# Ranks of elliptic curves

Notes taken by Daniel Miller

Fall 2014

## Contents

**1 Introduction** **2**
- 1.1 Disclaimer . . . 2
- 1.2 Motivation . . . 2
- 1.3 $L$-functions of elliptic curves . . . 3
- 1.4 Asymptotics of rank . . . 5
- 1.5 Proof strategy . . . 5
- 1.6 Review of the overview . . . 6

**2 Background** **10**
- 2.1 Riemann-Roch . . . 10
- 2.2 Elliptic curves . . . 12
- 2.3 Group law on an elliptic curve . . . 14
- 2.4 Kummer theory . . . 16
- 2.5 Weil pairing . . . 17
- 2.6 Isogenies . . . 19
- 2.7 Jacobians . . . 21
- 2.8 Weil conjectures . . . 26
- 2.9 $p$-adic numbers . . . 27
- 2.10 Selmer groups . . . 30
- 2.11 State-of-the-art . . . 31
- 2.12 Mordell-Weil . . . 34

**3 Main stuff** **38**
- 3.1 Group cohomology . . . 39
- 3.2 Geometric interpretation of cohomology . . . 41
- 3.3 Torsors . . . 43
- 3.4 Review and plan of attack . . . 45
- 3.5 The case $p = 2$ . . . 47
- 3.6 Binary quartic forms . . . 50
- 3.7 Responses to questions . . . 52
- 3.8 What we've done . . . 53

**References** **55**

# 1 Introduction

## 1.1 Disclaimer

These notes originated in the course MATH 7370: Ranks of elliptic curves, taught by Ravi Ramakrishna at Cornell University. The notes are not necessarily an exact reflection of the material as it was covered in class.

## 1.2 Motivation

Our main references will be the preprints [BSa; BSb; BSc; BSd; BSe; BSZ].

The fundamental question is how to solve general diophantine equations

$$f_1(x_1,\dots,x_m) = \cdots = f_n(x_1,\dots,x_m) = 0$$

for the $f_i$ polynomials over $\mathbf{Q}$ or $\mathbf{Z}$ and the $x_i$ in $\mathbf{Q}$ or $\mathbf{Z}$. This is very hard, so we'll focus on curves. This comes down to solving equations $f(x,y)=0$ where $f \in \mathbf{Z}[x,y]$ or $\mathbf{Q}[x,y]$. Or we could homogenize and consider points on the associated projective curve.

**Example 1.2.1.** Consider the equation $x^2+y^2=1$. There is one obvious solution $(0,1)$. From this we get all the other solutions by looking at lines $y=mx+1$ with $m \in \mathbf{Q}$. The equation $x^2+(mx+1)^2=1$ already has one rational solution, so the other must be rational, and all rational solutions to $x^2+y^2=1$ are of this form. So solutions to $x^2+y^2=1$ are in bijection with $\mathbf{Q}$. More geometrically, any nice (that is, smooth, proper and geometrically integral) curve $C_{/\mathbf{Q}}$ that has one rational point is isomorphic (over $\mathbf{Q}$) to $\mathbf{P}^1_{/\mathbf{Q}}$. ▷

Any smooth projective curve $C_{/\mathbf{Q}}$ is the homogeneous zero-set of an equation $f(x,y,z)=0$. The set $C(\mathbf{C})$ is naturally a compact Riemann surface of some genus $g$.

**Theorem 1.2.2** (Faltings)**.** *If $C_{/\mathbf{Q}}$ be a curve of genus $g>1$. Then $\#C(\mathbf{Q}) < \infty$.*

There still isn't an effective algorithm for curves of genus $\geqslant 2$ that will produce the set of zeros of $f$.

We've seen that when $g=0$, either $C(\mathbf{Q}) = \varnothing$ or $C \simeq \mathbf{P}^1$. When $g \geqslant 2$, Faltings' theorem tells us that $\#C(\mathbf{Q}) < \infty$. Our concern is the remaining case $g=1$. If $C_{/\mathbf{Q}}$ is a genus one curve and $C(\mathbf{Q}) = \varnothing$, there isn't much to do. For the remainder, we will concentrate on nice curves $E_{/\mathbf{Q}}$ together with a chosen point $0 \in E(\mathbf{Q})$. Such curves are called *elliptic curves*.

Let $E_{/\mathbf{Q}}$ be an elliptic curve. Basic algebraic geometry involving little more than Riemann-Roch shows that $E$ can be written in the form $y^2 = x^3+Ax+B$ with $A,B \in \mathbf{Z}$. Projectively, this is $y^2z = x^3+Axz^2+Bz^3$. The point $(0:1:0)$ is the $0 \in E(\mathbf{Q})$.

**Example 1.2.3.** Consider the curve $y^2 = x^3 - 9x + 9$. There are obvious solutions $(1, 1)$, $(3, 3)$. The line through them is $y = x$. Since the cubic $x^2 = x^3 - 9x - 9$ already has two rational solutions, the third must be rational. This third point is $(-3, -3)$. In general, if $P, Q, R \in E$, we say that $P + Q + R = 0$ if $P, Q, R$ are the intersection points of a line and $E$ in $\mathbf{P}^2$. For example, one can check that

$$(-3,3) + (1,1) = (\frac{9}{4}, -\frac{3}{8})$$
$$(-3,3) + \left(\frac{9}{4}, -\frac{3}{8}\right) = \left(\frac{57}{49}, -\frac{111}{343}\right).$$

▷

Any elliptic curve $E_{/\mathbf{Q}}$ has the canonical structure of a group variety over $\mathbf{Q}$. For our purposes, this means that there are regular maps $m : E \times E \to E$ and $i : E \to E$ that make $E(\mathbf{C})$ with the maps induced by $m, i$ an honest group with identity element 0. But for any field $F \supset \mathbf{Q}$, there is an abelian group $E(F)$ which is functorial in $F$.

**Theorem 1.2.4** (Mordell-Weil)**.** *Let $E_{/\mathbf{Q}}$ be an elliptic curve. Then $E(\mathbf{Q})$ is finitely generated.*

Thus it makes sense to define the *rank* of $E$ to be $\operatorname{rk}(E) = \operatorname{rk}_{\mathbf{Z}} E(\mathbf{Q})$. Given a specific elliptic curve $E$, we might ask: what are its rank and torsion? The second part is easy. In his paper [Maz77], Mazur proved that the torsion part of $E(\mathbf{Q})$ is one of the following groups:

$$\begin{array}{rl} \mathbf{Z}/m & \text{for } m \leqslant 10 \text{ or } m = 12 \\ (\mathbf{Z}/2) \oplus (\mathbf{Z}/2n) & \text{for } n \leqslant 4 \end{array}$$

This paper is very beautiful, and inspired a lot of amazing mathematics. If $E$ is a specific elliptic curve, it is easy to explicitly check which of these the torsion subgroup of $E(\mathbf{Q})$ is.

## 1.3 $L$-functions of elliptic curves

For $p$ sufficiently large, $E_{/\mathbf{F}_p}$ is an elliptic curve. Write $\#E(\mathbf{F}_p) = p + 1 - a_p$; we have the *Hasse bound* $|a_p| \leqslant 2\sqrt{p}$.

We define the $L$-function of $E$ as

$$L(E) = \prod_{p \text{ bad}} ? \times \prod_{p \text{ good}} \left(1 - \frac{a_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1}.$$

There only finitely many bad primes (they are the ones dividing the discriminant $\Delta = -(4A^3 + 27B^2)$ if $E$ is the curve $y^2 = x^3 + Ax + B$.), and the factors at the bad primes are rational functions in $p^s$. Nonetheless, this is the world's most awful definition! Let's give a better one. We know that $E[l^n] \simeq (\mathbf{Z}/l^n)^2$. This group admits an action of $G_{\mathbf{Q}} = \operatorname{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, an uncountable group with a natural compact, totally disconnected topology. We can paste these actions together to get a representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_l)$. There are conjugacy classes $\mathrm{fr}_p \in G_{\mathbf{Q}}$, and $p \nmid \Delta$, we have

$$\rho(\mathrm{fr}_p) \sim \begin{pmatrix} \alpha_p & \\ & \beta_p \end{pmatrix}.$$

It turns out that

$$1 - \frac{a_p}{p^s} + \frac{1}{p^{2s-1}} = \left(1 - \frac{\alpha_p}{p^s}\right)\left(1 - \frac{\beta_p}{p^s}\right).$$

The function $L(E,s)$ may not seem that complicated, but note that the zeta function built from the trivial representation $G_{\mathbf{Q}} \to \mathrm{GL}_1(\mathbf{C})$ is the Riemann zeta function

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}.$$

So we should expect the behavior of $L(E,s)$ to be very subtle! Most zeta functions encountered in number theory come from Galois representations in this manner.

**Conjecture 1.3.1** (Birch, Swinnerton-Dyer)**.** *Let $E_{/\mathbf{Q}}$ be an elliptic curve. Then* $\mathrm{rk}(E) = \mathrm{ord}_{s=1} L(E,s)$*.*

In fact, Birch and Swinnerton-Dyer predicted the leading term at $s = 1$ of $L(E,s)$ in terms of arithmetic data attached to $E$. The conjecture implicitly includes the assertion that $L(E,s)$ has a meromorphic continuation past $s = 1$. By the work of Wiles and his followers, we know that $E$ is modular, hence its $L$-function agrees with that of a modular form. Hecke showed that modular $L$-functions have such meromorphic continuations, so no problems there.

It is known that $L(E,s)$ satisfies a functional equation

$$L(E,s) = \pm ? L(E, 2-s)$$

where ? is easily computable. If the sign is negative, we know that $L(E,1) = 0$, which suggests that $\mathrm{rk}(E) > 0$.

**Conjecture 1.3.2** (Goldfeld, Katz-Sarnak)**.** *Let $E_{/\mathbf{Q}}$ be an elliptic curve. Then*

$$\mathrm{rk}(E) = \begin{cases} 0 & \textit{50\% of the time} \\ 1 & \textit{50\% of the time.} \end{cases}$$

We have to be careful about what we mean by “50% of the time” as there are infinitely many elliptic curves over $\mathbf{Q}$. To make probabilistic statements precise, we’ll order elliptic curves.

## 1.4 Asymptotics of rank

Given $A, B \in \mathbf{Z}$ with $4A^3 + 27B^2 \neq 0$, write $E_{A,B}$ for the elliptic curve $y^2 = x^3 + Ax + B$. Define its *height* to be $\mathrm{ht}(E) = \max(4|A|^3, 27|B|^2)$. It's easy to check that asymptotically, about $X^{5/6}$ curves have height $\leqslant X$. Let $A(X)$ be the average rank of the set of elliptic curves with height $\leqslant X$. Assuming the Generalized Riemann Hypothesis, these were the bounds on $A(X)$ prior to Bhargava's work:

$$\begin{aligned} \limsup_{X\to\infty} A(X) \leqslant & 2.3 && \text{[Bru92]} \\ & 2.0 && \text{[HB04]} \\ & 1.79 && \text{[You06]} \end{aligned}$$

Unconditionally, all that was known was the trivial bounds

$$0 \leqslant \liminf_{X\to\infty} A(X) \leqslant \limsup_{X\to\infty} A(X) \leqslant \infty.$$

Now, after Bhargava's work, we have

$$0.2 \leqslant \liminf_{X\to\infty} A(X) \leqslant \limsup_{X\to\infty} A(X) \leqslant 0.885.$$

We also know that $\mathrm{ord}_{s=1} L(E,s) = \mathrm{rk}\, E(\mathbf{Q})$ at least 66.43% of the time, and there is a strategy to get 100%. Unfortunately, this strategy only says things about the (conjecturally 100% of) elliptic curves with $\mathrm{rk} \leqslant 1$.

There is a folklore question: is $\mathrm{rk}(E)$ bounded? About 15 years ago, most people thought this wasn't bounded, now, most people think it is bounded.

## 1.5 Proof strategy

For any abelian group $A$, we it is trivial that $\mathrm{rk}(A) \leqslant \dim_{\mathbf{F}_p}(A/p)$. We can prove that the set of elliptic curves with $\mathbf{Z}/p \subset E[p]$ is density zero, so it won't affect density arguments.

There is an exact sequence

$$0 \longrightarrow E[p](\overline{\mathbf{Q}}) \longrightarrow E(\bar{\mathbf{Q}}) \xrightarrow{p} E(\bar{\mathbf{Q}}) \longrightarrow 0.$$

Take $G_{\mathbf{Q}}$-invariants and pass to the long exact sequence in Galois cohomology:

$$0 \longrightarrow E(\mathbf{Q})[p] \longrightarrow E(\mathbf{Q}) \xrightarrow{p} E(\mathbf{Q}) \longrightarrow \mathrm{H}^1(G_{\mathbf{Q}}, E[p]) \longrightarrow \cdots$$

Some fiddling around involving completions of $\mathbf{Q}$ gives a short exact sequence

$$0 \longrightarrow E(\mathbf{Q})/p \longrightarrow \mathrm{Sel}_p(E) \longrightarrow Ш(E)[p] \longrightarrow 0.$$

In the 60s, Cassels discovered a nice geometric way of describing $\mathrm{Sel}_p E$. Elements correspond to some geometric objects (a map $C \to E$), which in turn correspond to a embedding $C \hookrightarrow \mathbf{P}^{p-1}$ (at least if $p \geqslant 3$). When $p = 3$, $C$ is the zero locus of a ternary cubic form.

Ternary cubics have two invariants $I, J$. These correspond to $A$ and $B$. So rather than counting elliptic curves, we can count ternary cubics (up to equivalence).

The quadratic forms $x^2 + y^2$ and $(u + v)^2 + v^2$ are isomorphic over $\mathbf{Z}$. General quadratic forms $ax^2 + bxy + cy^2$ over $\mathbf{Z}$ have an invariant $b^2 - 4ac$ (invariant for action of $\mathrm{SL}_2(\mathbf{Z})$). Essentially, you have to find a fundamental domain for the action of $\mathrm{SL}_2(\mathbf{Z})$ on the upper half plane. It's a lot harder to find a fundamental domain for the action of $\mathrm{SL}_3(\mathbf{Z})$ on a bigger space.

For $p \leqslant 5$, you count equivalences of forms; this is done by finding a fundamental domain for the action of some arithmetic group. This has been done for $p = 2, 3, 5$.

Essentially, one counts lattice points in $G\backslash V_{\mathbf{Z}}$. The problem is, the fundamental domains can have cusps. It turns out that the nonzero elements of $\mathrm{Sel}_p E$ appear in the "main body" of the fundamental domain, and only 0 appears in the cusps.

