(E,0) = \varepsilon_p \cdot \frac{\prod_\ell c_\ell \cdot \#Ш(E/\mathbb{Q}) \cdot \operatorname{Reg}(E)}{\#E(\mathbb{Q})^2_{\mathrm{tor}}} \tag{2.5.2}$$

Notice in (2.5.2) that since $E(\mathbb{Q})$ has rank 0, we have $\operatorname{Reg}(E) = 1$, so there is no issue with the left hand side being a p-adic number and the right hand side not making sense. It would be natural to try to generalize (2.5.2) to higher order of vanishing as follows. Let $\mathcal{L}_p^*(E,0)$ denote the leading coefficient of the power series $\mathcal{L}_p(E,T)$. Then

$$\text{“}\mathcal{L}_p^*(E,0)\text{”} = \text{”}\varepsilon_p \cdot \frac{\prod_\ell c_\ell \cdot \#Ш(E/\mathbb{Q}) \cdot \operatorname{Reg}(E)}{\#E(\mathbb{Q})^2_{\mathrm{tor}}} \qquad \text{(nonsense!!)}. \tag{2.5.3}$$

Unfortunately (2.5.2) is total nonsense when the rank is bigger than 0. The problem is that $\operatorname{Reg}(E) \in \mathbb{R}$ is a real number, whereas ε_p and $\mathcal{L}_p^*(E,0)$ are both p-adic numbers.

The key *new idea* needed to make a conjecture is to replace the real-number regulator $\operatorname{Reg}(E)$ with a p-adic regulator $\operatorname{Reg}_p(E) \in \mathbb{Q}_p$. This new regulator is defined in a way analogous to the classical regulator, but where many classical complex analytic objects are replaced by p-adic analogues. Moreover, the p-adic regulator was, until recently (see [**MST06**]), much more difficult to compute than the classical real regulator. We will define the p-adic number $\operatorname{Reg}_p(E) \in \mathbb{Q}_p$ in the next section.

Conjecture 2.19 (Mazur, Tate, and Teitelbaum)**.** *Let E be an elliptic curve over $\mathbb{Q}$ and let p be a prime of good ordinary reduction for E. Then the rank of E equals* $\mathrm{ord}_T(\mathcal{L}_p(E,T))$ *and*

$$\mathcal{L}_p^*(E,0) = \varepsilon_p \cdot \frac{\prod_\ell c_\ell \cdot \#Ш(E/\mathbb{Q}) \cdot \mathrm{Reg}_p(E)}{\#E(\mathbb{Q})_{\mathrm{tor}}^2}, \tag{2.5.4}$$

where ε_p is as in (2.5.1)*, and the p-adic regulator $\mathrm{Reg}_p(E) \in \mathbb{Q}_p$ will be defined below.*

Remark 2.20. There are analogous conjectures in many other cases, e.g., good supersingular, bad multiplicative, etc. See [**SW07**] for more details.

2.5.1. Example: A Curve of Rank 2. We only consider primes p of good ordinary reduction for a given curve E in this section. If E is an elliptic curve with analytic rank 0, then the p-adic and classical BSD conjecture are the same, so there is nothing new to illustrate. We will thus consider only curves of rank ≥ 1 in this section.

We consider the elliptic curve 446d1 of rank 2 at the prime $p = 5$.

```
sage: E = EllipticCurve('446d1'); p = 5; E
Elliptic Curve defined by y^2 + x*y  = x^3 - x^2 - 4*x + 4
over Rational Field
```

Next we verify that the rank is 2, that p is a good ordinary prime, and that there are 10 points on E modulo p (so E is *ananomolous at p*, i.e., $p \mid \#E(\mathbb{F}_p)$).

```
sage: E.rank()
2
sage: E.is_ordinary(p)
True
sage: E.Np(p)
10
```

Next we compute the p-adic L-series of E at p. We add $O(T^7)$ so that the displayed series doesn't take several lines.

```
sage: Lp  = E.padic_lseries(p)
sage: LpT = Lp.series(4)
sage: LpT = LpT.add_bigoh(7); LpT
(5 + 5^2 + O(5^3))*T^2 + (2*5 + 3*5^2 + O(5^3))*T^3
          + (4*5^2 + O(5^3))*T^4 + (4*5 + O(5^2))*T^5
          + (1 + 2*5 + O(5^3))*T^6 + O(T^7)
```

We compute the p-adic modular form E_2 evaluated on our elliptic curve with differential ω to precision $O(p^8)$. This is the key difficult input to the computation of the p-adic regulator $\mathrm{Reg}_p(E)$.

```
sage: E.padic_E2(p, prec=8)
3*5 + 4*5^2 + 5^3 + 5^4 + 5^5 + 2*5^6 + 4*5^7 + O(5^8)
```

We compute the normalized p-adic regulator, normalized to the choice of $1+p$ as a topological generator of $1+p\,\mathbb{Z}_p$.

```
sage: Regp = E.padic_regulator(p, 10)
sage: R = Regp.parent()
sage: kg = log(R(1+p))
sage: reg = Regp * p^2 / log(R(1+p))^2
sage: reg*kg^2
2*5 + 2*5^2 + 5^4 + 4*5^5 + 2*5^7 + O(5^8)
```

We compute the Tamagawa numbers and torsion subgroup.

```
sage: E.tamagawa_numbers()
[2, 1]
sage: E.torsion_order()
1
```

We compute $\mathcal{L}_p^*(E,0)$, which is the leading term of the p-adic L-function. It is not a unit, so we call the prime p an *irregular* prime.

```
sage: Lpstar = LpT[2]; Lpstar
5 + 5^2 + O(5^3)
```

Finally, putting everything together we compute the conjectural p-adic order of $\#Ш(E/\mathbb{Q})$. In particular, we see that conjecturally $\#Ш(E/\mathbb{Q})(5)$ is trivial.

```
sage: eps = (1-1/Lp.alpha(20))^2
sage: Lpstar / (eps*reg*(2*1)) * (1)^2
1 + O(5^2)
```

2.5.2. The p-adic Regulator. Fix an elliptic curve E defined over $\mathbb{Q}$ and a prime p of good ordinary reduction for E. In this section we define the p-adic regulator $\mathrm{Reg}_p(E)$. See [**MTT86**], [**MST06**] and [**SW07**] and the references listed there for a more general discussion of p-adic heights, especially for bad or supersingular primes, and for elliptic curves over number fields. See also forthcoming work of David Harvey for highly optimized computation of p-adic regulators.

The p-adic logarithm $\log_p : \mathbb{Q}_p^* \to (\mathbb{Q}_p, +)$ is the unique group homomorphism with $\log_p(p) = 0$ that extends the homomorphism $\log_p : 1+p\mathbb{Z}_p \to \mathbb{Q}_p$ defined by the usual power series of $\log(x)$ about 1. Explicitly, if $x \in \mathbb{Q}_p^*$, then

$$\log_p(x) = \frac{1}{p-1} \cdot \log_p(u^{p-1}),$$

where $u = p^{-\operatorname{ord}_p(x)} \cdot x$ is the unit part of x, and the usual series for log converges at u^{p-1}.