**Theorem 1.5.1** (Bhargava-Shankar). *The average size of* $\mathrm{Sel}_p E = p + 1$ *for* $p = 2, 3, 5$.

Put $x = \dim_{\mathbf{F}_p} E(\mathbf{Q})/p$. It is easy to check that $(p^2 - p)x + 2p - p^2 \leqslant p^x$. Note that $p^x$ is $p + 1$ on average. It follows that on average, $\mathrm{rk}\, E \leqslant 1 + \frac{1}{p(p-1)}$. If we could prove this for all $p$, we get average $\leqslant 1$. Bhargava and Shankar use work of the Dokchitser's to get bounds $< 1$ without proving that the average of $\#\,\mathrm{Sel}_p E = p + 1$ for all $p$.

## 1.6 Review of the overview

*Note*: the above introduction was given in a department-wide lecture. What follows is a general overview given in the first day the class met.

Let $E_{/\mathbf{Q}}$ be an elliptic curve. This is a smooth genus 1 curve over $\mathbf{Q}$ of the form $y^2 = x^3 + Ax + B$, where $A, B \in \mathbf{Z}$, such that

$$p^4 \mid A \Rightarrow p^6 \nmid B.$$

It is a basic fact that every isomorphism class of elliptic curves over $\mathbf{Q}$ has a unique representative of this form.

Throughout, we'll write an equation $y^2 = x^3 + Ax + B$ to mean the subvariety of $\mathbf{P}^2$ cut out by the homogenization $y^2 z = x^3 + Axz^2 + Bz^3$ of this equation. So $E(\mathbf{Q})$ consists of solutions to $y^2 = x^3 + Ax + B$, as well as the point $(0 : 1 : 0)$ "at infinity." Some useful facts:

1. $E(\mathbf{Q})$ is a finitely-generated abelian group (Mordell-Weil).

2. $E(\mathbf{Q})_{\mathrm{tors}}$ is "understood" All possible such subgroups have been written down (see Mazur's list above), and they all occur. There is an effective algorithm to determine the torsion part of the Mordell-Weil group of an elliptic curve $E$. Since the group law is given by polynomials, the "multiply by $n$" map $[n] : E \to E$ is a polynomial. Simply check whether the roots of $[n]$ lie in $\mathbf{Q}$. There are only finitely many possible $n$, so the algorithm will terminate.

3. $\#E(\mathbf{Q})_{\mathrm{tors}} = 1$ one hundred percent of the time.

Recall that the *height* of $E_{A,B} : y^2 z = x^3 + Axz^2 + bz^3$ is $\max(4|A|^3, 27B^2)$. This definition is actually pretty natural if you know the definition of the discriminant of $E$.

Recall that our goal is to study the average rank of $E_{/\mathbf{Q}}$ with height $\leqslant X$, as $X \to \infty$. That is, we are interested in the asymptotics of

$$\lim_{X\to\infty} \frac{\sum_{\mathrm{ht}\, E \leqslant X} \mathrm{rk}(E)}{\#\{E : \mathrm{ht}\, E \leqslant X\}}.$$

Currently it is not known if this limit exists, but conjecturally it is $1/2$. Note that $\#\{E : \mathrm{ht}\, E \leqslant X\}$ is asymptotically $O(X^{5/6})$. We have to be careful, because some of the curves $E_{A,B}$ will be singular, but this happens on a thin set, so it will not affect our calculations.

Note that for any finitely-generated abelian group $A$, we have

$$\mathrm{rk}(A) = \dim_{\mathbf{Q}}(A \otimes \mathbf{Q}) \leqslant \dim_{\mathbf{F}_p}(A \otimes \mathbf{F}_p).$$

So to get upper bounds on $\mathrm{rk}(E)$, it suffices to bound $\dim_{\mathbf{F}_p}(E(\mathbf{Q})/p)$.

**Theorem 1.6.1.** *Let $E_{/\mathbf{Q}}$ be an elliptic curve. Then $E(\overline{\mathbf{Q}})$ is a divisible group.*

*Proof.* Given $n \in \mathbf{Z}$ and $x \in E(\overline{\mathbf{Q}})$, we need some $y \in E(\overline{\mathbf{Q}})$ such that $n \cdot y = x$. The coefficients of the polynomial $[n]$ will be algebraic over $\mathbf{Q}$, so all solutions to $[n]y = x$ will be algebraic over $\mathbf{Q}$. □

By [GEM14, Cor 5.11], we have $E[n](\overline{\mathbf{Q}}) \simeq (\mathbf{Z}/n)^2$ for all $n \geqslant 1$. Thus $E(\overline{\mathbf{Q}})_{\mathrm{tors}} \simeq (\mathbf{Q}/\mathbf{Z})^2$. Since $E(\overline{\mathbf{Q}})$ is divisible, we have an exact sequence

$$0 \longrightarrow E(\overline{\mathbf{Q}})[p] \longrightarrow E(\overline{\mathbf{Q}}) \xrightarrow{p} E(\overline{\mathbf{Q}}) \longrightarrow 0. \qquad (1)$$

Recall that $E(\mathbf{C}) \simeq S^1 \times S^1$ as real Lie groups. The finite group $E(\overline{\mathbf{Q}})[p] \simeq (\mathbf{Z}/p)^2$ comes with a standard pairing, the *Weil pairing*, coming from the cup product on $\mathrm{H}^1(\mathbf{Q}, E[p])$.

Let $\overline{\mathbf{Q}}$ be an algebraic closure of $\mathbf{Q}$, and let $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. This is an uncountable, totally disconnected compact topological group, and its cohomology has a good duality theory; see for example [NSW08]. There is an analogy between $G_{\mathbf{Q}}$ and 3-manifolds, see e.g. [Mor12].

The group $G_{\mathbf{Q}}$ acts on $E(\overline{\mathbf{Q}})$, respecting the group structure. So we can take its cohomology. The functor $M \mapsto M^{G_{\mathbf{Q}}}$ is left exact, so we can do the usual nonsense with enough injectives and derived functors to get $\mathrm{H}^\bullet(G_{\mathbf{Q}}, M)$. Or we can write a direct definition using cocycles and coboundaries. Often, to save space, if $F$ is a field, $G_F$ its absolute Galois group and $M$ a $G_F$-module, we'll write $\mathrm{H}^\bullet(F, M)$ instead of $\mathrm{H}^\bullet(G_F, M)$.

A commutative diagram

$$\begin{tikzcd}
\overline{\mathbf{Q}} \arrow[r, hook] & \mathbf{C} \\
\mathbf{Q} \arrow[u, hook] \arrow[r, hook] & \mathbf{R} \arrow[u, hook]
\end{tikzcd}$$

gives rise to an injection $G_{\mathbf{R}} = \mathrm{Gal}(\mathbf{C}/\mathbf{R}) \hookrightarrow G_{\mathbf{Q}}$. Also, for each prime $l$ we get an inclusion $G_{\mathbf{Q}_l} \hookrightarrow G_{\mathbf{Q}}$. The groups $G_{\mathbf{Q}_l}$ are much bigger than $G_{\mathbf{R}} = \mathbf{Z}/2$, but they're pretty well-behaved [for example, they're pro-solvable in a nice way]. The group $G_{\mathbf{Q}}$ is very poorly understood. We know its abelianization quite well, and 2-dimensional representations reasonably well, but higher-dimensional representations not well at all.

The long exact sequence in cohomology coming from (1) gives rise to a natural short exact sequence

$$\begin{tikzcd}
0 \arrow[r] & E(\mathbf{Q})/p \arrow[r] & \mathrm{H}^1(G_{\mathbf{Q}}, E[p]) \arrow[r] & \mathrm{H}^1(G_{\mathbf{Q}}, E)[p] \arrow[r] & 0
\end{tikzcd}$$

Unfortunately, $\mathrm{H}^1(G_{\mathbf{Q}}, E[p])$ is infinite-dimensional, so this doesn't seem very helpful. But we can extend this to a diagram

$$\begin{tikzcd}
0 \arrow[r] & E(\mathbf{Q})/p \arrow[r] \arrow[d] & \mathrm{H}^1(G_{\mathbf{Q}}, E[p]) \arrow[r] \arrow[d] & \mathrm{H}^1(G_{\mathbf{Q}}, E)[p] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \prod_v E(\mathbf{Q}_v)/p \arrow[r] & \prod_v \mathrm{H}^1(G_{\mathbf{Q}_v}, E[p]) \arrow[r] & \prod_v \mathrm{H}^1(G_{\mathbf{Q}_v}, E)[p] \arrow[r] & 0.
\end{tikzcd}$$

Here, by convention $v$ ranges over all primes *and* $\infty$, and we put $\mathbf{Q}_\infty = \mathbf{R}$. The vertical maps come from basic functoriality (restriction) of group cohomology. Put

$$\mathrm{Sel}_p(E) = \ker\left(\mathrm{H}^1(G_{\mathbf{Q}}, E[p]) \to \prod_v \mathrm{H}^1(G_{\mathbf{Q}_v}, E)[p]\right).$$

This is finite-dimensional, and $E(\mathbf{Q})/p \hookrightarrow \mathrm{Sel}_p E$. The group $\mathrm{Sel}_p(E)$ is measuring some local-global stuff. That is, cohomology classes in $\mathrm{H}^1(G_{\mathbf{Q}}, E[p])$ that "are" trivial locally everywhere.

In [Cas62], Cassels showed that elements of $\mathrm{Sel}_p(E)$ are in bijection with locally soluble $p$-coverings of $E$.

Briefly, the map $p : E \to E$ has field of definition $\mathbf{Q}$. Consider the varieties $U : x^2 + y^2 = 1$ and $V : x^2 + y^2 = 3$. There is an isomorphism $U_{\mathbf{Q}(\sqrt{3})} \to V_{\mathbf{Q}(\sqrt{3})}$ by $(x, y) \mapsto (\sqrt{3}x, \sqrt{3}y)$, but this isomorphism isn't defined over $\mathbf{Q}$. A *locally soluble $p$-covering* of $E$ is an isomorphism $\phi : C \xrightarrow{\sim} E$ (not necessarily defined over $\mathbf{Q}$) such that $[p] \circ \phi$ is defined over $\mathbf{Q}$. Moreover, $C$ must have points over $\mathbf{R}$ and all $\mathbf{Q}_l$.

Locally soluble $p$-coverings of $E$ give degree-$p$ divisors on $C$. This gives a map $C \to \mathbf{P}^{p-1}$, which is an embedding of degree 3 if $p \geqslant 3$.

Say $p = 3$. A degree-3 curve in $\mathbf{P}^2$ is easy to describe. So elements in $\mathrm{Sel}_3(E)$ correspond to degree-3 cubics over $\mathbf{Q}$ (up to equivalence).

Let's switch gears. Consider binary quadratic forms over $\mathbf{Z}$. These are just polynomials $ax^2+bxy+cy^2$ for $a,b\in\mathbf{Z}$. These have a natural $\mathrm{SL}_2(\mathbf{Z})$-action coming from

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}.$$

But $\mathrm{SL}_2(\mathbf{Z})$ has generators $\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$ and $\begin{pmatrix} & -1 \\ 1 & \end{pmatrix}$.

Claim: $d=b^2-4ac$ is an invariant of the action of $\mathrm{SL}_2(\mathbf{Z})$. We'll only check $\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$-invariance. We get

$$a(x+y)^2+b(x+y)y+cy^2 = ax^2+(2a+b)xy+(c+b+a)y^2,$$

and simply check that $(2a+b)^2-4a(a+b+c)=b^2-4ac$.

**Theorem 1.6.2** (Gauss)**.** *Given $d$, there exist only finitely many inequivalent binary quadratic forms over $\mathbf{Z}$ with discriminant $d$.*

It's natural to ask: "how many are there?" We'll ask the exact same question for ternary forms. In that case there are two invariants $I,J$. Proving that these are invariant is a simple computation. What is harder is the analogue of

$$\mathbf{Z}[b^2-4ac]=\mathbf{Z}[a,b,c]^{\mathrm{SL}_2(\mathbf{Z})}.$$

A general theorem of Borel and Harish-Chandra says that there are still only finitely many equivalence classes of forms with any given pair of invariants.

Q. what values $d$ occur? [easy: $d\equiv 0$ or $1 \pmod 4$]

Q. What is the arithmetic significance of

$$h(d)=\#\{\text{inequivalent quadratic forms with discriminant } d\}$$

It turns out that $h(d)$ is the *narrow class number* of $\mathbf{Q}(\sqrt{d})$. This measures failure of unique factorization in that field.

Q. What is the average value of $h(d)$?

**Theorem 1.6.3** (Mertens, Siegel)**.** *(a) For $-X<d<0$, the average value of $h(d)$ is $\frac{\pi}{18}X^{3/2}+O(X^{3/2-\varepsilon})$ for some explicit $\varepsilon>0$.*

*(b) For $0<d<X$, the average value of $h(d)\log(\epsilon_d)$ is $\frac{\pi^2}{18}X^{3/2}+O(X^{3/2-\varepsilon})$. Here $\epsilon_d$ is a fundamental unit of $\mathbf{Q}(\sqrt{d})$.*

What's different about $p=2$ and $p>2$? When $p=2$, $C\to\mathbf{P}^{p-1}$ isn't an embedding. But it is a degree-2 cover with four branch points. This comes down to counting binary quartic forms up to equivalence. Let

$$ax^4+bx^3y+cx^2y^2+dxy^3+ey^4$$

be such a form. The group $\mathrm{SL}_2(\mathbf{Z})$ acts as before. If

$$\begin{aligned} I &= 12ae-3bd+c^2 \\ J &= 72ace+9bcd-27ad^2-27eb^2-2c^3. \end{aligned}$$

then we have

**Theorem 1.6.4.** $\mathbf{Z}[I,J] = \mathbf{Z}[a,b,c,d,e]^{\mathrm{SL}_2(\mathbf{Z})}$.

*Proof.* Find source [not Hilbert!] □

So counting elements of $\mathrm{Sel}_2(E)$ of $E$ of height $X$ corresponds to counting binary quartic forms via $(I,J) \leftrightarrow (A,B)$.

**Theorem 1.6.5.** *The number of such forms up to height $X$ with*

$$\begin{array}{ll}
4 \text{ real roots} & \dfrac{4}{\zeta(2)}135X^{5/6} + O(X^{3/4}) \\
2 \text{ real roots} & 32\dfrac{\zeta(2)}{135}X^{5/6} + O(X^{3/4}) \\
\text{no real roots} & 8\dfrac{\zeta(2)}{135}X^{5/6} + O(X^{3/4}).
\end{array}$$

**Corollary 1.6.6.** *When ordered by height,* $\mathrm{avg}(\#\,\mathrm{Sel}_2) = 2 + 1$.

# 2 Background

We'll thread a very narrow path to the main theorems, assuming a bunch of facts along the way. A good source on the algebraic geometry we'll do is [Sil09, ch.2,3].

## 2.1 Riemann-Roch

We'll spend the rest of this subsection explaining the terms in the following theorem.