Example 2.21. For example, in SAGE we compute the logs of a couple of non-unit elements of $\mathbb{Q}_5$ as follows:

```
sage: K = Qp(5,8); K
5-adic Field with capped relative precision 8
sage: a = K(-5^2*17); a
3*5^2 + 5^3 + 4*5^4 + 4*5^5 + 4*5^6 + 4*5^7 + 4*5^8 + 4*5^9 + O(5^10)
sage: u = a.unit_part()
3 + 5 + 4*5^2 + 4*5^3 + 4*5^4 + 4*5^5 + 4*5^6 + 4*5^7 + O(5^8)
sage: b = K(1235/5); b
2 + 4*5 + 4*5^2 + 5^3 + O(5^8)
sage: log(a)
5 + 3*5^2 + 3*5^3 + 4*5^4 + 4*5^5 + 5^6 + O(5^8)
sage: log(a*b) - log(a) - log(b)
O(5^8)
```

Note that we can recover b:

```
sage: c = a^b; c
2*5^494 + 4*5^496 + 2*5^497 + 5^499 + 3*5^500 + 5^501 + O(5^502)
sage: log(c)/log(a)
2 + 4*5 + 4*5^2 + 5^3 + O(5^7)
```

Let $\mathcal{E}$ denote the Néron model of E over $\mathbb{Z}$. Let $P \in E(\mathbb{Q})$ be a non-torsion point that reduces to $0 \in E(\mathbb{F}_p)$ and to the connected component of $\mathcal{E}_{\mathbb{F}_\ell}$ at all primes ℓ of bad reduction for E. For example, given any point $Q \in E(\mathbb{Q})$ one can construct such a P by multiplying it by the least common multiple of the Tamagawa numbers of E.

Exercise 2.22. Show that any nonzero point $P = (x(P), y(P)) \in E(\mathbb{Q})$ can be written uniquely in the form $(a/d^2, b/d^3)$, where $a, b, d \in \mathbb{Z}$, $\gcd(a, d) = \gcd(b, d) = 1$, and $d > 0$. (Hint: Use that $\mathbb{Z}$ is a unique factorization domain.)

The function $d(P)$ assigns to P this square root d of the denominator of the x-coordinate $x(P)$.

Example 2.23. We compute a point on a curve, and observe that the denominator of the x coordinate is a perfect square.

```
sage: E = EllipticCurve('446d1')
sage: P = 3*E.gen(0); P
(32/49 : -510/343 : 1)
```

Let

$$x(t) = \frac{1}{t^2} + \cdots \in \mathbb{Z}_p((t)) \tag{2.5.5}$$

be the formal power series that expresses x in terms of the local parameter $t = -x/y$ at infinity. Similarly, let $y(t) = -x(t)/t$ be the corresponding series for y. If we do the change of variables $t = -x/y$ and $w = -1/y$, so $x = t/w$ and $y = -1/w$, then the Weierstrass equation for E becomes

$$s = t^3 + a_1 st + a_2 wt^2 + a_3 w^2 + a_4 w^2 t + a_6 w^3 = F(w, t).$$

Repeatedly substituting this equation into itself recursively yields a power series expansion for $w = -1/y$ in terms of t, hence for both x and y.

Remark 2.24. The *formal group* of E is a power series

$$F(t_1, t_2) \in R = \mathbb{Z}[a_1, \ldots, a_6][[t_1, t_2]].$$

defined as follows. Since $x(t)$ and $y(t)$ satisfy the equation of E, the points $P_1 = (x(t_1), y(t_1))$ and $P_2 = (x(t_2), y(t_2))$ are in $E(R)$. As explained explicitly in [**Sil92**, §IV.1], their sum is

$$Q = P_1 + P_2 = (x(F), y(F)) \in E(R)$$

for some $F = F(t_1, t_2) \in R$.

Example 2.25. We compute the above change of variables in SAGE:

```
sage: var('a1 a2 a3 a4 a6')
sage: E = EllipticCurve([a1,a2,a3,a4,a6]); E
Elliptic Curve defined by
     y^2 + a1*x*y + a3*y = x^3 + a2*x^2 + a4*x + a6
over Symbolic Ring
sage: eqn = SR(E); eqn
(y^2 + a1*x*y + a3*y) == (x^3 + a2*x^2 + a4*x + a6)
sage: F = eqn.lhs() - eqn.rhs(); F
y^2 + a1*x*y + a3*y - x^3 - a2*x^2 - a4*x - a6
sage: G = w^3*F(x=t/s, y=-1/w); G.expand()
-t^3 - a2*w*t^2 - a4*w^2*t - a1*w*t - a6*w^3 - a3*w^2 + w
```

Example 2.26. We use SAGE to compute the formal power series $x(t)$ and $y(t)$ for the rank 1 elliptic curve 37a.

```
sage: E = EllipticCurve('37a'); E
Elliptic Curve defined by y^2 + y = x^3 - x over Rational Field
sage: F = E.formal_group(); F
Formal Group associated to the Elliptic Curve defined by
y^2 + y = x^3 - x over Rational Field
sage: x = F.x(prec=8); x
t^-2 - t + t^2 - t^4 + 2*t^5 - t^6 - 2*t^7 + O(t^8)
sage: y = F.y(prec=8); y
-t^-3 + 1 - t + t^3 - 2*t^4 + t^5 + 2*t^6 - 6*t^7 + O(t^8)
```

Notice that the power series satisfy the equation of the curve.

```
sage: y^2 + y == x^3 - x
True
```

Recall that $\omega_E = \frac{dx}{2y+\underline{a}_1 x+\underline{a}_3}$ is the differential on a fixed choice of Weierstrass equation for E. Let

$$\omega(t) = \frac{dx}{2y + \underline{a}_1 x + \underline{a}_3} \in \mathbb{Q}((t))dt$$

be the formal invariant holomorphic differential on E.

Example 2.27. Continuing the above example, we compute the formal differential on E:

```
sage: F.differential(prec=8)
1 + 2*t^3 - 2*t^4 + 6*t^6 - 12*t^7 + O(t^8)
```

We can also compute $\omega(t)$ directly from the definition:

```
sage: x.derivative()/(2*y+1)
1 + 2*t^3 - 2*t^4 + 6*t^6 - 12*t^7 + 6*t^8 + 20*t^9 + O(t^10)
```

The following theorem, which is proved in [**MT91**], uniquely determines a power series $\sigma \in t\mathbb{Z}_p[[t]]$ and constant $c \in \mathbb{Z}_p$.

Theorem 2.28 (Mazur-Tate)**.** *There is exactly one odd function $\sigma(t) = t + \cdots \in t\mathbb{Z}_p[[t]]$ and constant $c \in \mathbb{Z}_p$ that together satisfy the differential equation*

$$x(t) + c = -\frac{d}{\omega}\left(\frac{1}{\sigma}\frac{d\sigma}{\omega}\right), \tag{2.5.6}$$

where ω is the invariant differential $dx/(2y + a_1x + a_3)$ associated with our chosen Weierstrass equation for E.

The above theorem produces a (very inefficient) algorithm to compute c and $\sigma(t)$. Just view c as a formal indeterminate and compute $\sigma(t) \in \mathbb{Q}[c][[t]]$, then obtain constraints on c using that the coefficients of σ must be in $\mathbb{Z}_p$. These determine c to some precision, which increases as we compute $\sigma(t)$ to higher precision. Until recently this was the only known way to compute c and $\sigma(t)$ – fortunately the method of [**MST06**] is much faster in general.