**Theorem 2.1.1** (Riemann-Roch)**.** *Let $C_{/k}$ be a smooth projective curve. Let $K$ be the canonical divisor and $D$ a divisor. Then $l(D) - l(K - D) = \deg D - g + 1$.*

For us, a curve $C_{/k}$ is the zero locus of a (non-constant) polynomial $f \in k[x,y]$. We stress the fact that $k$ is *not* necessarily algebraically closed here. Pictorially, smoothness means that $C$ has no cusps or self-intersections. For example, $f$ can't be something like $xy$ or $x^2 - y^3$. More formally, we want the tangent space to be 1-dimensional at every point on $C$. For any $c \in C$, we have a matrix $\left(\frac{\partial f}{\partial x}(c), \frac{\partial f}{\partial y}(c)\right)$ which needs to be nondegenerate, i.e. the partials of $f$ never simultaneously vanish. Note that here, "$c \in C$" means $c \in C(\bar{k})$, so we consider points not defined over $k$. We'll constantly move between the affine curve $V(f) \subset \mathbf{A}^2$ and the projective curve in $\mathbf{P}^2$ cut out by the projectivisation of $f$.

A *divisor* on a curve $C$ is a formal $\mathbf{Z}$-linear combination of points (defined over $\bar{k}$).

**Example 2.1.2.** Let $C : x^2 + y^2 = 10$. Let $P = (4, i\sqrt{6})$ and $Q = (4, -i\sqrt{6})$. Then $P$ and $Q$ are not defined over $\mathbf{Q}$, but $P + Q$ is a divisor on $C$ defined over $\mathbf{Q}$. ▷

The absolute Galois group $G_k$ of $k$ acts on the space of divisors on $C$. We say a divisor $D$ is *defined over* $k$ if $D = D^\sigma$ for all $\sigma \in G_k$.

We put an equivalence relation on divisors: $D_1 \sim D_2$ if $D_1 - D_2 = \operatorname{div}(f)$ for some rational function $f$ on $C$. So we need to define $\operatorname{div}(f)$. Let $k[C] = k[x, y]/f$ be the ring of regular functions on $f$, and let $k(C)$ be the field of fractions of $k[C]$; we call $k(C)$ the field of *rational functions* on $C$. Any rational function $f$ induces a morphism $f : C \to \mathbf{P}^1$. Since $C$ is projective, this map is either constant or surjective. We can now put

$$\operatorname{div}(f) = \sum_{c \in C(\bar{k})} \operatorname{ord}_c(f) \cdot c.$$

We put $\operatorname{Pic}(C) = \operatorname{Div}(C)/\operatorname{div}(k(C)^\times)$.

Now we need to define the canonical divisor. It is the class of a nonvanishing differential on $C$. More formally, it's the divisor class corresponding to the line bundle $\Omega^1_C$.

We put $l(D) = \dim \mathscr{L}(D)$, where

$$\mathscr{L}(D) = \{f : C \twoheadrightarrow \mathbf{P}^1 : \operatorname{Div}(f) + D \geqslant 0\} \cup \{0\}.$$

It is a theorem that $l(D) < \infty$ for all divisors $D$.

Aside: let $[L : \mathbf{Q}] < \infty$, i.e. let $L$ be a number field. Then there is an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathcal{O}_L^\times \arrow[r] & L^\times \arrow[r] & I_L \arrow[r] & \operatorname{Pic}(O_L) \arrow[r] & 0, \end{tikzcd}$$

where $I_L$ is the group of fractional ideals in $L$. See [Lor96] for more on the parallel between algebraic number theory and algebraic geometry. This is analogous to the sequence

$$\begin{tikzcd} 0 \arrow[r] & k^\times \arrow[r] & k(C)^\times \arrow[r, "\operatorname{div}"] & \operatorname{Div}^\circ(C) \arrow[r] & \operatorname{Pic}^\circ(C) \arrow[r] & 0. \end{tikzcd}$$

Here the degree $\deg(\sum n_c c) = \sum n_c$. It is a basic fact that for $f \in k(C)^\times$, we have $\deg(f) = 0$. In fact, $\operatorname{Pic}(X)$ makes sense for $X$ any scheme (e.g. a curve or the spectrum of $\mathcal{O}_L$).

If $C_{/\mathbf{Q}}$ is a smooth projective curve, then $C(\mathbf{C})$ will be a compact Riemann surface, hence a torus with $g$ holes. We call $g$ the *genus* of $C$. Geometrically, $g = \dim \mathrm{H}^0(\Omega^1)$.

**Theorem 2.1.3.** *Let $C_{/k}$ be a smooth projective curve, $D$ a divisor on $C$. Then*

1. $\deg D < 0 \Rightarrow l(D) = 0$.
2. $l(D) < \infty$.
3. $D \sim D' \Rightarrow \mathscr{L}(D) \simeq \mathscr{L}(D')$.
4. $l(K_C) = g$ *and* $\deg(K_C) = 2g - 2$.

*5.* $\deg(D) > 2g-2 \Rightarrow l(D) = \deg(D) - g + 1$*.*

*Proof.* Choose $D$ cleverly (i.e. 0 or $K_C$) in the Riemann-Roch Theorem, and use $l(0) = 1$. □

## 2.2 Elliptic curves

If we're analyzing the case $g = 0$, diophantine properties were known to the Greeks. For $g \geqslant 2$, Faltings tells that $\#C(\mathbf{Q}) < \infty$. The remaining case is $g = 1$.

**Definition 2.2.1.** *Let $k$ be a field. An* elliptic curve over $k$ *is a smooth projective curve $E_{/k}$ together with a point $0 \in E(k)$.*

Let $E_{/k}$ be an elliptic curve, $e \in E(k)$. What is $l(e)$? From Theorem 2.1.3, we get:

| $n$ | $l(n \cdot e)$ | basic of $\mathscr{L}(n \cdot e)$ |
|---|---|---|
| 1 | 1 | $\{1\}$ |
| 2 | 2 | $\{1, x\}$ |
| 3 | 3 | $\{1, x, y\}$ |
| 4 | 4 | $\{1, x, y, x^2\}$ |
| 5 | 5 | $\{1, x, t, x^2, xy\}$ |
| 6 | 6 | $\{1, x, y, x^2, xy, x^3$ or $y^2\}$ |

The last set could have seven elements, but $\mathscr{L}(6 \cdot e)$ is 6-dimensional. It follows that there is a dependence relation

$$\alpha_0 + \alpha_1 x + \alpha_2 y + \alpha_3 x^2 + \alpha_4 xy + \alpha_5 x^3 + \alpha_6 y^2 = 0.$$

We claim that $(\alpha_4, \alpha_6) \neq (0,0)$. Basic consideration of the orders of poles in the remaining equation at $e$ shows this. We can assume that $\alpha_6 \neq 0$. Say $\alpha_6 = 0$ (then $\alpha_4 \neq 0$). Consider the change of variables

$$\begin{aligned} x &\mapsto x + cy \\ y &\mapsto y. \end{aligned}$$

The new coefficient of $y^2$ is $\alpha_3 c^2 + \alpha_4 c$, and we can choose $c$ so that this is $\neq 0$. There's a better proof that $\alpha_6 \neq 0$. If $\alpha_6 = 0$, since $\{1, x, y, x^2, xy, x^3\}$ is a basis of $\mathscr{L}(6 \cdot e)$, all the $\alpha_i = 0$, which we can assume is not the case.

Divide through by $\alpha_6$ to get the following:

$$y^2 + y(\alpha_2 + \alpha_4 x) + \left(\frac{\alpha_2 + \alpha_4 x}{2}\right)^2 - \left(\frac{\alpha_2 + \alpha_4 x}{2}\right)^2 + \alpha_3 x^3 + \alpha_1 x + \alpha_0 = 0.$$

Replace $y$ by $y + \frac{\alpha_2 + \alpha_4 x}{2}$; we get:

$$y^2 = \gamma_3 x^3 + \gamma_2 x^2 + \gamma_1 x + \gamma_2.$$

Replace $y$ by $\gamma_3^2 y$ and $x$ by $\gamma_3 x$; this gives $x^3$ and $y^2$ the same coefficient. Rescale and we get

$$y^2 = x^3 + \delta_2 x^2 + \delta_1 x + \delta_0.$$

Replace $x$ by $x - \frac{\delta_2}{3}$, and we get an equation

$$y^2 = x^3 + Ax + B$$

with $A, B \in k$.

Note we have used that $k$ has characteristic not 2 or 3. Completion of squares doesn't work in characteristic 2, and the first step in solving cubics doesn't work in characteristic 3. So in characteristic 3, you can get $y^2 = \text{(cubic)}$, but for characteristic 2, you can't really simplify the equation at all. In general, if $A$ is a $d$-dimensional abelian variety, it is noted in [ST68] that primes $p \leqslant 2d+1$ can be especially nasty.

We will need to reduce elliptic curves modulo 2 and 3. Given $E_{/\mathbf{Q}}$, there is an integer $N$, called the *conductor* of $E$, that measures the "badness" of the singularities in the reductions of $E$. For $p \geqslant 3$, we have $v_p(N) \leqslant 2$. For $p = 3$, we just have $v_3(N) \leqslant 4$, and for $p = 2$, we can have $v_2(N) = 6$.

We'll continue under the assumption that $k = \mathbf{Q}$. Write our curve $E_{/\mathbf{Q}}$ as

$$y^2 = x^3 + \frac{N_1}{D} x + \frac{N_2}{D},$$

with $N_1, N_2, D \in \mathbf{Z}$. Make the change of variables

$$x \mapsto x/D^2$$
$$y \mapsto y/D^3.$$

Then multiply through by $D^6$ and relabel. We get

$$y^2 = x^3 + Ax + Bx,$$

with $A, B \in \mathbf{Z}$. For any prime $p$, say $p^4 \mid A$ and $p^6 \mid B$. Make the change of variables

$$x \mapsto p^2 x$$
$$y \mapsto p^3 y.$$

you can rescale again until one of these possibilities fail. We end up with a Weierstrass form $y^2 = x^3 + Ax + B$ with $p^4 \mid A \Rightarrow p^6 \nmid B$. This is the *minimal model* of $E$.

Now we can study $E_{/\mathbf{Q}}$ and write $E = E_{A,B}$, given by $y^2 = x^3 + Ax + B$, for $A, B \in \mathbf{Z}$ with ($p^4 \nmid A$ or $p^6 \nmid B$). Recall that $E_{A,B}$ is singular exactly if

$$\begin{pmatrix} 2y & 3x^2 + A \end{pmatrix} = 0$$

for some $(x, y) \in E(\overline{\mathbf{Q}})$. This can happen only if $27B^2 + 4A^3 = 0$. The set of such $(A, B)$ is thin.

This procedure works over $\mathbf{Z}[\frac{1}{6}] \subset \mathbf{Z}$.

## 2.3 Group law on an elliptic curve

Let $E_{/k}$ be an elliptic curve in strong Weierstrass form $y^2 = x^3 + Ax + B$. We will give $E$ the structure of an abelian variety over $k$. We declare $P + Q + R = 0$ if $P$, $Q$, and $R$ lie on the same line through $E$ in $\mathbf{P}^2$. This determines a morphism $E \times E \to E$ defined over $k$. From the definition, it is clear that addition is commutative. We won't verify that the group law is associative. It can be directly, but this is very tedious. A more conceptual approach is to use the Picard variety. To summarize:

**Theorem 2.3.1.** *Let $E_{/k}$ be an elliptic curve given by $y^2 = x^3 + Ax + B$. Then $E$ has the unique structure of an abelian variety such that* $(0 : 1 : 0)$ *is the identity element.*

*Proof.* Existence follows from the fact that the map $E \to \operatorname{Pic}^0(E)$ is an isomorphism of varieties over $k$. Uniqueness follows from Proposition 1.13 of [GEM14]. □

Let $P = (\alpha, \beta)$. What is $2P = P + P$? We can implicitly differentiate $y^2 = x^3 + Ax + B$ to get

$$y' = \left.\frac{3x^2 + A}{2y}\right|_{(\alpha,\beta)} = \frac{3\alpha^2 + A}{2\beta}.$$

We can solve the equation

$$\left(\beta + \frac{3\alpha^2 + A}{2\beta}(x - \alpha)\right)^2 = x^3 + Ax + B,$$

to see that the third root is $\frac{(3\alpha^2+A)^2}{4\beta^2} - 2\alpha$. So

$$x_{2P} = \frac{(3\alpha^2 + A)^2}{4(\alpha^3 + A\alpha + B)} - 2\alpha,$$

and $y_{2P}$ can be computed similarly.

Given $Q = (\alpha, \beta) \in E(\overline{K})$, let's find $P$ such that $2P = Q$. Since $\#E[2](\overline{K}) = 4$, we expect four such $P$. It comes down to solving the equation

$$\frac{(3\alpha^2 + A)^2}{4(\alpha^3 + A\alpha + B)} - 2\alpha = r.$$

The polynomial on the left has degree 4, so there will indeed be four $P$.

In general, given $Q \in E(\overline{K})$, the equation $nP = Q$ has $n^2$ solutions, provided $n$ is invertible in $k$. Also, if $n$ is invertible in $k$, then $E[n] \simeq (\mathbf{Z}/n)^2$, and $G_K = \operatorname{Gal}(\overline{K}/K)$ acts on $E[n]$ by group automorphisms. This is really easy. To verify this, all we need to check is that $\sigma(P + Q) = \sigma(P) + \sigma(Q)$ for all $\sigma \in G_K$ and $P, Q \in E(\overline{K})$. But $x_{P+Q}$ and $y_{P+Q}$ are rational functions in the coordinates of $P$ and $Q$, *defined over* $K$. If $f \in K(t)$ is a rational function, then $\sigma(f(x)) = f(\sigma(x))$ for all $x \in \overline{K}$, whence $\sigma(x_{P+Q}) = x_{\sigma P + \sigma Q}$.

Given $E_{/\mathbf{Q}}$, set $a_p = p + 1 - \#E(\mathbf{F}_p)$, where $E(\mathbf{F}_p)$ is the $\mathbf{F}_p$-points of the projective curve associated to $E$. Note that $p + 1 = \mathbf{P}^1(\mathbf{F}_p)$. Note that this only makes sense for $p \nmid \Delta$.

**Theorem 2.3.2** (Hasse). *$|a_p| \leqslant 2\sqrt{p}$.*

Recall the $L$-function of $E$ is defined in terms of the $a_p$:

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

If $\Re s = \frac{3}{2} + \epsilon$, then

$$\left|-\frac{a_p}{p^s} + \frac{p}{p^{2s}}\right| \leqslant \frac{2}{p^{1+\epsilon}} + \frac{1}{p^{2+2\epsilon}} \leqslant p^{-1-\epsilon/2},$$

at least for $p \gg 0$. We know that $\prod(1-p^{-s})^{-1}$ converges for $\Re s > 1$. Thus $L(E,s)$ is defined for $\Re s > 3/2$.

We know that $|a_p| \leqslant p+1$. This gives well-definedness of $L(E,s)$ for $\Re s > 2$, and it isn't too hard to get $\Re s > 3/2$. The following theorem was proved in the course of Wiles' proof of Fermat's Last Theorem.