Definition 2.29 (Canonical p-adic Height)**.** Let E be an elliptic curve over $\mathbb{Q}$ with good ordinary reduction at the odd prime p. Let $\log_p$, d, and $\sigma(t)$ be as above and suppose $P \in E(\mathbb{Q})$ and that nP is a nonzero multiple of P such that nP reduces to the identity component of the Néron model of E at each prime of bad reduction. Then the *p-adic canonical height* of P is

$$h_p(P) = \frac{1}{n^2} \cdot \frac{1}{p} \cdot \log_p\left(\frac{\sigma(P)}{d(P)}\right).$$

Definition 2.30 (p-adic Regulator)**.** The *p-adic regulator* of E is the discriminant (well defined up to sign) of the bilinear $\mathbb{Q}_p$-valued pairing

$$(P, Q)_p = h_p(P) + h_p(Q) - h_p(P + Q).$$

Conjecture 2.31 (Schneider)**.** *The p-adic regulator $\mathrm{Reg}_p(E)$ is nonzero.*

Theorem 2.32 (Kato, Schneider, et al.)**.** *Let E be an elliptic curve over $\mathbb{Q}$ with good ordinary reduction at the odd prime p and assume that the p-adic Galois representation $\rho_{E,p}$ is surjective. If*

$$\mathrm{ord}_T(\mathcal{L}_p(E, T)) \leq \mathrm{rank}\, E(\mathbb{Q}),$$

then $\#Ш(E/\mathbb{Q})(p)$ is finite. Moreover, if $\mathrm{Reg}_p(E)$ is nonzero, then

$$\mathrm{ord}_p(\#Ш(E/\mathbb{Q})(p)) \leq \mathrm{ord}_p\left(\frac{\mathcal{L}_p^*(E, 0)}{\prod c_\ell \cdot \mathrm{Reg}_p(E)}\right).$$

Chapter 3

Heegner Points and Kolyvagin's Euler System

3.1. CM Elliptic Curves

In this section we state, and in some cases sketch proofs of, some basic facts about CM elliptic curves.

If E is an elliptic curve over a field K we let $\mathrm{End}(E/K)$ be the ring of all endomorphisms of E that are defined over K.

Definition 3.1 (CM Elliptic Curve)**.** An elliptic curve E over a subfield of $\mathbb{C}$ has *complex multiplication* if $\mathrm{End}(E/\mathbb{C}) \neq \mathbb{Z}$.

Remark 3.2. If E is an elliptic curve over $\mathbb{Q}$, then $\mathrm{End}(E/\mathbb{Q}) = \mathbb{Z}$. This is true even if E has complex multiplication, in which case the complex multiplication must be defined over a bigger field than $\mathbb{Q}$. The reason $\mathrm{End}(E/\mathbb{Q}) = \mathbb{Z}$ is because $\mathrm{End}(E/\mathbb{Q})$ acts faithfully on the 1-dimensional $\mathbb{Q}$-vector space of invariant holomorphic differentials on E over $\mathbb{Q}$ and $\mathrm{End}(E/\mathbb{Q})$ is finitely generated as a $\mathbb{Z}$-module.

A *complex lattice* $\Lambda \subset \mathbb{C}$ is a subgroup abstractly isomorphic to $\mathbb{Z} \times \mathbb{Z}$ such that $\mathbb{R}\Lambda = \mathbb{C}$. Using the Weierstrass $\wp$-function associated to the lattice Λ, one proves that there is a group isomorphism

$$\mathbb{C}/\Lambda \cong E_\Lambda(\mathbb{C}),$$

where E_Λ is an elliptic curve over $\mathbb{C}$. Conversely, if E is any elliptic curve over $\mathbb{C}$, then there is a lattice Λ such that $E = E_\Lambda$. Explicitly, if ω_E is an

invariant differential we may take Λ to be the lattice of all periods $\int_\gamma \omega_E \in \mathbb{C}$, where γ runs through the integral homology $\mathrm{H}_1(E(\mathbb{C}), \mathbb{Z})$.

Proposition 3.3. *Let Λ_1 and Λ_2 be complex lattices. Then*

$$\mathrm{Hom}(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2) \cong \{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\},$$

where the homomorphisms on the left side are as elliptic curves over $\mathbb{C}$. Moreover, the complex number $\alpha \in \mathbb{C}$ corresponds to the homomorphism $[\alpha]$ induced by multiplication by α, and the kernel of $[\alpha]$ is isomorphic to $\Lambda_2/(\alpha\Lambda_1)$.

Corollary 3.4. *If α is any nonzero complex number and Λ is a lattice, then $\mathbb{C}/\Lambda \cong \mathbb{C}/(\alpha\Lambda)$.*

Proof. Since multiplication by α sends Λ into $\alpha\Lambda$, Proposition 3.3 implies that α defines a homomorphism with 0 kernel, hence an isomorphism. □

Now suppose $E/\mathbb{C}$ is a CM elliptic curve, and let Λ be a lattice such that $E \cong E_\Lambda$. Then

$$\mathrm{End}(E/\mathbb{C}) \cong \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}.$$

Proposition 3.5. *Let $E = E_\Lambda$ be a CM elliptic curve. Then there is a complex number ω and a quadratic imaginary field such K that*

$$\omega\Lambda \subset \mathcal{O}_K,$$

where $\mathcal{O}_K$ is the ring of integers of K. Moreover, $\mathrm{End}(E/\mathbb{C})$ is an order (=subring of rank 2) of $\mathcal{O}_K$.

Proof. Write $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$. By Corollary 3.4, we have $E_\Lambda \cong E_{\omega_1^{-1}\Lambda}$, so we may assume that $\omega_1 = 1$, i.e., that $\Lambda = \mathbb{Z} + \beta\mathbb{Z}$ for some $\beta \in \mathbb{C}$. To complete the proof, we will show that $\omega\Lambda \subset \mathcal{O}_K$ for some quadratic imaginary field K and complex number ω.

By our hypothesis that E is CM there is a complex number $\alpha \notin \mathbb{Z}$ such that $\alpha\Lambda \subset \Lambda$. Fixing a basis for Λ, we see that α acts on Λ via a 2×2 integral matrix, so satisfies a quadratic equation. Thus α is an algebraic integer of degree 2. In particular, there are integers a, b, c, d such that

$$\alpha 1 = a + b\beta, \qquad \text{and} \qquad \alpha\beta = c + d\beta.$$

Since $\alpha \notin \mathbb{Z}$, the first equation above implies that $\beta \in \mathbb{Q}(\alpha)$, so since $\beta \notin \mathbb{Q}$, $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$. Note that $\beta \notin \mathbb{R}$ since Λ is a lattice with basis 1 and β, so $K = \mathbb{Q}(\beta)$ is a quadratic imaginary field. Thus the ring $\mathrm{End}(E/\mathbb{C})$ generated by all such α is an order in the ring $\mathcal{O}_K$ of integers of an imaginary quadratic field. Finally, since $\beta \in K$, there is a complex number ω such that $\omega(\mathbb{Z} + \mathbb{Z}\beta) \subset \mathcal{O}_K$, where ω is chosen so that $\omega\beta \in \mathcal{O}_K$. □

3.1.1. The Set of CM Elliptic Curves with Given CM.

Definition 3.6 (Fractional Ideal)**.** A *fractional ideal* $\mathfrak{a}$ of a number field K is an $\mathcal{O}_K$-submodule of K that is isomorphic to $\mathbb{Z}^{[K:\mathbb{Q}]}$ as an abelian group. In particular, $\mathfrak{a}$ is nonzero.

If $\mathfrak{a}$ is a fractional ideal, the *inverse* $\mathfrak{a}^{-1}$ of $\mathfrak{a}$, which is the set of $x \in K$ such that $x\mathfrak{a} \subset \mathcal{O}_K$, is also a fractional ideal. Moreover, $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$.

Fix a quadratic imaginary field K. Let $\mathrm{Ell}(\mathcal{O}_K)$ be the set of $\mathbb{C}$-isomorphism classes of elliptic curves $E/\mathbb{C}$ with $\mathrm{End}(E) \cong \mathcal{O}_K$. By the above results we may also view $\mathrm{Ell}(\mathcal{O}_K)$ as the set of lattices Λ with $\mathrm{End}(E_\Lambda) \cong \mathcal{O}_K$.

If $\mathfrak{a}$ is a fractional $\mathcal{O}_K$ ideal, then $\mathfrak{a} \subset K \subset \mathbb{C}$ is a lattice in $\mathbb{C}$. For the elliptic curve $E_\mathfrak{a}$ we have

$$\mathrm{End}(E_\mathfrak{a}) = \mathcal{O}_K,$$

because $\mathfrak{a}$ is an $\mathcal{O}_K$-module by definition. Since rescaling a lattice produces an isomorphic elliptic curve, for any nonzero $c \in K$ the fractional ideals $\mathfrak{a}$ and $c\mathfrak{a}$ define the same elements of $\mathrm{Ell}(\mathcal{O}_K)$.

The *class group* $\mathrm{Cl}(\mathcal{O}_K)$ is the group of fractional ideals modulo principal fractional ideals. If $\mathfrak{a}$ is a fractional $\mathcal{O}_K$ ideal, denote by $\overline{\mathfrak{a}}$ its ideal class in the class group $\mathrm{Cl}(\mathcal{O}_K)$ of K. We have a natural map

$$\mathrm{Cl}(\mathcal{O}_K) \to \mathrm{Ell}(\mathcal{O}_K),$$

which sends $\overline{\mathfrak{a}}$ to $E_\mathfrak{a}$.

Theorem 3.7. *Fix a quadratic imaginary field K, and let Λ be a lattice in $\mathbb{C}$ such that $E_\Lambda \in \mathrm{Ell}(\mathcal{O}_K)$. Let $\mathfrak{a}$ and $\mathfrak{b}$ be nonzero fractional $\mathcal{O}_K$-ideals. Then*

(1) *$\mathfrak{a}\Lambda$ is a lattice in $\mathbb{C}$,*

(2) *We have $\mathrm{End}(E_{\mathfrak{a}\Lambda}) \cong \mathcal{O}_K$.*

(3) *We have $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$ if and only if $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$.*

Thus there is a well-defined action of $\mathrm{Cl}(\mathcal{O}_K)$ on $\mathrm{Ell}(\mathcal{O}_K)$ given by

$$\overline{\mathfrak{a}}E_\Lambda = E_{\overline{\mathfrak{a}}^{-1}\Lambda}.$$

Theorem 3.8. *The action of $\mathrm{Cl}(\mathcal{O}_K)$ on $\mathrm{Ell}(\mathcal{O}_K)$ is simply transitive.*

Example 3.9. Let $K = \mathbb{Q}(\sqrt{-23})$. Then the class number h_K is 3. An elliptic curve with CM by $\mathcal{O}_K$ is $\mathbb{C}/(\mathbb{Z} + (1 + \sqrt{-23})/2\mathbb{Z})$, and one can obtain the other two elements of $\mathrm{Ell}(\mathcal{O}_K)$ by multiplying the lattice $\mathbb{Z} + (1 + \sqrt{-23})/2\mathbb{Z}$ by two representative ideal classes for $\mathrm{Cl}(\mathcal{O}_K)$.

3.1.2. Class Field Theory. Class field theory makes sense for arbitrary number fields, but for simplicity in this section and because it is all that is needed for our application to the BSD conjecture, we assume henceforth that K is a totally imaginary number field, i.e., one with no real embeddings.

Let L/K be a finite abelian extension of number fields, and let $\mathfrak{a}$ be any unramified prime ideal in $\mathcal{O}_K$. Let $\mathfrak{b}$ be an prime of $\mathcal{O}_L$ over $\mathfrak{a}$ and consider the extension $k_\mathfrak{b} = \mathcal{O}_L/\mathfrak{b}$ of the finite field $k_\mathfrak{a} = \mathcal{O}_K/\mathfrak{a}$. There is an element $\overline{\sigma} \in \mathrm{Gal}(k_\mathfrak{b}/k_\mathfrak{a})$ that acts via qth powering on $k_\mathfrak{b}$, where $q = \#k_\mathfrak{a}$. A basic fact one proves in algebraic number theory is that there is an element $\sigma \in \mathrm{Gal}(L/K)$ that acts as $\overline{\sigma}$ on $\mathcal{O}_L/\mathfrak{b}$; moreover, replacing $\mathfrak{b}$ by a different ideal over $\mathfrak{a}$ just changes σ by conjugation. Since $\mathrm{Gal}(L/K)$ is abelian it follows that σ is uniquely determined by $\mathfrak{a}$. The association $\mathfrak{a} \mapsto \sigma = [\mathfrak{a}, L/K]$ is called the *Artin reciprocity map*.

Exercise 3.10. Prove that if an unramified prime $\mathfrak{p}$ of K splits completely in an abelian exension L/K, then $[\mathfrak{p}, L/K] = 1$.

Let $\mathfrak{c}$ be an integral ideal divisible by all primes of K that ramify in L, and let $I(\mathfrak{c})$ be the group of fractional ideals that are coprime to $\mathfrak{c}$. Then the reciprocity map extends to a map

$$I(\mathfrak{c}) \to \mathrm{Gal}(L/K) \qquad a \mapsto [\mathfrak{a}, L/K]$$

Let

$$P(\mathfrak{c}) = \{(\alpha) : \alpha \in K^*, \quad \alpha \equiv 1 \pmod{\mathfrak{c}}\}.$$

Here $\alpha \equiv 1 \pmod{\mathfrak{c}}$ means that $\mathrm{ord}_\mathfrak{p}(\alpha - 1) \geq \mathrm{ord}_p(\mathfrak{c})$ for each prime divisor $\mathfrak{p} \mid \mathfrak{c}$.

Definition 3.11 (Conductor of Extension)**.** The *conductor* of an abelian extension L/K is the largest (nonzero) integral ideal $\mathfrak{c} = \mathfrak{c}_{L/K}$ of $\mathcal{O}_K$ such that $[(\alpha), L/K] = 1$ for all $\alpha \in K^*$ such that $\alpha \equiv 1 \pmod{\mathfrak{c}}$.

Proposition 3.12. *The conductor of L/K exists.*

If $\mathfrak{c} = \mathfrak{c}_{L/K}$ is the conductor of L/K then Artin reciprocity induces a group homomorphism

$$I(\mathfrak{c})/P(\mathfrak{c}) \to \mathrm{Gal}(L/K).$$

Definition 3.13 (Ray Class Field)**.** Let $\mathfrak{c}$ be a nonzero integral ideal of $\mathcal{O}_K$. A *ray class field* associated to $\mathfrak{c}$ is a finite abelian extension $K_\mathfrak{c}$ of K such that whenever L/K is an abelian extension such that $\mathfrak{c}_{L/K} \mid \mathfrak{c}$, then $L \subset K_\mathfrak{c}$.

Theorem 3.14 (Existence Theorem of Class Field Theory)**.** *Given any nonzero integral ideal $\mathfrak{c}$ of $\mathcal{O}_K$ there exists a unique ray class field $K_\mathfrak{c}$ associated to $\mathfrak{c}$, and the conductor of $K_\mathfrak{c}$ divides $\mathfrak{c}$.*

Theorem 3.15 (Reciprocity Law of Class Field Theory)**.** *Let L/K be a finite abelian extension.*

(1) *The Artin map is a surjective homomorphism $I(\mathfrak{c}_{L/K}) \to \mathrm{Gal}(L/K)$.*
(2) *The kernel of the Artin map is $N_{L/K}(I_L) \cdot P(\mathfrak{c}_{L/K})$, where $N_{L/K}(I_L)$ is the group of norms from L to K of the fractional ideals of L.*

Definition 3.16 (Hilbert Class Field)**.** The *Hilbert class field* of a number field K is the maximal unramified abelian extension of K.