**Theorem 2.3.3.** *$L(E,s)$ has a meromorphic continuation to $\mathbf{C}$.*

Recall the weak Birch and Swinnerton-Dyer conjecture:

**Conjecture 2.3.4.** *$\operatorname{ord}_{s=1} L(E,s) = \operatorname{rk} E$.*

Note that $\operatorname{rk} E$ is global data, while the $a_p$ only depend on the reduction $E_{/\mathbf{F}_p}$. The following theorem was known as the Sato-Tate conjecture.

**Theorem 2.3.5** (Taylor et. al.). *Define $\theta_p$ by $\frac{a_p}{2\sqrt{p}} = \cos(\theta_p)$ and $\theta_p \in [-\pi/2, \pi/2)$. Then*

$$\lim_{X\to\infty} \frac{\#\{p \leqslant X : c \leqslant \theta_p \leqslant d\}}{\pi(X)} = \frac{2}{\pi}\int_c^d \sin^2(u)\,\mathrm{d}u.$$

*Proof.* In [Ser68], Serre outlined a strategy. It relied on $L(\operatorname{sym}^n E, s)$ being analytic at 1 for infinitely many $n$. At the time, we didn't even know this for $n=1$! This requires a vast generalization of Wiles et. al. (who worked with $n=1$). □

In some ways, the Sato-Tate conjecture is unsatisfying because it says that "all (non-CM) elliptic curves are the same." On the other hand, the Birch and Swinnerton-Dyer conjecture is about how local data of elliptic curves gives information about global data.

**Conjecture 2.3.6** (Harris). *Let $E_1$, $E_2$ be non-isogenous (up to twist) elliptic curves over $\mathbf{Q}$. Then the Sato-Tate distributions of $E_1$, $E_2$ are independent.*

See [Har] for a careful statement and motivation. There is an obvious family to pairwise non-isogenous families $\{E_1, \cdots, E_n\}$, but there isn't a clear approach to prove this.

## 2.4 Kummer theory

Let $K \subset L$ be a Galois field extension. There is a version of Galois theory for $G = \mathrm{Gal}(L/K)$, but we need to give $G$ a topology. Let a basis of 1 be the subgroups of the form $G_x = \mathrm{Stab}_G(x)$ for $x \in L$. Under this topology (the *Krull topology*), the group $G$ is compact, Hausdorff, and totally disconnected. See Chapter IV of [Neu99] for details.

Let $k$ be a field, $p$ a prime invertible in $k$ such that $\boldsymbol{\mu}_p \subset k$. Let $k^{(p)}$ be the composite of all $\mathbf{Z}/p$-Galois extensions of $k$ in $\overline{k}$.

**Theorem 2.4.1.** *The pairing* $\mathrm{Gal}(k^{(p)}/k) \times k^\times/p \to \boldsymbol{\mu}_p$ *given by*

$$\langle \sigma, x \rangle = \frac{\sigma(x^{1/p})}{x^{1/p}}$$

*is a well-defined perfect pairing of topological groups.*

*Proof.* Say $\langle \sigma, x_0 \rangle = 1$ for all $\sigma \in \mathrm{Gal}(k^{(p)}/k)$. Then $\sigma(x_0^{1/p}) = x_0^{1/p}$ for all $\sigma$. This implies $x_0^{1/p}$ is fixed by $\mathrm{Gal}(k^{(p)}/k)$, which implies $x_0^{1/p} \in k$, which implies $x_0 \in (k^\times)^p$.

Now suppose $\langle \sigma_0, x \rangle = 1$ for all $x \in k^\times$. So $\sigma_0(x^{1/p}) = x^{1/p}$ for all $x \in k^\times$. In particular, $\sigma_0$ is trivial on $k(x^{1/p} : x \in k^\times)$. We want for this field to be $k^{(p)}$. It suffices to check that if $K/k$ is a $\mathbf{Z}/p$-extension, then $K = k(x^{1/p})$ for some $x \in k$. Recall Hilbert's Theorem 90: an element $x \in K^\times$ satisfies $\mathrm{N}_{K/k}(x) = 1$ if and only if there exists $y$ such that $x = y/\tau(y)$, where $\tau$ is any generator of $\mathrm{Gal}(K/k)$. Since $\mathrm{N}_{K/k}(\zeta_p) = \zeta_p^p 1$, we get $\zeta_p = y/\tau(y)$, so $\tau(y) = \zeta_p^{-1} y$. Since $y \in K \smallsetminus k$, we know that $K = k(y)$. But $\tau(y) = \zeta_p^{-1} y$ tells us that $y^p \in k$, so $K$ is generated by a $p$-th root of an element of $k$. □

See [Neu99, IV §3] for a proof. The theorem, correctly rephrased, works with arbitrary $n$ invertible in $k$. Hilbert's Theorem 90 is a very special case of the extremely general result that $\mathrm{H}^1(X_{\text{ét}}, \mathbf{G}_{\mathrm{m}}) = \mathrm{Pic}(X)$ for any noetherian scheme $X$ [SGA $4\frac{1}{2}$, I 2.2.3].

As an example, for $p = 2$ and $k = \mathbf{R}$, we see that there is only one $\mathbf{Z}/2$-extension of $\mathbf{R}$. This can be used to show that $\mathbf{C}$ has no solvable extensions.

There is a purely geometric approach to Kummer theory. Let $X$ be a scheme on which $n$ is invertible. The *Kummer exact sequence* is the sequence

$$1 \to \boldsymbol{\mu}_n \to \mathbf{G}_{\mathrm{m}} \xrightarrow{n} \mathbf{G}_{\mathrm{m}} \to 1$$

of étale sheaves on $X$. The long exact sequence in sheaf cohomology gives us a short exact sequence:

$$1 \to \mathscr{O}(X)^\times/n \to \mathrm{H}^1(X, \boldsymbol{\mu}_n) \to \mathrm{Pic}(X)[n] \to 1.$$

Since $\boldsymbol{\mu}_n \simeq \mathbf{Z}/n$, we have $\mathrm{H}^1(X, \boldsymbol{\mu}_n) = \hom(\pi_1(X), \mathbf{Z}/n)$. When $X = \mathrm{Spec}(k)$, we have $\mathrm{Pic}(X) = 0$, so $k^\times/n \simeq \hom(G_k, \mathbf{Z}/n)$. For arbitrary $X$, the Kummer exact sequence can be used to get a pretty good grasp of $\pi_1(X)^{\mathrm{ab}}$. See [Sza09, p. 5.8.3] for details.

Kummer theory is used to study solvable extensions in classical algebraic number theory. More generally, it is used in class field theory to build the abelian extensions of a field. Finally, it is used in local and global duality theorems in the cohomology of $G_{\mathbf{Q}}$, $G_{\mathbf{Q}_l}$.

The Weil pairing is a kind of "geometric Kummer theory." It is a perfect pairing $E[m] \times E[m] \to \boldsymbol{\mu}_m$. This means that $E[m] \simeq \hom(E[m], \boldsymbol{\mu}_m) = E[m]^\vee$, the dual in the correct sense. So $E[m]$ is self-dual in some sense. Even better, $E[m]^\vee \simeq \mathrm{H}^1_{\mathrm{et}}(E, \mathbf{Z}/m)$, and the Weil pairing is comes from the cup-product pairing in étale cohomology:

$$\mathrm{H}^1(E, \mathbf{Z}/m) \times \mathrm{H}^1(E, \mathbf{Z}/m) \to \mathrm{H}^2(E, \mathbf{Z}/m).$$

**Example 2.4.2.** Let $p = 2$ and $k = \mathbf{Q}$. Then $\mathbf{Q}^{(2)} = \mathbf{Q}(\sqrt{-1}, \sqrt{l} \text{ all prime } l)$. Note that

$$\mathrm{Gal}(\mathbf{Q}^{(2)}/\mathbf{Q}) \simeq \prod_{l,-1} \mathbf{Z}/2.$$

On the other hand, $\mathbf{Q}^\times/2 = \bigoplus_{l,-1} \mathbf{Z}/2$. The point is that the Kummer pairing is between a discrete group and a (uncountable) compact group. ▷

In general, Galois groups are either finite or uncountable (because they're compact). There is one case in which we can explicitly describe the entire absolute Galois group of a field.

**Theorem 2.4.3.** *Let $\mathbf{F}_q$ be the finite field of cardinality $q$. For each $n \geqslant 1$, there is a unique degree $n$ extension $\mathbf{F}_{q^n}/\mathbf{F}_q$. This extension satisfies* $\mathrm{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q)$.

*Proof.* Find such $\mathbf{F}_{q^n}$ in $\overline{\mathbf{F}_q}$. It has cardinality $q^n$, and $\mathbf{F}_{q^n}^\times \simeq \mathbf{Z}/(q^n - 1)$. Indeed, if it wasn't cyclic, then $x^{q^n} - 1$ has too many roots in $\mathbf{F}_{q^n}$. The splitting field of $x^{q^n} - x$ gives a degree $n$ extension of $\mathbf{F}_q$, and this must be unique because any other degree-$n$ extension of $\mathbf{F}_q$ must contain all $(q^n - 1)$-th roots of unity. □

## 2.5 Weil pairing

We start with some needed facts, which are proved using Riemann-Roch. Let $k$ be a field, $n \geqslant 2$ an integer invertible in $k$, and let $E_{/k}$ be an elliptic curve. Suppose $D = \sum n_x(x)$ is a divisor on $E$.

1. If $\deg(D) = 0$, then $D = \mathrm{div}(f)$ for some rational function $f$ on $E$ if and only if $\sum [n_x]x = 0$ as an element of $E(\overline{k})$.
2. If $x \neq 0$ in $E$, then $(x) - (0) \neq \mathrm{div}(f)$ in $\mathrm{Pic}^\circ(E)$.

Given $x, y \in E[n]$, we'll define $e_n(x, y) \in \boldsymbol{\mu}_n$ following [Sil09, III §8]. By fact 1 above, the divisor $D = n(y) - n(0)$ is $\mathrm{div}(f)$ for some function $f$ on $E$. Let $y'$ be such that $[n]y' = y$, and consider

$$[n]^* D = \sum_{z \in E[n]} (y' + z) - (z),$$

where $y' + z$ is defined using the addition in $E$. This is a degree-0 diivisor, and within $E$, we have $\sum_{z \in E[n]}(y' + z - z) = n^2 y' = ny = 0$. Thus $[n]^* D = \operatorname{div}(g)$ for some $g$, and it is easy to check that we must have $f = cg^n$ for some $c \in \overline{k}$. We can replace $g$ by a scalar multiple to get $f = g^n$. Note that $g(t+x)^n = f([n]t+[n]x) = f([n]t) = g(t)^n$. Thus we can define

$$e_n(x, y) = \frac{g(t + x)}{g(t)}$$

for any $t$ in the domain of $g$. Note that this definition is asymmetric with respect to $x, y$. Also $f, g$ are independent of $y$.

**Theorem 2.5.1.** *Let $E_{/k}$ be an elliptic curve. Then:*

1. $e_n(x_1 + x_2, y) = e_n(x_1, y)e_n(x_2, y)$
2. $e_n(x, y_1 + y_2) = e_n(x, y_1)e_n(x, y_2)$
3. $e_n(x, x) = 1$, *so* $e_n(x, y) = e_n(y, x)^{-1}$
4. $e_n(x, y)^\sigma = e_n(x^\sigma, y^\sigma)$ *for all* $\sigma \in G_k$.
5. $e_n(x, y) = 1$ *for all* $x$ *implies* $y = 0$*, and vice versa.*

*Proof.* This is Proposition III.8.1 in [Sil09].

1. We have

$$\begin{aligned} e_n(x_1 + x_2, y) &= \frac{g(t + x_1 + x_2)}{g(t)} \\ &= \frac{g((t + x_1) + x_2)}{g(t + x_1)} \frac{g(t + x_1)}{g(t)} \\ &= e_n(x_1, y)e_n(x_2, y). \end{aligned}$$

The other part is more involved. Call $y_3 = y_1 + y_2$. Let $f_i, g_i$ be the functions for $y_i$. We must relate $g_3$ to $g_1, g_2$. Put $D = (y_3) - (y_1) - (y_2) + (0)$; this has degree 0, and the sum of its points is 0 in $E$, so $D = \operatorname{div}(h)$ for some $h$. Recall that $\operatorname{div}(f_i) = n(y_i) - n(0)$. Thus

$$\operatorname{div}\left(\frac{f_3}{f_1 f_2}\right) = \operatorname{div}(h^n).$$

Thus $f_3 = cf_1 f_2 h^n$ for some $c$. It follows that $f_3 \circ [n] = cf_1 \circ [n] f_2 \circ [n](h \circ [n])^n$, so $g_3^n = g_1^n g_2^n (h \circ [n])^n$. Take $n$-th roots: we get $g_3 = \widetilde{c} g_1 g_2 (h \circ [n])$. We can now compute:

$$\begin{aligned} e_n(x, t_3) &= \frac{g_3(t + x)}{g_3(t)} \\ &= \frac{g_1(t + x)g_2(t + x)h([n]t + [n]x)}{g_1(t)g_2(t)h([n]t)} \\ &= e_n(x, y_1)e_n(x, y_2). \end{aligned}$$

4. We compute

$$e_n(x,y)^\sigma = \left(\frac{g(t+x)}{g(t)}\right)^\sigma = \frac{g^\sigma(t^\sigma + x^\sigma)}{g^\sigma(t^\sigma)} = e_n(x^\sigma, y^\sigma).$$

We leave the rest of the proof as an exercise. □

The alternating property and Galois-equivariance of the Kummer pairing have a nice consequence. Choose a generating set $x, y \in E[n]$, $\sigma \in G_k$. Then $\sigma$ acts on $E[n]$ via some matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z}/n)$ with respect to the basis $\{x, y\}$. Suppose $e_n(x,y) = \zeta \in \boldsymbol{\mu}_n$. Then $\sigma(\zeta) = \zeta^{\chi(\sigma)}$, where $\chi : G_k \to \mathrm{GL}_1(\mathbf{Z}/n)$ is the cyclotomic character. Write $\rho_{E,n} : G_k \to \mathrm{GL}_2(\mathbf{Z}/n)$ for the representation coming from $E$. We claim that $\det \rho_{E,n} = \chi_n$. All we need to show is that $e_n(x,y)^\sigma = \zeta^\sigma = \zeta^{ad-bc}$. We know that $e_n(x,y)^\sigma = e_n(x^\sigma, y^\sigma) = e_n(ax+cy, bx+dt)$; we're left with $e_n(x,y)^{ab-cd}$, as desired.