In particular, since the Hilbert class field is unramified over K, we have:

Theorem 3.17. *Let K be a number field and let H be the Hilbert class field of K. The Artin reciprocity map induces an isomorphism*

$$\mathrm{Cl}(\mathcal{O}_K) \xrightarrow{\cong} \mathrm{Gal}(H/K).$$

3.1.3. The Field of Definition of CM Elliptic Curves.

Theorem 3.18. *Let F be an elliptic curve over $\mathbb{C}$ with CM by $\mathcal{O}_K$, where K is a quadratic imaginary field. Let H be the Hilbert Class Field of K.*

(1) *There is an elliptic curve E defined over K such that $F \cong E_{\mathbb{C}}$.*
(2) *The $\mathrm{Gal}(H/K)$-conjugates of E are representative elements for $\mathrm{Ell}(\mathcal{O}_K)$.*
(3) *If $\sigma \in \mathrm{Gal}(H/K)$ corresponds via Artin reciprocity to $\overline{\mathfrak{a}} \in \mathrm{Cl}(\mathcal{O}_K)$, then*
$$E^\sigma = \overline{\mathfrak{a}}E.$$

Theorem 3.18 generalizes in a natural way to the more general situation in which $\mathcal{O}_K$ is replaced by an order $\mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_K \subset \mathcal{O}_K$. Then the Hilbert class field is replaced by the ray class field K_f, which is a finite abelian extension of H that is unramified outside f (see Definition 3.13 above). There is an elliptic curve E defined over K_f whose endomorphism ring is $\mathcal{O}_f$, and the set of $\mathrm{Gal}(K_f/K)$-conjugates of E forms a set of representatives for $\mathrm{Ell}(\mathcal{O}_f)$. Moreover, the group $I(\mathfrak{c}_{L/K})/(N \cdot P(\mathfrak{c}_{L/K}))$ of Theorem 3.15 acts simply transitively on $\mathrm{Ell}(\mathcal{O}_f)$, and the action of $\mathrm{Gal}(K_f/K)$ on the set of conjugates of E is consistent with the Artin reciprocity map.

3.2. Heegner Points

Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N, and fix a modular parametrization $\pi_E : X_0(N) \to E$.

Let K be a quadratic imaginary field such that the primes dividing N are all unramified and split in K. For simplicity, we will also assume that $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$. Let $\mathcal{N}$ be an integral ideal of $\mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. Then $\mathbb{C}/\mathcal{O}_K$ and $\mathbb{C}/\mathcal{N}^{-1}$ define two elliptic curves over $\mathbb{C}$, and since $\mathcal{O}_K \subset \mathcal{N}^{-1}$, there is a natural map

$$\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathcal{N}^{-1}. \tag{3.2.1}$$

By Proposition 3.3 the kernel of this map is

$$\mathcal{N}^{-1}/\mathcal{O}_K \cong \mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}.$$

Exercise 3.19. Prove that there is an isomorphism $\mathcal{N}^{-1}/\mathcal{O}_K \cong \mathcal{O}_K/\mathcal{N}$ of finite abelian group.

The modular curve $X_0(N)$ parametrizes isomorphism classes of pairs (F, ϕ), where ϕ is an isogeny with kernel cyclic of order N. Thus $\mathbb{C}/\mathcal{O}_K$ and the isogeny (3.2.1) define an element $x_1 \in X_0(N)(\mathbb{C})$. The discussion of Section 3.1.3 along with properties of modular curves proves the following proposition.

Proposition 3.20. *We have*

$$x_1 \in X_0(N)(H),$$

where H is the Hilbert class field of K.

Definition 3.21 (Heegner point)**.** The *Heegner point* associated to K is

$$y_K = \mathrm{Tr}_{H/K}(\pi_E(x_1)) \in E(K).$$

More generally, for any integer n, let $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$ be the order in $\mathcal{O}_K$ of index n. Then $\mathcal{N}_n = \mathcal{N} \cap \mathcal{O}_n$ satisfies $\mathcal{O}_n/\mathcal{N}_n \cong \mathbb{Z}/N\mathbb{Z}$, and the pair

$$(\mathbb{C}/\mathcal{O}_n,\ \mathbb{C}/\mathcal{O}_n \to \mathbb{C}/\mathcal{N}_n^{-1})$$

defines a point $x_n \in X_0(N)(K_n)$, where K_n is the ray class field of conductor n over K.

Definition 3.22 (Heegner point of conductor n)**.** The Heegner point of conductor n is

$$y_n = \pi_E(x_n) \in E(K_n).$$

3.3. Computing Heegner Points

[[This section will be my take on what's in Cohen's book and Watkins paper, hopefully generalized to compute Heegner points over ring class fields (?).]]

3.4. Kolyvagin's Euler System

3.4.1. Kolyvagin's Cohomology Classes. In this section we define Kolyvagin's cohomology classes. Later we will explain the properties that these classes have, and eventually use them to sketch a proof of finiteness of Shafarevich-Tate groups of certain elliptic curves.

We will use, when possible, similar notation to the notation Kolyvagin uses in his papers (e.g., [**Kol91**]). If A is an abelian group let $A/M = A/(MA)$. Kolyvagin writes A_M for the M-torsion subgroup, but we will instead write $A[M]$ for this group.

Let E be an elliptic curve over $\mathbb{Q}$ with no constraint on the rank of E. Fix a modular parametrization $\pi : X_0(N) \to E$, where N is the conductor of E. Let K be a quadratic imaginary field with discriminant D that satisfies the Heegner hypothesis for E, so each prime dividing N splits in K, and assume for simplicity that $D \neq -3, -4$.

Let $\mathcal{O}_K$ be the ring of integer of K. Since K satisfies the Heegner hypothesis, there is an ideal $\mathcal{N}$ in $\mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N}$ is cyclic of order N. For any positive integer λ, let K_λ be the ray class field of K associated to the conductor λ (see Definition 3.13). Recall that K_λ is an abelian extension of K that is unramified outside λ, whose existence is guaranteed by class field theory. Let $\mathcal{O}_\lambda = \mathbb{Z} + \lambda\mathcal{O}_K$ be the order in $\mathcal{O}_K$ of conductor λ, and let $\mathcal{N}_\lambda = \mathcal{N} \cap \mathcal{O}_\lambda$. Let

$$z_\lambda = [(\mathbb{C}/\mathcal{O}_\lambda, \mathcal{N}_\lambda^{-1}/\mathcal{O}_\lambda)] = X_0(N)(K_\lambda)$$

be the Heegner point associated to λ. Also, let

$$y_\lambda = \pi(z_\lambda) \in E(K_\lambda)$$

be the image of the Heegner point on the curve E.

Let $R = \mathrm{End}(E/\mathbb{C})$, and let $B(E)$ be the set of primes $\ell \geq 3$ in $\mathbb{Z}$ that do not divide the discriminant of R and are such that the image of the representation

$$\rho_{E,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(\mathrm{Tate}_\ell(E))$$

contains $\mathrm{Aut}_R(\mathrm{Tate}_\ell(E))$, where $\mathrm{Aut}_R(\mathrm{Tate}_\ell(E))$ is the set of automorphisms that commute with the action of R on $\mathrm{Tate}_\ell(E)$. Note that if $\ell \geq 5$ the condition that $\rho_{E,\ell}$ is surjective is equivalent to the simpler condition that

$$\overline{\rho}_{E,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_R(E[\ell])$$

is surjective. The set $B(E)$ contains all but finitely many primes, by theorems of Serre [**Ser72**], Mazur [**Maz78**], and CM theory, and one can compute $B(E)$.

```
sage: E = EllipticCurve('11a')
sage: E.non_surjective()
[(5, '5-torsion')]
sage: E = EllipticCurve('389a')
sage: E.non_surjective()
[]
```

Fix a prime $\ell \in B(E)$. We next introduce some very useful notation. Let Λ^1 denote the set of all primes $p \in \mathbb{Z}$ such that $p \nmid N$, p remains prime in $\mathcal{O}_K$, and for which

$$n(p) = \mathrm{ord}_\ell(\gcd(p+1, a_p)) \geq 1.$$

For any positive integer r, let Λ^r denote the set of all products of r distinct primes in Λ^1; by definition $\Lambda^0 = \{1\}$. Finally, let

$$\Lambda = \bigcup_{r \geq 0} \Lambda^r.$$

For any $r > 0$ and $\lambda \in \Lambda^r$, let

$$n(\lambda) = \min_{p|\lambda} n(p)$$

be the "worst" of all the powers of p that divide $\gcd(p+1, a_p)$. If $\lambda = 1$, set $n(\lambda) = +\infty$.