The Weil pairing makes $E[n]$ self-dual as a representation of $G_k$. Let $X_{/k}$ be a smooth projective curve. There is a canonical pairing ("cup-product"):

$$\mathrm{H}^1_{\text{ét}}(X, \boldsymbol{\mu}_n) \times \mathrm{H}^1_{\text{ét}}(X, \boldsymbol{\mu}_n) \to \mathrm{H}^2_{\text{ét}}(X, \boldsymbol{\mu}_n) = \boldsymbol{\mu}_n.$$

Moreover, $\mathrm{H}^1_{\text{ét}}(X, \boldsymbol{\mu}_n) \simeq \mathrm{Jac}(X)[n]$, where $\mathrm{Jac}(X)$ is the *Jacobian* of $X$, a $g$-dimensional abelian variety containing $X$. Thus $\mathrm{Jac}(X)$ has a group structure, while $X$ does not.

The algebraic analogue of the notion of a local diffeomorphism is a *finite étale cover*. It turns out that $\mathrm{Jac}(X)[n]$ parameterizes degree-$n$ finite étale covers of $X$ with abelian Galois group. There is a "Weil pairing" on $\mathrm{Jac}(X)$ coming from the Poincaré bundle, but it agrees with the cup-product.

There is an analogy between Kummer theory and the Weil pairing. Recall that if $k$ is a field of characteristic not $p$ which contains all $p$-th roots of unity, and if $k^{(p)}$ is the maximal abelian $p$-extension of $k$, then the obvious pairing $\mathrm{Gal}(k^{(p)}/k) \times k^\times/p \to \boldsymbol{\mu}_p$ is perfect.

## 2.6 Isogenies

An *isogeny* will be morphisms between elliptic curves, defined over the base field. Since elliptic curves are varieties, we should require these morphisms to be polynomial (or rational). Since elliptic curves have a group law, we also want these morphisms to respect this structure. Summing up: if we think of elliptic curves as group objects in the category of projective varieties (projective ⇒ abelian), an isogeny is a non-constant morphism of such objects. More formally,

**Definition 2.6.1.** *Let $E_1, E_2$ be elliptic curves over $k$, $\phi : E_1 \to E_2$ a morphism. We say $\phi$ is an* isogeny *if it is a dominant morphism of varieties, and satisfies $\phi(0) = 0$.*

It turns out that if $\phi$ is an isogeny, then $\phi$ is actually a morphism of group schemes. If $\phi : E_1 \to E_2$ is defined over $k$, then $\ker \phi$ is $G_k$-stable as a group (not pointwise). Given $E_{/\mathbf{Q}}$ and an isogeny $\phi : E \to E$, usually $\phi$ is $[n]$ for some $n \in \mathbf{Z} \smallsetminus 0$. When there are isogenies not of this form, amazing congruences happen.

**Example 2.6.2.** Let $\Delta = q \prod_{n \geqslant 1} (q - 1^n)^{24} = \sum \tau(n) q^n$; the first few terms are:

$$\Delta = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 + \cdots .$$

Ramanujan observed that $(m, n) = 1$ implies $\tau(mn) = \tau(m)\tau(n)$. He also observed that for a prime $p$, $\tau(p^{r+1}) = \tau(p)\tau(p^r) - p^{11}\tau(p^{r-1})$. Also, $|\tau(p)| \leqslant 2p^{11/2}$ (this is hard: it was proved by Deligne in the course of the Weil conjectures). Finally,

$$\tau(n) \equiv \sigma_{11}(n) = \sum_{d \mid n} d^{11} \pmod{691}.$$

This congruence is a manifestation of the "existence of a non-trivial isogeny." $\triangleright$

This example is one of the first cases of a congruence between a *cusp form* and *Eisenstein series*. The first paper to make much use of this idea is [Rib76], in which Ribet used modular forms to prove the converse of Kummer's criterion. The ideas here were crucial in the proof of Iwasawa's Main Conjecture, Skinner and Urban's recent work, and many other parts of modern number theory. See Mazur's survey article [Maz11] for an excellent overview of this circle of ideas.

If $V_{/k}$ is an irreducible variety, it has a function field $k(V)$. If $\phi : V \to W$ is a morphism of varieties, there is a inclusion $\phi^* : k(W) \to k(V)$, assuming $\phi$ is surjective. So the Frobenius $\mathbf{P}^1_{/\mathbf{F}_p} \to \mathbf{P}^1_{/\mathbf{F}_p}$ sending $(x_0 : x_1)$ to $(x_0^p : x_1^p)$ induces a map $\mathbf{F}_p(t) \to \mathbf{F}_p(t)$, $f(t) \mapsto f(t^p)$. The field extension $\mathbf{F}_p(t^{1/p})/\mathbf{F}_p(t)$ is purely inseparable, and has degree $p$. In characteristic $p$, the geometric Frobenius $\mathrm{Fr} : E \to E$ an isogeny, but *not* an isomorphism of varieties, as "the inverse" involves taking $p$-th roots. It turns out that Fr has degree $p$, and is purely inseparable.

In characteristic zero, $\deg(\phi)$ is $\#\phi^{-1}(x)$ for "generic" $x$, and $[k(E_1) : \phi^* k(E_2)]$ in characteristic $p$. One has to check that these two quantities agree in characteristic zero. If $V_{/\mathbf{F}_q}$ is a $d$-dimensional variety, then $\mathrm{Fr}_q : V \to V$ has degree $q^d$.

Let $E_{/\mathbf{Q}}$ be an elliptic curve. Consider an isogeny $\phi : E \to \widetilde{E}$ of degree $p$ defined over $\mathbf{Q}$. Since $\# \ker(\phi) = p$, we have $\ker(\phi) \subset E[p]$. Moreover, $\ker(\phi)$ is stable under the action of $G_{\mathbf{Q}}$. Note that $\widetilde{E} = E / \ker \phi$. So we have a pair $(E, C)$, where $E_{/\mathbf{Q}}$ is an elliptic curve, and $C \subset E$ is a subgroup of order $p$ defined over $\mathbf{Q}$. Alternatively, we could study pairs $(E, P)$, where $E_{/\mathbf{Q}}$ is an elliptic curve and $P \in E[p](\mathbf{Q})$ has order $p$. Since $G_{\mathbf{Q}}$ acts on $E[p]$, we have a representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}/p)$. In the first case, the image fits inside $\begin{pmatrix} * & * \\ & * \end{pmatrix}$, and in the second case it looks like $\begin{pmatrix} 1 & * \\ & \varepsilon \end{pmatrix}$, where $\varepsilon : G_{\mathbf{Q}} \to \mathbf{F}_p^\times$ must be the cyclotomic character, defined by $\sigma(\zeta_p) = \zeta_p^{\varepsilon(\sigma)}$.

There are moduli spaces for pairs $(E, C)$ and $(E, P)$ as above, namely the modular curves $Y_0(p)_{/\mathbf{Q}}$ and $Y_1(p)_{/\mathbf{Q}}$. There is a natural isomorphism $Y_0(p)(\mathbf{C}) = \mathfrak{H}/\Gamma_0(p)$, where

$$\Gamma_0(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) : c \equiv 0 \pmod p \right\}.$$

The curve $Y_0(p)$ is affine; let $X_0(p)$ be its compactification. The classification of pairs $(E, C)$ defined over $\mathbf{Q}$ comes down to the study of $Y_0(p)(\mathbf{Q})$. The complex points of $Y_1(p)$ are in bijection with $\mathfrak{H}/\Gamma_1(p)$, where

$$\Gamma_1(p) = \left\{ \gamma \in \mathrm{SL}_2(\mathbf{Z}) : \gamma \equiv \begin{pmatrix} 1 & * \\ & 1 \end{pmatrix} \pmod p \right\}.$$

**Theorem 2.6.3** (Mazur)**.** *$Y_0(p)(\mathbf{Q}) = \varnothing$ for all $p \geqslant 11$.*

This implies that there does not exist an $E_{/\mathbf{Q}}$ and (for $p \geqslant 11$) $P \in E(\mathbf{Q})$ of order $p$. This theorem is proved in the seminal paper [Maz77]. This allows the classification of $E(\mathbf{Q})_{\mathrm{tors}}$ for $E_{/\mathbf{Q}}$. Mazur's theorem tells us that $p \nmid E(\mathbf{Q})_{\mathrm{tors}}$ for $p \geqslant 11$. All that remains are the primes $p < 11$, and this is a finite list.

Note that an isogeny can be given by a pair $(E, C)$, where $E_{/k}$ is an elliptic curve and $C_{/k}$ is a subgroup scheme of $E$. The quotient $E/C$ must be defined in the appropriate sense – this can get pretty complicated.

Are isogenies ramified? Let's restrict to characteristic zero. We are asking: if $\phi : E_1 \to E_2$ is an isogeny, are there points $x \in E_2(\bar{k})$ such that $\#\phi^{-1}(x) < \deg(\phi)$? The answer is no: isogenies are étale, hence unramified. This is because $\phi$ is a group homomorphism, so $\#\phi^{-1}(x) = \#\phi^{-1}(0) = \deg(\phi)$ for all $x$. If $\phi : C_1 \to C_2$ is a map between curves over $k$, then if one of the curves isn't elliptic, it's possible for $\phi$ to have ramification points. The Riemann-Hurwitz formula gives us a bound on possible ramification.

## 2.7 Jacobians

Let $C_{/k}$ be a curve. The *Jacobian* of $C$, denoted $\mathrm{Jac}(C)$, is a group variety build from $C$, which has a natural map $C \to \mathrm{Jac}(C)$. If $C$ has genus $g$, then $\mathrm{Jac}(C)$ is $g$-dimensional.

The *divisor group* of $C$, denoted $\mathrm{Div}(C)$, is the free abelian group on $C(\bar{k})$. It contains a subgroup $\mathrm{Div}^\circ(C)$ consisting of degree-zero divisors. There is a smaller subgroup of *principal divisors*, which are of the form $\mathrm{div}(f)$ for $f \in k(C)^\times$. One can show that $\deg(\mathrm{div}(f)) = 0$ for all such $f$. Define $\mathrm{Pic}^\circ(C)$ to be the quotient $\mathrm{Div}^\circ(C)/\,\mathrm{div}(k(C)^\times)$.

**Theorem 2.7.1.** *Let $C_{/k}$ be a genus-$g$ curve. Then $\mathrm{Pic}^\circ(C)$ naturally has the structure of the $\bar{k}$-points of a $g$-dimensional abelian variety over $k$.*

Note that we've only constructed $\mathrm{Jac}(C)$ as an abstract group. The underlying variety can be quite complicated. See [Kle05] for a survey of general Picard schemes.

**Example 2.7.2.** Work over $\mathbf{C}$. An elliptic curve $E_{/\mathbf{C}}$ is just a complex torus. Let $L_1, L_2$ be generators for $\pi_1(E)$. Since $E$ has genus 1, the space of holomorphic differential forms is one-dimensional, spanned by $\omega$. Let $A_i = \int_{L_i} \omega$. Then $\mathbf{C}/\langle A_1, A_2\rangle \simeq E(\mathbf{C})$. ▷

If $C$ has genus $g \geqslant 2$, there are $2g$ loops $L_1, \dots, L_{2g}$ and $g$ holomorphic differentials $\omega_1, \dots, \omega_g$. One gets $\operatorname{Jac}(C)(\mathbf{C}) = \mathbf{C}^g/\Lambda$, where $\Lambda$ is the lattice spanned by the vectors

$$\int_{L_i} \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_g \end{pmatrix} \qquad (1 \leqslant i \leqslant 2g).$$

Back to an elliptic curve $E_{/k}$. There is a map $\kappa : E \to \operatorname{Pic}^\circ(E)$; this is an isomorphism. It sends $x \in E$ to the divisor $(x) - (0)$. If $\phi : E_1 \to E_2$ is an isogeny, it induces a map $\phi^* : \operatorname{Pic}^\circ(E_2) \to \operatorname{Pic}^\circ(E_1)$ by pullback of divisors: $D \mapsto \phi^* D$, where

$$\phi^* \sum n_x (x) = \sum n_x \phi^{-1}(x).$$

We can use our isomorphisms $E_i \xrightarrow{\sim} \operatorname{Pic}^\circ(E_i)$ to get an isogeny $\phi^\vee : E_2 \to E_1$, given by $\phi^\vee = \kappa_1^{-1} \circ \phi^* \circ \kappa_2$. We call $\phi^\vee : E_2 \to E_1$ the *dual isogeny* to $\phi$. We have not (and will not) checked, but it is true, that:

- $\operatorname{Pic}^\circ(C)$ is a smooth projective variety over $k$.
- $\kappa$ is an isomorphism of varieties.
- $\phi^\vee$ is an isogeny.

It turns out that $\deg : \hom_k(E, E) \to \mathbf{N}$ is a positive definite quadratic form. This depends on the fact that $\phi^\vee \circ \phi = [\deg \phi]$. The degree map is clearly positive-definite. To show that it's a quadratic form, just check that $\deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$ is bilinear. We can compute:

$$\begin{aligned} (\phi + \psi)^\vee(\phi + \psi) - \phi^\vee\phi - \psi^\vee\psi &= \phi^\vee\phi + \psi^\vee\phi + \phi^\vee\psi + \psi^\vee\psi - \phi^\vee\phi - \psi^\vee\psi \\ &= \phi^\vee\psi - \psi^\vee\phi, \end{aligned}$$

which yields the desired result.

In general, if $d : A \to \mathbf{Z}$ is a positive definite quadratic form for some abelian group $A$, then $|d(\psi - \phi) - d(\psi) - d(\phi)| \leqslant 2\sqrt{d(\phi)d(\psi)}$. This is basically Cauchy-Schwarz.

**Theorem 2.7.3.** *Let $E_{/\mathbf{F}_q}$ be an elliptic curve. Then $|\#E(\mathbf{F}_q) - q - 1| \leqslant 2\sqrt{q}$.*

*Proof.* Given $E_{/\mathbf{F}_q}$, the map $\operatorname{Fr}_q - 1$ is separable. Moreover, $\ker(\operatorname{Fr}_q - 1) = E(\mathbf{F}_q)$. Now we use Cauchy-Schwarz for the isogenies $\phi = \operatorname{Fr}$, $\psi = 1$. We get

$$\begin{aligned} |\#E(\mathbf{F}_q) - q - 1| &= |\deg(\operatorname{Fr} - 1) - \deg(\operatorname{Fr}) - \deg(1)| \\ &\leqslant 2\sqrt{\deg(\operatorname{Fr})\deg(1)} \\ &= 2\sqrt{1 \cdot q}. \end{aligned}$$

□

This is a real theorem. A Putnam exam had the following question: consider the equation $y^2 = x^3 + Ax + B$ for $A, B \in \mathbf{Z}$. Show that there exist solutions modulo $p$ for all $p$. Assume the induced (projective) curve $E$ is smooth. It is also true that $E_{/\mathbf{F}_p}$ is smooth for all but finitely many $p$. For these good $p$, we know that $|\#E(\mathbf{F}_p) - p - 1| \leqslant 2\sqrt{p}$. The curve $E$ has no affine solutions only when $\#E(\mathbf{F}_p) = 1$, which gets $1 < 2/\sqrt{p}$. This gives us the solution for all $p$ of good reduction.

Note that as $q \to \infty$, we get $\#E(\mathbf{F}_q) \sim q + 1$, which clearly goes to infinity. So for $q$ large, *all* $E_{/\mathbf{F}_q}$ will have nonzero points. If $(6, q) = 1$, then $E_{/\mathbf{F}_q}$ is of the form $y^2 = x^3 + Ax + B = f(x)$. Define a character $\chi : \mathbf{F}_q \to \mathbf{Z}$ by

$$\chi(x) = \begin{cases} 1 & x \in (\mathbf{F}_q^\times)^2 \\ -1 & x \notin (\mathbf{F}_q^\times)^2 \\ 0 & x = 0 \end{cases}.$$

We have

$$\#E(\mathbf{F}_q) = 1 + \sum_{x \in \mathbf{F}_q} (\chi(f(x)) + 1) = q + 1 + \sum_{x \in \mathbf{F}_q} \chi(f(x)).$$

So there is some finite Fourier analysis going on here – this has a distant relation with the Langlands program. Recall that in characteristic $p$, if you want a degree $p$ separable extension, you don't study $x^p - \alpha$ – rather, you study Artin-Schreier theory and study equations of the form $x^p - x - \alpha$. In general, we want *separable* polynomials, where $g$ is separable if $(g, g') = 1$.

**Theorem 2.7.4.** *No elliptic curve $E_{/\mathbf{Q}}$ given by $y^2 = x^3 + Ax + B$ with $A, B \in \mathbf{Z}$ has good reduction at all primes, i.e. is smooth modulo $p$ for all $p$.*

*Proof.* For $E$ to be smooth modulo $p$ for all $p$, we need $x^3 + Ax + B$ to have distinct roots modulo $p$ for all $p$. Let $\alpha, \beta, \gamma$ be the roots, and set $\Delta = ((\alpha - \beta)(\beta - \gamma)(\gamma - \alpha))^2$. You can check that $\Delta = \pm(4A^3 + 27B^2)$. If $\Delta \notin \{\pm 1\}$, then some prime $p \mid \Delta$, which means that $E_{/\mathbf{F}_p}$ is singular. So we need $\Delta = \pm 1$, which gives $4A^3 \equiv \pm 1 \pmod 9$. This means $x^3 \in \{0, \pm 1\} \pmod 9$, and there is no way that $0, \pm 4$ can be congruent to $\pm 1$ modulo 9. □

It is known that there are finite extensions $L/\mathbf{Q}$ and elliptic schemes $E_{/\mathcal{O}_L}$. On the other hand, we have the following:

**Theorem 2.7.5** (Fontaine)**.** *There are no abelian varieties over $\mathbf{Z}$.*

*Proof.* See Fontaine's beautiful paper [Fon85]. □

Let $k$ be a field of characteristic $p$ and $E_{/k}$ be an elliptic curve $y^2 = x^3 + ax + b$. Then $\mathrm{Fr}_q$ is *not* a morphism $E \to E$. Rather, it is a morphism $E \to E^{(q)}$, where $E^{(q)}$ has Weierstrass equation $y^2 = x^2 + a^q x + b^q$. When $k \subset \mathbf{F}_q$, then $a^q = a, b^q = b$, so $\mathrm{Fr}_q$ is actually a morphism $E \to E$.

We've looked informally at the reduction of $E_{/\mathbf{Q}}$ modulo $p$. This can be done directly via the Weierstrass equations. The relation between an elliptic curve and its Weierstrass equation is analogous to the relation between a vector space and its basis. Often, when proving (and computing) facts in linear algebra, we want to use bases, but basis-free proofs are often cleaner. In algebraic geometry, it is often possible to prove the same theorems about elliptic curves without using Weierstrass equations, but this requires more algebraic machinery in general.

If $\phi : E \to E$ is an isogeny, then $e_m(\phi^\vee(x), y) = e_m(x, \phi(y))$ for all $x, y \in E[m]$. So $\phi$ is "self-adjoint" as an operator on $E[m] \simeq (\mathbf{Z}/m)^2$. It would be nice to have an operator in characteristic zero. Define

$$\mathrm{T}_l E = \varprojlim E[l^n] \simeq \varprojlim (\mathbf{Z}/l^n)^2 \simeq \mathbf{Z}_l^2.$$

The ring $\mathbf{Z}_l$ is a complete discrete valuation ring of characteristic zero. It is uncountable, and contains $\mathbf{Z}$ as a dense subring. Elements can be written as $\sum_{n \geqslant 0} a_n p^n$, where $a_n \in \{0, \ldots, l-1\}$, but this isn't very helpful. Isogenies of $E$ act on $\mathrm{T}_l E$ by linear transformations. So we have a representation $\mathrm{End}(E) \to \mathrm{M}_2(\mathbf{Z}_l)$. Usually, for $k$ a number field, $\mathrm{End}(E) \simeq \mathbf{Z}$. Rarely, $\mathrm{End}(E) \otimes \mathbf{Q} \simeq \mathbf{Q}(\sqrt{-d})$ for some $d \in \mathbf{N}$. For $k$ of characteristic $p$, $\mathrm{End}(E) \otimes \mathbf{Q}$ will either be a quadratic imaginary field or a quaternion algebra.

**Theorem 2.7.6** (Faltings)**.** *Let $k$ be a number field, $E_{/k}$ an elliptic curve. Then $\mathrm{End}(E) \otimes \mathbf{Z}_l \xrightarrow{\sim} \mathrm{End}_{\mathbf{Z}_l[G_k]}(\mathrm{T}_l E)$.*

This theorem is highly non-trivial, and holds for arbitrary abelian varieties over a global field. The Tate module $\mathrm{T}_l E$ with its Galois action, "knows" $L(E, s)$, which (if we believe BSD) "knows" $\mathrm{rk}(E)$. Faltings proved that $\mathrm{T}_l E$ determines $E$ up to isogeny.

**Proposition 2.7.7.** *Let $k$ be a field, $E_1, E_2$ elliptic curves over $k$, and $n$ an integer invertible in $k$. If $\phi : E_1 \to E_2$ is an isogeny and $\ker\phi \supset E_1[n]$, then there exists $\psi : E_1 \to E_2$ such that $\phi = \psi \circ [n]$.*

*Proof.* This follows directly from [Sil09, p. III 4.11]. □

**Proposition 2.7.8.** *Let $E_{/k}$ be an elliptic curve. Then $\mathrm{End}(E)$ is a finitely generatd abelian group of rank $\leqslant 4$.*

*Proof.* Let $R = \mathrm{End}(E)$. We will first show that if $M \subset R$ is a finitely generated subgroup, then

$$M^{\mathrm{div}} = \{\phi \in R : [n]\phi \in M \text{ for some } n \geqslant 1\}$$

is also finitely generated. Indeed, we can naturally extend the degree map to $\deg : M_{\mathbf{R}} = M \otimes \mathbf{R} \to \mathbf{R}$. There is a natural embedding $M^{\mathrm{div}} \subset M_{\mathbf{R}}$, and $M^{\mathrm{div}}$ is a discrete subgroup since all $\phi \in \mathrm{End}(E)$ have degree $\geqslant 1$,which implies the open set $\{\phi \in M_{\mathbf{R}} : \deg\phi < 1\}$ is disjoint from $M^{\mathrm{div}}$. Any discrete subgroup of $M_{\mathbf{R}}$ has rank $\leqslant \dim(M_{\mathbf{R}})$, so we even know that $\mathrm{rk}(M^{\mathrm{div}}) \leqslant \mathrm{rk}(M)$.

Next, we'll prove that $R_l = R \otimes \mathbf{Z}_l \hookrightarrow \mathrm{End}(\mathrm{T}_l E)$. If $\phi \in R_l$ is the zero map on $\mathrm{T}_l E$. Then there exists a finitely generated group $M \subset R$ such that $\phi \in M_l = M \otimes \mathbf{Z}_l$. Since $M^{\mathrm{div}}$ is finitely generated, for each $n$ there exists $\phi_n \in M^{\mathrm{div}}$ such that $\phi_n \equiv \phi$

(mod $l^n$). Since $\phi[l^n] = 0$, Proposition 2.7.7 yields that $\phi_n \equiv 0 \pmod{l^n}$. Since $n$ was arbitrary, we see that $\phi = 0$.

Finally, we show that $R$ has $\mathbf{Z}$-rank $\leqslant 4$. Let $\phi_1, \dots, \phi_t$ be a $\mathbf{Z}_l$-basis for $R_l$ such that $\phi_i \in R$. (Such a basis exists because $R$ is dense in $R_l$.) Note that $t \leqslant 4$. Then for $M = \langle \phi_1, \dots, \phi_t \rangle$, we have $R = M^{\mathrm{div}}$, whence $\mathrm{rk}_{\mathbf{Z}}(R) \leqslant 4$. □

**Proposition 2.7.9.** *Let $E$ be an elliptic curve. Then* $\mathrm{End}(E) \otimes \mathbf{Q}$ *is either* $\mathbf{Q}$*, an imaginary quadratic field, or a quaternion algebra.*

*Proof.* Note that $\mathrm{End}(E)$ has no zero-divisors. Indeed, isogenies have finite kernel, so the composite of two isogenies has finite kernel. Thus the only way for the composite of two endomorphisms to be zero is for one of them to have been 0 to begin with.

Now we apply [Sil09, p. III 9.3] to show that any such ring posessing an anti-involution is either $\mathbf{Z}$, an order in an imaginary quadratic field, or an order in a quaternion algebra. The involution we use is the *Rosatti involution*, given by $\phi \mapsto \phi^\vee$. □

As an aside, note that $\mathbf{Q}(\boldsymbol{\mu}_{p^\infty})/\mathbf{Q}$ has Galois group $\mathbf{Z}_p^\times \simeq \mathbf{Z}/(p-1) \times \mathbf{Z}_p$. So there is a $\mathbf{Z}_p$-extension $L$ of $\mathbf{Q}$ (this extension is unique by class field theory). More generally, if $k$ is a number field, let $L$ be the composite of all $\mathbf{Z}_p$-extensions of $k$. Write $r = \mathrm{rk}_{\mathbf{Z}_p} \mathrm{Gal}(L/k)$. The famous *Leopoldt conjecture* is that $r = r_2 + 1$ where $r_2$ is the number of complex places of $k$. In [Bru67], Brumer proved Leopoldt's conjecture for abelian extensions of $\mathbf{Q}$. At the moment, despite several claimed proofs, the general case is wide open. It is not even clear if the conjecture holds for any specific non-solvable extensions of $\mathbf{Q}$.

This is relevant to Proposition 2.7.8 because of the following argument. Note that there is a natural map $\mathcal{O}_k^\times \to \mathcal{O}_{k,p}^\times$, where $\mathcal{O}_{k,p} = \mathcal{O}_k \otimes \mathbf{Z}_p = \prod_{\mathfrak{p}|p} \mathcal{O}_{k,\mathfrak{p}}$. Leopoldt's conjecture is equivalent to this map being an injection, i.e. $\mathbf{Z}$-linearly independent elements remaining $\mathbf{Z}_p$-independent.

**Proposition 2.7.10.** *Let $E_{/k}$ be an elliptic curve, $\psi : E \to E$ be an isogeny. Then* $\det(\psi, \mathrm{T}_l E) = \deg(\psi) \in \mathbf{Z}$ *and* $\mathrm{tr}(\psi, \mathrm{T}_l E) = 1 + \deg\psi - \deg(1-\psi)$.

*Proof.* Write $\psi_l$ for $\psi$ considered as an endomorphism of $\mathrm{tr}_l\, E$.. We can write $\psi_l = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbf{Z}_l)$ with respect to some basis. We'll use $\varprojlim e_{l^n}$ to get a pairing $e : \mathrm{T}_l E \times \mathrm{T}_l E \to \varprojlim \boldsymbol{\mu}_{l^n} = \mathrm{T}_l \mathbf{G}_{\mathrm{m}}$. We now compute

$$\begin{aligned} e(v_1, v_2)^{\deg\psi} &= e([\deg\psi] v_1, v_2) \\ &= e(\psi_l^\vee \psi_l v_1, v_2) \\ &= e(\psi_l v_1, \psi_l v_2) \\ &= e(a v_1 + c v_2, b v_1 + d v_2) \\ &= e(v_1, v_2)^{ad-bc} \\ &= e(v_1, v_2)^{\det(\psi_l)}. \end{aligned}$$

Since the Weil pairing is perfect, this forces $\deg\psi = \det(\psi_l)$.

In general, we know that for any $2 \times 2$ matrix $\theta$, we have

$$\operatorname{tr}(\theta) = 1 + \det(\theta) - \det(1-\theta);$$

so we're done. □

Let's apply this result to $\mathrm{Fr}_5$ on $E_{/\mathbf{F}_5} : y^2 = x^3 + 3x + 1$. We know $\deg(\mathrm{Fr}_5) = 5$. Consider the characteristic polynomial $\det(T - \mathrm{Fr}_5, \mathrm{T}_l E)$; it has two roots $\alpha, \beta$. We know that $\alpha\beta = \deg(\mathrm{Fr}_5) = 5$. From our identity (2.7) with $\theta = \mathrm{Fr}_{5,l}$, we get $\alpha + \beta = 1 + 5 - \det(1 - \mathrm{Fr}_{5,l}) = 6 - \#E(\mathbf{F}_5)$. Consider the following table:

| $x$ | $x^3 + 3x + 1$ | $\#\sqrt{x^3 + 3x + 1}$ |
|---|---|---|
| 0 | 1 | 2 |
| 1 | 0 | 1 |
| 2 | 0 | 1 |
| 3 | 2 | 0 |
| 4 | 2 | 0 |

We conclude that $\#E(\mathbf{F}_5) = 5$, so $\alpha + \beta = 1$. In general, $\#E(\mathbf{F}_{5^f}) = (1-\alpha^f)(1-\beta^f)$, so for example

$$\begin{aligned}
\#E(\mathbf{F}_{5^3}) &= (1-\alpha^3)(1-\beta^3) \\
&= 1 - (\alpha^3 + \beta^3) + (\alpha\beta)^2 \\
&= 1 - (\alpha+\beta)^3 + 3\alpha\beta(\alpha+\beta) + (2\beta)^3 \\
&= 1 - 1^3 + 3 \cdot 5 \cdot 1 + 5^3 \\
&= 140.
\end{aligned}$$

So we see that computing something like $\#E(\mathbf{F}_q)$ is easy. More importantly, $\#E(\mathbf{F}_q), \#E(\mathbf{F}_{q^2}), \ldots$ depnds only on two pieces of data. This brings us to the Weil Conjectures.

## 2.8 Weil conjectures

Let $V_{/\mathbf{F}_q}$ be a smooth proper $d$-dimensional variety. Set

$$Z(V,T) = \exp\left(\sum_{n \geqslant 1} \#V(\mathbf{F}_{q^n}) \frac{T^n}{n}\right).$$

This is just a fancy generating series encoding the numbers $\#V(\mathbf{F}_{q^n})$.