Fix an element $\lambda \in \Lambda$, with $\lambda \neq 1$, and consider the ℓ-power

$$M = M_\lambda = \ell^{n(\lambda)}.$$

Recall from Section 2.2.1 that we associate to the short exact sequence

$$0 \to E[M] \to E \xrightarrow{[M]} E \to 0$$

an exact sequence

$$0 \to E(K)/M \to \mathrm{H}^1(K, E[M]) \to H^1(K, E)[M] \to 0.$$

Our immediate goal is to construct an *interesting* cohomology class

$$c_\lambda \in \mathrm{H}^1(K, E[M]).$$

If L/K is any Galois extension, we have (see Section 2.1.2 for most of this) an exact sequence

(3.4.1)

$$0 \to \mathrm{H}^1(L/K, E[M](L)) \to \mathrm{H}^1(K, E[M]) \to \mathrm{H}^1(L, E[M])^{\mathrm{Gal}(L/K)} \to 0.$$

Lemma 3.23. *We have* $E[M](K_\lambda) = 0$.

Proof. For simplicity we prove the statement only in the non-CM case. The integer M is a power of a prime ℓ, so it suffices to show that $E[\ell](K_\lambda) = 0$. Since $\ell \in B(E)$ the Galois representation

$$\overline{\rho}_{E,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell)$$

is surjective. The group $\mathrm{GL}_2(\mathbb{F}_\ell)$ acts transitively on $(\mathbb{F}_\ell)^2$, so the $G_{\mathbb{Q}}$ orbit of any nonzero point in $E[\ell](\overline{\mathbb{Q}})$ is equal to the set of all nonzero points in $E[\ell](\overline{\mathbb{Q}})$. By class field theory, the extension K_λ of $\mathbb{Q}$ is Galois, so if $E[\ell](K_\lambda)$ is nonzero, then it is equal to $E[\ell](\overline{\mathbb{Q}})$. Using properties of the Weil pairing, we see that the field generated by the coordinates of the elements of $E[\ell](\overline{\mathbb{Q}})$ contains the cyclotomic field $\mathbb{Q}(\zeta_\ell)$, which is a field totally ramified at ℓ. But $K \cap \mathbb{Q}(\zeta_\ell) = \mathbb{Q}$, since $\mathrm{disc}(K) \neq -3, -4$, and K_λ is ramified only at primes in Λ^1 and $\ell \notin \Lambda^1$. We conclude that $K_\lambda \cap \mathbb{Q}(\zeta_\ell) = \mathbb{Q}$, so we must have $E[\ell](K_\lambda) = 0$. (Compare [**Gro91**, Lem. 4.3].) □

Thus (3.4.1) with $L = K_\lambda$ becomes

$$\mathrm{H}^1(K, E[M]) \xrightarrow{\cong} \mathrm{H}^1(K_\lambda, E[M])^{G_\lambda} \tag{3.4.2}$$

where $G_\lambda = \mathrm{Gal}(K_\lambda/K)$. Putting this together, we obtain the following commutative diagram with exact rows and columns:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & (E(K_\lambda)/M)^{G_\lambda} & \longrightarrow & \mathrm{H}^1(K_\lambda, E[M])^{G_\lambda} & \longrightarrow & \mathrm{H}^1(K_\lambda, E)[M]^{G_\lambda} & & \\
 & & \uparrow & & \cong \uparrow \mathrm{res} & & \mathrm{res} \uparrow & & \\
0 & \longrightarrow & E(K)/M & \longrightarrow & \mathrm{H}^1(K, E[M]) & \longrightarrow & \mathrm{H}^1(K, E)[M] & \longrightarrow & 0 \\
 & & & & & & \inf \uparrow & & \\
 & & & & & & \mathrm{H}^1(K_\lambda/K, E)[M] & &
\end{array}$$

Thus to construct $c_\lambda \in \mathrm{H}^1(K, E[M])$, it suffices to construct a class $c'_\lambda \in \mathrm{H}^1(K_\lambda, E[M])$ that is invariant under the action of G_λ. We will do this by constructing an element of $E(K_\lambda)$ and using the inclusion

$$E(K_\lambda)/M \hookrightarrow \mathrm{H}^1(K_\lambda, E[M]). \tag{3.4.3}$$

In particular, we will construct an element of the group $E(K_\lambda)/M$ that is invariant under the action of G_λ.

Recall that $y_\lambda \in E(K_\lambda)$. Unfortunately, there is no reason that the class

$$[y_\lambda] \in E(K_\lambda)/M$$

should be invariant under the action of G_λ. To deal with this problem, Kolyvagin introduced a *new and original idea* which we now explain.

Let $H = K_1$ be the Hilbert class field of K. Write $\lambda = p_1 \cdots p_r$, and for each $p = p_i$ let $G_p = \mathrm{Gal}(K_p/K)$ where K_p is the ray class field associated to p. Class field theory implies that the natural map

$$\mathrm{Gal}(K_\lambda/K_1) \cong\to G_{p_1} \times G_{p_2} \times \cdots \times G_{p_r}$$

is an isomorphism. Moreover, each group G_{p_i} is cyclic of order $p_i + 1$. For each $p = p_i$, let σ_p be a fixed choice of generator of G_p, and let

$$\mathrm{Tr}_p = \sum_{\sigma \in G_p} \sigma \in \mathbb{Z}[G_p].$$

Finally, let $D_p \in \mathbb{Z}[G_p]$ be any solution of the equation

$$(\sigma_p - 1) \cdot D_p = p + 1 - \mathrm{Tr}_p\,. \tag{3.4.4}$$

For example, Kolyvagin always takes

$$D_p = \sum_{i=1}^{p} i\sigma_p^i = -\sum_{i=1}^{p+1} (\sigma_p^i - 1)/(\sigma_p - 1).$$

Notice that the choice of D_p is well defined up to addition of elements in $\mathbb{Z}\,\mathrm{Tr}_p$. Let

$$D_\lambda = \prod D_p = D_{p_1} \cdot D_{p_2} \cdot \cdots \cdot D_{p_r} \in \mathbb{Z}[G_\lambda].$$

Finally, let S be a set of coset representatives for $\mathrm{Gal}(K_\lambda/K_1)$ in $G_\lambda = \mathrm{Gal}(K_\lambda/K)$, and let

$$J_\lambda = \sum_{\sigma \in S} \sigma \in \mathbb{Z}[G_\lambda].$$

Let

$$P_\lambda = J_\lambda D_\lambda y_\lambda \in E(K_\lambda).$$

Note that if $\lambda = 1$, then $K_\lambda = K_1$, so

$$P_1 = J_1 y_\lambda = \mathrm{Tr}_{K_1/K}(y_\lambda) = y_K \in E(K).$$

Before proving that we can use P_λ to define a cohomology class in $\mathrm{H}^1(K, E[M])$, we state two crucial facts about the structure of the Heegner points y_λ.