**Conjecture 2.8.1** (Weil)**.**

*1.* $Z(V,T) \in \mathbf{Q}(T)$.

*2.* $Z\left(V, \dfrac{1}{q^d T}\right) = \pm q^{d\chi/2} T^{\chi} Z(V,T)$

*3.* $Z(V,T)=\prod_{i=0}^{2d}P_i(T)^{(-1)^{i+1}}$, *where* $P_i\in\mathbf{Z}[T]$ *and the roots of* $P_i$ *are pure of size* $q^{i/2}$*.*

Part 1 of the Weil Conjectures tells us that $Z(V,T)$ actually contains only a finite amount of information. This was proved by Dwork in [find source]. In part 2, $\chi$ is the Euler characteristic of $V$; this was proved by Grothendieckin SGA 5. Part 3 was proved by Deligne in [source].

The roots of $P_i$ are algebraic numbers. An algebraic number $\omega\in\overline{\mathbf{Q}}$ is *pure* if the absolute value $|\iota(\omega)|$ is the same for all embeddings $\iota:\overline{\mathbf{Q}}\hookrightarrow\mathbf{C}$. Grothendieck proved more than 2; we have

$$Z(V,T)=\prod_{i=0}^{2d}\det\left(T-\mathrm{Fr}_q,\mathrm{H}^i_{\text{ét}}(V_{\overline{\mathbf{F}_q}},\mathbf{Q}_l)\right)^{(-1)^{i+1}}.$$

You should think about $\mathrm{Fr}_q$ acting on $\mathrm{T}_lE=\mathrm{H}^1_{\text{ét}}(E_{\overline{\mathbf{F}_q}},\mathbf{Z}_l)$. This is basically a rephrasing of the Lefschetz trace formula from algebraic topology. However, the algebraic Lefschetz trace formula is enormously difficult.

Deligne's result settles the Ramanujan conjecture for modular forms. For example, define $\tau$ by

$$\Delta=q\prod_{n\geqslant 1}(1-q^n)^{24}=\sum_{n\geqslant 0}\tau(n)q^n.$$

The Ramanujan conjecture is: $|\tau(p)|\leqslant p^{11/2}$. Even here, algebraic geometry is lurking under the surface.

## 2.9 $p$-adic numbers

Recall the $p$-adic norm $|\cdot|_p:\mathbf{Q}\to\mathbf{R}_{\geqslant 0}$, defined by $|p^r\frac{m}{n}|_p=p^{-r}$, if $p\nmid m,n$. It is an easy exercise to check that this actually is a norm, i.e. it is multiplicative and satisfies $|x+y|\leqslant\max\{|x|,|y|\}$. The completion of $\mathbf{Q}$ with respect to this norm is denoted $\mathbf{Q}_p$. There is an obvious embedding $\mathbf{Q}\hookrightarrow\mathbf{Q}_p$ with dense image. Let

$$\mathbf{Z}_p=\{x\in\mathbf{Q}_p:|x|_p\leqslant 1\}.$$

It turns out that $\mathbf{Z}_p$ is a complete discrete valuation ring which is compact. Thus $\mathbf{Q}_p$ is locally compact as a topological field.

**Lemma 2.9.1** (Hensel)**.** *Let* $f\in\mathbf{Z}_p[x]$*. Suppose* $f(x_0)\equiv 0\pmod p$ *for some* $x_0\in\mathbf{F}_p$ *for which* $f'(x_0)\not\equiv 0\pmod p$*. Then there exists* $\widetilde{x_0}\in\mathbf{Z}_p$ *such that* $\widetilde{x_0}\equiv x_0\pmod p$ *and* $f(\widetilde{x_0})=0$*.*

*Proof.* Let $X=\mathrm{Spec}(\mathbf{Z}_p[x]/f)$. This is a scheme over $S=\mathrm{Spec}(\mathbf{Z}_p)$. The condition on $f'(x_0)$ is exactly that the fiber $X_{x_0}$ is smooth over $S$. It is known that smooth morphisms are formally smooth, so $X_{x_0}(\mathbf{Z}/p^{n+1})\twoheadrightarrow X_{x_0}(\mathbf{Z}/p^n)$ for all $n$, whence the result. □

**Example 2.9.2** (Selmer)**.** The curve $C_{/\mathbf{Q}}$ given by $3x^3+4y^3+5z^3=0$ satisfies $C(\mathbf{A_Q})\neq\varnothing$, but $C(\mathbf{Q})=\varnothing$. That $C(\mathbf{R})\neq\varnothing$ is an elementary exercise. We'll show that $C(\mathbf{Q}_p)\neq\varnothing$ or $p\equiv 2 \pmod 3$. Let $x=y=1$. Then $7+5z^3=0$ is equivalent to $z^3=-7/5$. Let's solve this modulo $p$ for $p\neq 5$. Note that $\mathbf{F}_p^\times\simeq\mathbf{Z}/(p-1)$, and $3\nmid(p-1)$, which means that raising to the third power is surjective as a map $\mathbf{F}_p^\times\to\mathbf{F}_p^\times$. The derivative condition in Lemma 2.9.1 applies, so there is a solution in $\mathbf{Q}_p$. For $p=5$, let $x=1,z=0$ and we get $y^3=-3/4$. Repeat the process in $\mathbf{F}_5^\times$. ▷

As a homework problem, show that if $p\equiv 1 \pmod 3$, then $C(\mathbf{Q}_p)\neq\varnothing$.

Let $\overline{\mathbf{Q}_p}$ be an algebraic closure of $\mathbf{Q}_p$. Then by [Neu99, II 6.6], the absolute value on $\mathbf{Q}_p$ has a unique extension to one on $\overline{\mathbf{Q}_p}$. We will write $|\cdot|=|\cdot|_p$ for both. We can define

$$\mathcal{O}_{\overline{\mathbf{Q}_p}}=\{x\in\overline{\mathbf{Q}_p}:|x|\leqslant 1\}$$
$$\mathfrak{m}_{\overline{\mathbf{Q}_p}}=\{x\in\overline{\mathbf{Q}_p}:|x|<1\}.$$

Then $\mathcal{O}_{\overline{\mathbf{Q}_p}}$ is a (non-noetherian) local ring with maximal ideal $\mathfrak{m}_{\overline{\mathbf{Q}_p}}$ and residue field $\overline{\mathbf{F}_p}$. By the uniqueness of the extension of $|\cdot|$ to $\overline{\mathbf{Q}_p}$, we see that $|\sigma(x)|=|x|$ for all $x\in\overline{\mathbf{Q}_p}$. This allows us to define a short exact sequence of Galois groups:

$$\begin{tikzcd}1 \arrow[r] & I_p \arrow[r] & G_{\mathbf{Q}_p} \arrow[r] & G_{\mathbf{F}_p} \arrow[r] & 1.\end{tikzcd}$$

The map $G_{\mathbf{Q}_p}\to G_{\mathbf{F}_p}$ is $\sigma(\bar{x})=\overline{\sigma(x)}$ for $\bar{x}\in\mathcal{O}_{\overline{\mathbf{Q}_p}}/\mathfrak{m}_{\overline{\mathbf{Q}_p}}$. The group $I_p$, called the *inertia group*, can be defined directly by

$$I_p=\{\sigma\in G_{\mathbf{Q}_p}:\sigma(x)\equiv x \mod \mathfrak{m}_{\overline{\mathbf{Q}_p}} \text{ for all } x\in\mathcal{O}_{\overline{\mathbf{Q}_p}}\}.$$

Write $\mathbf{Q}_p^{\mathrm{ur}}$ for the field $(\overline{\mathbf{Q}_p})^{I_p}$; it turns out that $p$ is prime in $\mathbf{Z}_p^{\mathrm{ur}}=\mathcal{O}_{\mathbf{Q}_p^{\mathrm{ur}}}$. For each $l\neq p$, define $t_l:I_p\to\mathbf{Z}_l$ by

$$\sigma(p^{1/l^n})=\zeta_{l^n}^{t_l(\sigma)\pmod{l^n}}p^{1/l^n}.$$

Then $t=\prod_l t_l$ induces another canonical short exact sequence (this can be derived from [Neu99, II 7.7]):

$$\begin{tikzcd}1 \arrow[r] & P \arrow[r] & I_p \arrow[r, "t"] & \widehat{\mathbf{Z}}/\mathbf{Z}_p \arrow[r] & 1.\end{tikzcd}$$

The group $P$ is pro-$p$; in fact it is the Sylow $p$-subgroup of $I_p$. We don't "understand" representations $G_{\mathbf{Q}}\to\mathrm{GL}_n(\mathbf{Z}_p)$ largely because $G_{\mathbf{Q}}\supset G_{\mathbf{Q}_p}\supset P$, and we don't understand the image of $P$ in $\mathrm{GL}_n(\mathbf{Z}_p)$. The field of *p-adic Hodge theory* seeks to understand this image, among other things.

**Definition 2.9.3.** *Let $E_{/\mathbf{Q}}$ be an elliptic curve, $p$ a prime. We say that $E$ has* good reduction *at $p$ if there exists an abelian scheme $\mathcal{E}$ over $\mathbf{Z}_{(p)}$ such that $\mathcal{E}_{\mathbf{Q}}\simeq E$.*

From the theory of Néron models (see [BLR90]), such an $\mathcal{E}$ is unique up to isomorphism. Moreover, if $p \geqslant 5$, it is equivalent to require that there exist a model $y^2 = x^3 + Ax + B$ for $E$ with $A, B \in \mathbf{Z}_{(p)}$ and $p \nmid (4A^3 + 26B^2)$. For a general elliptic curve $E_{/\mathbf{Q}}$, write $\rho_{E,l}$ for the Galois representation $G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_l)$ coming from the $l$-adic Tate module $\mathrm{T}_l E$.

**Theorem 2.9.4** (Néron-Ogg-Shafarevich)**.** *An elliptic curve $E_{/\mathbf{Q}}$ has good reduction at $p \neq l$ if and only if $\rho_{E,l}(I_p) = 1$.*

*Proof.* See [ST68] for a beautiful proof using the theory of Néron models. □

Suppose $E$ has good reduction at some $p \neq l$. Since $\rho_{E,l}(I_p) = 1$, the representation $\rho_{E,l}|_{G_{\mathbf{Q}_p}}$ factors through $G_{\mathbf{F}_p} = \widehat{\mathbf{Z}}$, which is (canonically) generated by Frobenius $\mathrm{fr}_p : x \mapsto x^p$. The matrix $\rho_{E,l}(\mathrm{fr}_p)$ is semisimple, hence conjugate to $\begin{pmatrix}\alpha_p & \\ & \beta_p\end{pmatrix}$, where $\# E(\mathbf{F}_f) = p^f + 1 - (\alpha_p^f + \beta_p^f)$ for all $f$.

If $E$ has bad reduction at $p$, the inertia at $p$ will act nontrivially on $\mathrm{T}_l E$, so $\rho_{E,l}(\mathrm{fr}_p)$ is not meaningful here. But we still have an action of $\mathrm{fr}_p$ on $(\mathrm{T}_l E)^{I_p} = \mathrm{H}^0(I_p, \mathrm{T}_l E)$. This lets us define the $L$-factors of $L(E,s)$ at primes of bad reduction. Namely,

$$\begin{aligned} L_p(E,t) &\det\left(1 - \mathrm{fr}_p \cdot t, (\mathrm{T}_l E)^{I_p}\right)^{-1} && \text{(any } l \neq p\text{)} \\ L(E,s) &= \prod_p L_p(E, p^{-s}). \end{aligned}$$

If $(\mathrm{T}_l E)^{I_p} = \mathrm{T}_l E$, we get

$$\det\left(1 - \begin{pmatrix}\alpha_p p^{-s} & \\ & \beta_p p^{-s}\end{pmatrix}\right) = \left(1 - \frac{\alpha_p}{p^s}\right)\left(1 - \frac{\beta_p}{p^s}\right) = 1 + a_p p^{-s} + p^{1-2s},$$

so this definition of $L(E,s)$ agrees with our earlier definition at the places of good reduction. One thing that is not *a priori* clear is whether $L_p(E,s)$ depends on the choice of the prime $l$. If $E$ has good reduction at $p$, then we can see that $L_p(E,s)$ doesn't depend on $l$, but in general it is not obvious. Fortunately, by [Del80, 3.3.9], this is the case. At primes of bad reduction, this is even harder. For elliptic curves (and more generally, abelian varieties), this can be done directly using Néron models.

**Conjecture 2.9.5** (Birch, Swinnerton-Dyer)**.** *Let $E_{/\mathbf{Q}}$ be an elliptic curve. Then $L(E,s)$ admits a meromorphic continuation to a neighborhood of $s = 1$, and $\mathrm{ord}_{s=1} L(E,s) = \mathrm{rk}(E)$.*

We have essentially proved that the product formula for $L(E,s)$ is analytic for $\Re s > 3/2$. This is easy when we know there are only finitely many primes of bad reduction, and

$$\begin{gathered} |\alpha_p + \beta_p = a_p| \leqslant 2\sqrt{p} \\ \alpha_p \beta_p = p. \end{gathered}$$

In our definition of $L_p(E,t)$, we looked at $\rho_{E,l}|_{G_{\mathbf{Q}_p}} : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(\mathbf{Z}_l)$ for some prime $l$ that is *not* equal to $p$. Also, in the Néron-Ogg-Shafarevich criterion (2.9.4), we needed $l = p$. What can be said about $\rho_p = \rho_{E,p}|_{G_{\mathbf{Q}_p}} : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(\mathbf{Z}_p)$? Even if $E$ has good reduction at $p$, this representation can be ramified. There are two cases. If $E$ has *ordinary reduction*, then we have

$$\rho_p \sim \begin{pmatrix} \varepsilon\chi & * \\ & \psi^{-1} \end{pmatrix},$$

where $\psi : G_{\mathbf{Q}_p} \to \mathbf{Z}_p^\times$ is unramified and $\varepsilon$ is the $p$-adic cyclotomic character. If $E$ has good supersingular reduction at $p$, then $\rho_p$ is irreducible.

Although it is ramified, the representation $\rho_p$ knows quite a lot about $E$. For example, the $L$-factor at $p$ can be recovered from $\rho_p$, though this is quite tricky and involves Fontaine's semistable period ring $\mathbf{B}_{\mathrm{st}}$ [Och99].