Proposition 3.24. *Write $\lambda = p\lambda'$, and let $a_p = a_p(E) = p + 1 - \#E(\mathbb{F}_p)$.*

(1) *We have*

$$\mathrm{Tr}_p(y_\lambda) = a_p y_{\lambda'}$$

in $E(K_{\lambda'})$.

(2) *Each prime factor $\wp_\lambda$ of p in K_λ divides a unique prime $\wp_{\lambda'}$ of $K_{\lambda'}$, and we have a congruence*

$$y_\lambda \equiv \mathrm{Frob}(\wp_{\lambda'})(y_{\lambda'}) \pmod{\wp_\lambda}.$$

Proof. See [**Gro91**, Prop. 3.7]. The proof uses a description of the action of Hecke operators on modular curves. □

Proposition 3.25. *The class* $[P_\lambda]$ *of* P_λ *in* $E(K_\lambda)/M$ *is fixed by* G_λ.

Proof. We follow the proof of [**Gro91**, Prop. 3.6]. It suffices to show that $[D_\lambda y_\lambda]$ is fixed by σ_p for each prime $p \mid \lambda$, since the σ_p generate $\mathrm{Gal}(K_\lambda/K_1)$, the elements of the set S of coset representatives fix the image of J_λ, and G_λ is generated by the σ_p and S. Thus we will prove that

$$(\sigma_p - 1)D_\lambda y_\lambda \in ME(K_\lambda)$$

for each $p \mid \lambda$.

Write $\lambda = pm$. By (3.4.4), we have in $\mathbb{Z}[G_\lambda]$ that

$$(\sigma_p - 1)D_\lambda = (\sigma_p - 1)D_p D_m = (p + 1 - \mathrm{Tr}_p)D_m,$$

so using Proposition 3.24 we have

$$\begin{aligned}(\sigma_p - 1)D_\lambda y_\lambda &= (p + 1 - \mathrm{Tr}_p)D_m y_\lambda \\ &= (p+1)D_m y_\lambda - D_m \,\mathrm{Tr}_p(y_\lambda) \\ &= (p+1)D_m y_\lambda - a_p D_m y_{\lambda'}\end{aligned}$$

Since $p \in \Lambda^1$ and $M = \ell^{n(p)}$ and $n(p) = \min(\mathrm{ord}_\ell(p+1), \mathrm{ord}_\ell(a_p))$, we have $M \mid p+1$ and $M \mid a_p$. Thus $(p+1)D_m y_\lambda \in ME(K_\lambda)$ and $a_p y_{\lambda'} \in ME(K_\lambda)$, which proves the proposition. □

We have now constructed an element of $E(K_\lambda)/M$ that is fixed by G_λ. Via (3.4.3) this defines an element $c'_\lambda \in \mathrm{H}^1(K_\lambda, E[M])$. But then using (3.4.2) we obtain our sought after class $c_\lambda \in \mathrm{H}^1(K, E[M])$.

We will also be interested in the image d_λ of c_λ in $\mathrm{H}^1(K, E)[M]$.

Proposition 3.26. *If* v *is archimedean or* $v \nmid \lambda$, *then*

$$\mathrm{res}_v(d_\lambda) = 0.$$

Proof. If v is archimedean we are done, since $K_v = \mathbb{C}$ is algebraically closed. Otherwise, the class d_λ splits over K_λ and K_λ is unramified at v, so

$$\mathrm{res}_v(d_\lambda) \in \mathrm{H}^1(K_v^{\mathrm{unr}}/K_v, E).$$

But the latter group is isomorphic to the component group of E at v, and a theorem of Gross-Zagier implies that the Heegner point maps to the identity component. (See [**Gro91**, Prop. 6.2] for more details.) □

Proposition 3.27. *Write $\lambda = pm$ and let $\wp = p\mathcal{O}_K$ be the unique prime ideal of K dividing p. Let v be a place of K_m that divides $\wp$. Then the order of $\mathrm{res}_\wp(d_\lambda)$ is the same as the order of*

$$[P_m] \in E(K_\wp)/ME(K_\wp),$$

where $K_\wp$ denotes the completion of K at $\wp$. (Note that $\wp$ splits completely in K_m/K by class field theory, since $\wp = p\mathcal{O}_K$ is principal and coprime to m, so $P_m \in E(K_\wp)$.)

Proof. See [**Gro91**, Prop. 6.2] for the case $M = \ell$. The argument involves standard properties of Galois cohomology of elliptic curves, some diagram chasing, reduction modulo a prime, and use of formal groups. □

Next we consider a consequence of Proposition 3.27 when y_K is not a torsion point. Note that y_K nontorsion implies that $y_K \notin ME(K)$ for all but finitely many M. Moreover, the Gross-Zagier theorem implies that y_K is nontorsion if and only if $\mathrm{ord}_{s=1} L(E, s) \leq 1$.

Proposition 3.28. *Suppose that $y_K \in E(K)$ is not divisible by M. Then there are infinitely many $p \in \Lambda^1$ such that $d_p \in \mathrm{H}^1(K, E)[M]$ is nonzero.*

Proof. This follows from Proposition 3.27 with $m = 1$ and the Chebotarev density theorem. See e.g., [**Ste02**, §4.1] for a proof. □

Remark 3.29. See, e.g., [**Ste02**] for an application of this idea to a problem raised by Lang and Tate in [**LT58**].

Theorem 3.30 (Kolyvagin)**.** *Suppose E is a modular elliptic curve over $\mathbb{Q}$ and K is a quadratic imaginary field that satisfies the Heegner hypothesis for E and is such that $y_K \in E(K)$ is nontorsion. Then $E(K)$ has rank 1 and*

$$\#Ш(E/K) \mid b \cdot [E(K) : \mathbb{Z}y_K]^2,$$

where b is a positive integer divisible only by primes $\ell \in B(E)$ (i.e., for which the ℓ-adic representation is not as surjective as possible).

Proof. See the entire paper [**Gro91**]. Kolyvagin proves this theorem by bounding $\mathrm{Sel}^{(M)}(E/K)$ for various M using Proposition 3.28 in conjunction with a careful study of various pairings coming from Galois cohomology, the Weil pairing, Tate local daulity, etc. Since

$$0 \to E(K)/ME(K) \to \mathrm{Sel}^{(M)}(E/K) \to Ш(E/K),$$

a bound on the Selmer group translates into a bound on $E(K)$ and $Ш(E/K)$. □

After Kolyvagin proved his theorem, independently Murty-Murty, Bump-Friedberg-Hoffstein, Waldspurger, each proved that infinitely many such quadratic imaginary K always exists so long as E has analytic rank 0 or 1. Also, Taylor and Wiles proved that every E over $\mathbb{Q}$ is modular. Thus we have the following theorem:

Theorem 3.31. *Suppose E is an elliptic curve over $\mathbb{Q}$ with*

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

Then $E(\mathbb{Q})$ has rank $r_{E,\mathrm{an}}$, the group $Ш(E/\mathbb{Q})$ is finite, and there is an explicit computable upper bound on $\#Ш(E/\mathbb{Q})$.

The author has computed the upper bound of the theorem for all elliptic curves with conductor up to 1000 and $r_{E,\mathrm{an}} \leq 1$.

3.4.2. Kolyvagin's Conjectures. What about curves E with $r_{E,\mathrm{an}} \geq 2$? Suppose that E is an elliptic curve over $\mathbb{Q}$ with $r_{E,\mathrm{an}} \geq 2$. In the short paper [**Kol91**], Kolyvagin states an amazing structure theorems for Selmer groups assuming the following unproved conjecture, which is the appropriate generalization of the condition that P_1 has infinite order.

Conjecture 3.32 (Kolyvagin [**Kol91**])**.** *Let E be any elliptic curve over $\mathbb{Q}$ and fix a prime $\ell \in B(E)$ and a prime power $M = \ell^n$ of ℓ. Then there is at least one cohomology class $c_\lambda \in H^1(K, E[M])$ that is nonzero.*

So far nobody has been able to show that Conjecture 3.32 is satisfied by every elliptic curve E over $\mathbb{Q}$, though several people are currently working hard on this problem (including Vatsal and Cornut). Proposition 3.28 above implies that Conjecture 3.32 is true for elliptic curves with $r_{E,\mathrm{an}} \leq 1$.

Kolyvagin also goes on in [**Kol91**] to give a *conjectural construction* of a subgroup

$$V \subset E(K)/E(K)_{\mathrm{tor}}$$

for which $\mathrm{rank}(E(\mathbb{Q})) = \mathrm{rank}(V)$. Let ℓ be an arbitrary prime, i.e., so we do not necessarily assume $\ell \in B(E)$. One can construct cohomology class $c_\lambda \in \mathrm{H}^1(K, E[M])$, so long as $\lambda \in \Lambda^{n+k_0}$, where $\ell^{k_0/2} E(\mathbf{K})[\ell^\infty] = 0$, and $\mathbf{K}$ is the compositum of all class field K_λ for $\lambda \in \Lambda$. For any $n \geq 1$, $k \geq k_0$, and $r \geq 0$, let

$$V_{n,k}^r \subset \varinjlim_m \mathrm{H}^1(K, E[\ell^m])/E(K)_{\mathrm{tor}}$$

be the subgroup generated by the images of the classes $\tau_\lambda = \tau_{\lambda,n} \in \mathrm{H}^1(K, E[\ell^n])$ where λ runs through Λ_{n+k}^r.

Conjecture 3.33 (Kolyvagin)**.** *Let E be any elliptic curve over $\mathbb{Q}$. Then for all prime numbers ℓ, there exists an integer r such that for all $k \geq k_0$ there is an n such that $V_{n,k}^r \neq 0$.*

Recall that

$$n(p) = \mathrm{ord}_\ell(\gcd(p+1, a_p)) \geq 1$$

and

$$n(\lambda) = \min_{p|\lambda} n(p).$$

Let $m'(\lambda)$ be the maximal nonnegative integer such that $P_\lambda \in \ell^{m'(\lambda)} E(K_\lambda)$. Let $m(\lambda) = m'(\lambda)$ if $m'(\lambda) < n(\lambda)$, and $m(\lambda) = \infty$ otherwise. For any $r \geq 0$, let

$$m_r = \min\{m(\lambda) : \lambda \in \Lambda^r\},$$

and let f be the minimal r such that m_r is finite.

Proposition 3.34. *We have $f = 0$ if and only if y_K has infinite order.*

Let $SD = \ell^n S$, where

$$S = \varinjlim_n \mathrm{Sel}^{(\ell^n)}(K, E[\ell^n]).$$

If A is a $\mathbb{Z}[1, \sigma]$-module and $\varepsilon = (-1)^{r_{E,\mathrm{an}}-1}$. then

$$A^v = \{b \in A : \sigma(b) = (-1)^{v+1}\varepsilon b\}$$

Assuming his conjectures, Kolyvagin deduces that for every prime number ℓ there exists integers k_1 and k_2 such that for any integer $k \geq k_1$ we have

$$\ell^{k_2} SD^{(f+1)}[M] \subset V_{n,k}^f \subset SD^{(f+1)}[M].$$

Here the exponent of $f+1$ means the $+1$ or -1 eigenspace for the conjugation action.

Conjecture 3.35 (Kolyvagin)**.** *Let E be any elliptic curve over $\mathbb{Q}$ and ℓ any prime. There exists $v \in \{0, 1\}$ and a subgroup*

$$V \subset (E(K)/E(K)_{\mathrm{tors}})^{(v)}$$

such that

$$1 \leq \mathrm{rank}(V) \equiv v \pmod 2.$$

Let $a = \mathrm{rank}(V) - 1$. Then for all sufficiently large k and all n, one has that

$$V_{n,k}^a \equiv V \mod \ell^n(E(K)/E(K)_{\mathrm{tor}}).$$

Assuming the above conjecture for all primes ℓ, the group V is uniquely determined by the congruence condition in the second part of the conjecture. Also, Kolyvagin proves that if the above conjecture is true, then the rank of $E^v(\mathbb{Q})$ equals the rank of V, and that $Ш(E^v/\mathbb{Q})[\ell^\infty]$ is finite. (Here E^v is E or its quadratic twist.)

When P_1 has infinite order, the conjecture is true with $v = 1$ and $V = \mathbb{Z}P_1$. (I think here E has $r_{E,\mathrm{an}} = 0$.)

3.5. The Gross-Zagier Theorem

Chapter 4

Computational Verification of the Conjecture

Bibliography

[BCDT01] C. Breuil, B. Conrad, Fred Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic). MR 2002d:11058

[Bir71] B. J. Birch, *Elliptic curves over* $\mathbf{Q}$*: A progress report*, 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), Amer. Math. Soc., Providence, R.I., 1971, pp. 396–400.

[Coh00] Henri Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000. MR MR1728313 (2000k:11144)

[Cp86] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, London, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], 1986, Reprint of the 1967 original.

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

[CS00] J. Coates and R. Sujatha, *Galois cohomology of elliptic curves*, Tata Institute of Fundamental Research Lectures on Mathematics, 88, Published by Narosa Publishing House, New Delhi, 2000. MR MR1759312 (2001b:11046)

[Dok04] Tim Dokchitser, *Computing special values of motivic L-functions*, Experiment. Math. **13** (2004), no. 2, 137–149.

[Elk87] Noam D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* $\mathbf{Q}$, Invent. Math. **89** (1987), no. 3, 561–567. MR MR903384 (88i:11034)

[GJP+05] G. Grigorov, A. Jorza, S. Patrikis, C. Patrascu, and W. Stein, *Verification of the Birch and Swinnerton-Dyer Conjecture for Specific Elliptic Curves*, (Submitted) `http://www.wstein.org/papers/bsdalg/` (2005).

[Gro91] B. H. Gross, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic (Durham, 1989), Cambridge Univ. Press, Cambridge, 1991, pp. 235–256.

[Kol91] V. A. Kolyvagin, *On the structure of Selmer groups*, Math. Ann. **291** (1991), no. 2, 253–259. MR 93e:11073

[LT58] S. Lang and J. Tate, *Principal homogeneous spaces over abelian varieties*, Amer. J. Math. **80** (1958), 659–684.

[Maz78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.

[MST06] Barry Mazur, William Stein, and John Tate, *Computation of p-adic heights and log convergence*, Doc. Math. (2006), no. Extra Vol., 577–614 (electronic). MR MR2290599

[MT91] B. Mazur and J. Tate, *The p-adic sigma function*, Duke Math. J. **62** (1991), no. 3, 663–688. MR 93d:11059

[MTT86] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), no. 1, 1–48.

[Ser72] J-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

[Ser79] ———, *Local fields*, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.

[Ser97] ———, *Galois cohomology*, Springer-Verlag, Berlin, 1997, Translated from the French by Patrick Ion and revised by the author.

[Sil92] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, corrected reprint of the 1986 original.

[Ste02] W. A. Stein, *There are genus one curves over* $\mathbf{Q}$ *of every odd index*, J. Reine Angew. Math. **547** (2002), 139–147. MR 2003c:11059

[SW07] William Stein and Chris Wuthrich, *Computations About Tate-Shafarevich Groups Uusing Iwasawa Theory*, In preparation (2007).

[Wil95] A. J. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551. MR 1333035 (96d:11071)

[Wil00] ———, *The Birch and Swinnerton-Dyer Conjecture*, `http://www.claymath.org/prize_problems/birchsd.htm`.