## 2.10 Selmer groups

Let $E_{/\mathbf{Q}}$ be an elliptic curve. Recall we have a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & E[p](\overline{\mathbf{Q}}) \arrow[r] & E(\overline{\mathbf{Q}}) \arrow[r] & E(\overline{\mathbf{Q}}) \arrow[r] & 0. \end{tikzcd}$$

Take $G_{\mathbf{Q}}$ (resp. $G_{\mathbf{Q}_l}$)-invariants. We get a commutative diagram:

$$\begin{tikzcd} 0 \arrow[r] & E(\mathbf{Q})/p \arrow[r] \arrow[d] & \mathrm{H}^1(G_{\mathbf{Q}}, E[p]) \arrow[r] \arrow[d] & \mathrm{H}^1(G_{\mathbf{Q}}, E)[p] \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & \prod_l E(\mathbf{Q}_l)/p \arrow[r] & \prod_l \mathrm{H}^1(G_{\mathbf{Q}_l}, E[p]) \arrow[r] & \prod_l \mathrm{H}^1(G_{\mathbf{Q}_l}, E)[p] \arrow[r] & 0. \end{tikzcd}$$

The *Selmer group* of $E$ is

$$\mathrm{Sel}_p(E) = \ker\left(\mathrm{H}^1(G_{\mathbf{Q}_p}, E[p]) \to \prod_l \mathrm{H}^1(G_{\mathbf{Q}_l}, E)[p]\right).$$

It is easy to check that $\mathrm{Sel}_p(E) \supset E(\mathbf{Q})/p$. Moreover, $\dim_{\mathbf{F}_p}(E(\mathbf{Q})/p) \geqslant \mathrm{rk}(E(\mathbf{Q}))$ (once we know finite generation of $E(\mathbf{Q})$).

**Theorem 2.10.1.** *Let $E_{/\mathbf{Q}}$ be an elliptic curve. Assume the Mordell-Weil theorem holds for $E$. For $p \geqslant 3$, we have $\dim(E(\mathbf{Q}) \otimes \mathbf{F}_p) = \mathrm{rk}(E) + \delta$, where*

$$\delta = \begin{cases} 0 & E[p](\mathbf{Q}) = 0 \\ 1 & \textit{else}. \end{cases}$$

*Proof.* We can ignore prime-to-$p$ torsion. We know that $E[p](\mathbf{Q}) \simeq (\mathbf{Z}/p)^\delta$, where $\delta \leqslant 2$. We need to exclude $\delta = 2$. If this happened, then $G_{\mathbf{Q}}$ acts trivially on $E[p]$. But $\det(\rho_{E,p}) = \varepsilon_p$, and $\varepsilon_p \not\equiv 1 \pmod p$ for $p \geqslant 3$. Alternatively, $\boldsymbol{\mu}_p \not\subset \mathbf{Q}$ for $p \geqslant 3$. □

What about $p = 2$? Is it possible for $E[2](\mathbf{Q}) = (\mathbf{Z}/2)^2$? Let $E_{/\mathbf{Q}}$ be the curve $y^2 = (x-17)(x-19)(x-21)$. Then $E(\mathbf{Q}) \supset \{(17,0),(19,0),(21,0)\}$, and points on $E(\mathbf{Q})$ of the form $(x,0)$ are 2-torsion. More generally, if $E_{/\mathbf{Q}}$ is of the form $y^2 = f(x)$ and $f$ has three distinct rational roots, then $E[2](\mathbf{Q}) \simeq (\mathbf{Z}/2)^2$.

For $p = 2,3,5$, with $E_{/\mathbf{Q}}$ ordered by height, Bhargava-Shankar proved that $\operatorname{avg}(\#\operatorname{Sel}_p) = p+1$. If $\dim(\operatorname{Sel}_p E) = t$, then $\#\operatorname{Sel}_p(E) = p^t$. For integral $t$, we have $p^t \geqslant (p^2-p)(t-1)+p$. Some basic arithmetic gives $1 + \frac{1}{p(p-1)} \geqslant \operatorname{rk}(E)$.

Proceeding naïvely won't get an average $\leqslant 1$. We expect $\operatorname{avg}(\operatorname{rk}) = 1/2$.

## 2.11 State-of-the-art

Our definition of $L(E,s)$ actually works for any sufficiently nice Galois representation. The correct definition of "sufficiently nice" is a bit tricky. For us, it will mean "coming from a pure motive." The upshot of this is that we will have a family $\rho = \{\rho_l : G_{\mathbf{Q}} \to \operatorname{GL}_n(\mathbf{Q}_l)\}$ of Galois representations, one for each prime $l$, such that for each $l$, the representation $\rho_l$ is unramified at all but finitely many primes, and whenever $\rho_l$ and $\rho_{l'}$ are both unramified at $p$, we have

$$\det(1 - t\cdot\rho_l(\mathrm{fr}_p)) = \det(1 - t\cdot\rho_{l'}(\mathrm{fr}_p) \in \mathbf{Q}[t].$$

We write $\det(1 - t\cdot\rho(\mathrm{fr}_p))$ for the common value. One puts

$$\begin{aligned} L_p(\rho,t) &= \det\left(1 - \rho(\mathrm{fr}_p)\cdot t, \rho^{I_p}\right) \\ L(\rho,s) &= \prod_p L_p(\rho, s^{-p}). \end{aligned}$$

We could make the same definition if $\chi : G_{\mathbf{Q}} \to \operatorname{GL}_n(\mathbf{C})$ is a continuous character. This recovers the classical *Artin L-functions*. If $n = 1$, these are *Dirichlet L-functions*, and it is known that if $\chi : G_{\mathbf{Q}} \to \mathbf{C}^\times$ is a nontrivial character, then $L(\chi,s)$ has analytic continuation to $\mathbf{C}$ and satisfies $L(\chi,1) \neq 0$. This has as a corollary Dirichlet's theorem that for $(a,n) = 1$, there are infinitely many primes in the sequence $\{a + nk : k \geqslant 1\}$. For general $\rho$, very little is known about analytic continuation of $L(\rho,s)$.

For example, if $\rho = \rho_E$ for $E_{/\mathbf{Q}}$ an elliptic curve, one proves that $L(E,s) = L(\rho_E,s)$ has meromorphic continuation by proving that $E$ is modular! That is, set $\xi(s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$, where $N$ is the conductor of $E$. One proves that $\xi(s) = \pm\xi(2-s)$. But this is done by proving that $L(E,s)$ is actually $L(f,s)$ for a cuspidal eigenform $f$.

**Theorem 2.11.1** (Wiles, Taylor-Wiles, …). *Let $E_{/\mathbf{Q}}$ be an elliptic curve. Then for $N$ the conductor of $E$, there exists a regular surjection $X_0(N) \twoheadrightarrow E$.*

*Strategy of proof.* One considers the associated Galois representation $\rho_{E,l} : G_{\mathbf{Q}} \to \operatorname{GL}_2(\mathbf{Z}_l)$ coming from $\mathrm{T}_l E$. This gives an action of $G_{\mathbf{Q}}$ on $\operatorname{Ad}^\circ(\mathrm{T}_l E) \otimes (\mathbf{Q}_l/\mathbf{Z}_l)$. Here $M = \operatorname{Ad}^\circ \subset \mathfrak{gl}_2$ is the subalgebra of trace-zero matrices, with action of $\operatorname{GL}(2)$ by conjugation. Consider the kernel of

$$\mathrm{H}^1(G_{\mathbf{Q}}, M) \to \bigoplus_p \mathrm{H}^1(G_{\mathbf{Q}_p}, M)/(\text{some subgroup}).$$

Wiles reduced proving the modularity of $E$ to a precise computation of the kernel (called a generalized Selmer group). $\square$

The curve $X_0(N)$ is a smooth curve over $\mathbf{Q}$. A complex-analytic model for $X_0(N)$ (minus the cusps) is $\Gamma_0(N)\backslash\mathfrak{H}$, where $\mathfrak{H}$ is the upper half plane and

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) : c \equiv 0 \pmod{N} \right\}.$$

Given such a surjection $\pi : X_0(N) \twoheadrightarrow E$, we can pullback the unique holomorphic differential $\omega$ on $E$ to get a holomorphic differential $\pi^*\omega$ on $X_0(N)$. The differential $\pi^*\omega$ will be $f(z)\mathrm{d}z$ for a modular form $f$. It is this $f$ which satisfies $L(f,s) = L(E,s)$.

As an aside, let $k \supset \mathbf{Q}$ be a number field. Then we can define the *zeta-function* of $k$ by

$$\zeta_k(s) = \sum_{\mathfrak{a} \subset \mathcal{O}_k} \frac{1}{\mathrm{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_k)} \left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s}\right)^{-1}.$$

**Theorem 2.11.2.** *The function $\zeta_k$ has a simple pole at $s = 1$ with residue $2^{r_1}(2\pi)^{r_2}\frac{hR}{w\sqrt{D_k}}$, where*

- *$r_1$ is the number of real places of $k$,*
- *$r_2$ is the number of complex places of $k$,*
- *$h = \#\,\mathrm{Pic}(\mathcal{O}_k)$ is the class number of $k$,*
- *$w = \#\boldsymbol{\mu}(k)$ is the number of roots of unity in $k$,*
- *$D_k$ is the discriminant of $k$, and*
- *$R$ is the regulator of $k$.*

Given $k$, it's not hard to compute the residue of $\zeta_k$ at $s = 1$ with reasonable accuracy. It's easy to compute $r_1, r_2, w$, and $D_k$. So we can compute $hR$ pretty easily. But computing $h$ and $R$ individually is quite difficult. Quadratic imaginary fields are "easy," because for these fields we have $R = 1$.

We are not able to state the (correct) version of the Birch and Swinnerton-Dyer conjecture.

**Conjecture 2.11.3.** *Let $E_{/\mathbf{Q}}$ be an elliptic curve. Set $r = \mathrm{rk}(E)$. Then $\mathrm{ord}_{s=1} L(E,s) = r$, with residue $\frac{\Omega \prod_v c_v R Ш}{\#E(\mathbf{Q})^2_{\mathrm{tors}}}$, where*

- *$\Omega$ is the period of $E$ (a complex integral),*
- *$R$ is the regulator of $E$,*
- *$Ш = \#\ker\left(\mathrm{H}^1(\mathbf{Q}, E) \to \prod_l \mathrm{H}^1(\mathbf{Q}_l, E)\right)$, and*

- *the $c_v$ are Tamagawa numbers, namely $\#\pi_0(\mathcal{E}_{\mathbf{F}_v})$, where $\mathcal{E}$ is the Néron model of $E$ at $v$.*

We know the following easy fact: let $\phi : E_1 \to E_2$ be an isogeny of elliptic curves over $\mathbf{Q}$. Then $L(E_1, s) = L(E_2, s)$. But all other of the numbers appearing in BSD except $\#E(\mathbf{Q})_{\text{tors}}$ can be different for $E_1$ and $E_2$. The paper [Tate: arithmetic of elliptic curves] is a great overview of the arithmetic of elliptic curves. In this paper, Tate asked whether $\#Ш < \infty$ and whether $L(E, s)$ is defined at $s = 1$? The first question is wide open. The second is known, via the modularity theorem.

**Theorem 2.11.4** (Gross-Zagier, Kolyvagin, Kato)**.** *Let $E_{/\mathbf{Q}}$ be an elliptic curve. If* $\operatorname{ord}_{s=1} L(E, s) \leqslant 1$*, then the Birch and Swinnerton-Dyer conjecture holds for $E$.*

The original proof of this theorem assumed the curve $E$ was modular. Thanks to Wiles et. al., we know this is the case.

**Theorem 2.11.5** (Skinner-Urban)**.** *If* $\operatorname{rk}(E) = 0$ *and* $Ш < \infty$ *[and some technical hypotheses hold], then BSD holds for $E$.*

**Theorem 2.11.6** (Skinner)**.** *If* $\operatorname{rk}(E) = 1$ *and* $Ш < \infty$*, then* $\operatorname{ord}_{s=1} L(E, s) = 1$.

**Theorem 2.11.7** (Dokchitser-Dokchitser)**.** *If* $Ш < \infty$*, then* $r_{\text{an}} \equiv r_{\text{alg}} \pmod 2$.

We expect this congruence. Indeed, we know that

$$L(E, s) = \pm(\text{stuff} > 0)L(E, 2 - s).$$

From this, assuming BSD, we get the parity conjecture proved by Skinner under the assumption that $Ш < \infty$.

**Theorem 2.11.8** (Bhargava-Shankar)**.** $\operatorname{avg}(\text{rk}) \leqslant \operatorname{avg}(\dim \operatorname{Sel}_p) \leqslant 1 + \frac{1}{p(p-1)}$ *for* $p \in \{2, 3, 5\}$.

Even if this could be proved for all $p$, we would only know that $\operatorname{avg}(\text{rk}) \leqslant 1$, but we expect the average to be $1/2$. If we could get $\operatorname{avg}(\text{rk}) < 1$, this would imply that a positive proportion of elliptic curves have rank 0.

Bhargava et. al. construct a family $\mathfrak{F}$ of elliptic curves over $\mathbf{Q}$, that is a positive fraction of the set of all elliptic curves over $\mathbf{Q}$. All the technical hypotheses of Skinner, Skinner-Urban are satisfied on $\mathfrak{F}$. They use Dokchitser-Dokchitser as well. Let $p_i$ be the proportion of $E$ in $\mathfrak{F}$ with $\dim(\operatorname{Sel}_3) = i$. They prove that $\operatorname{avg}(\# \operatorname{Sel}_3) = 4$ in $\mathfrak{F}$. They also prove that half of the curves in $\mathfrak{F}$ have sign 1 (resp. $-1$) in their functionnal equations. Consider the sum

$$p_0 \cdot 1 + p_1 \cdot 3 + \left(\frac{1}{2} - p_0\right) \cdot 3^2 + \left(\frac{1}{2} - p_0\right) \cdot 3^3 \leqslant 4.$$

Note that $p_0 \leqslant p_n$ for $n \geqslant 2$. Now the sign $w = 1$ if and only if $\dim \operatorname{Sel}_p$ is even. We also know that $p_0, p_1 \leqslant 1/2$. Playing around with the inequality, we get

$$\begin{aligned} p_1 &\geqslant 5/12 \\ p_0 &\geqslant 1/4. \end{aligned}$$

This implies that a positive fraction of all $E$ (not just those in $\mathfrak{F}$) have ranks 0 or 1.

## 2.12 Mordell-Weil

Let $k$ be a field of characteristic not equal to 2. Then we understand quadratic extensions of $k$ via Kummer theory. Namely, $\mathrm{H}^1(k, \mathbf{Z}/2) = \mathrm{H}^1(k, \boldsymbol{\mu}_2) = k^\times/2$. So quadratic extensions of $k$ are in bijection with $k^\times/k$.

Consider an extension $\mathbf{Q}(\sqrt{\alpha})$ with $\alpha \in \mathbf{Z}$ square-free. The "bad primes" (primes at which $\mathbf{Q}(\sqrt{\alpha})/\mathbf{Q}$ ramifies) are contained in the set of primes dividing the discriminant $4|\alpha|$. We have a (not short exact) sequence

$$\begin{tikzcd} I_p \arrow[r, hook] & G_{\mathbf{Q}_p} \arrow[r, hook] & G_{\mathbf{Q}} \arrow[r, two heads] & \mathrm{Gal}(\mathbf{Q}(\sqrt{\alpha})/\mathbf{Q}). \end{tikzcd}$$

The extension is *ramified* at $p$ if $I_p \twoheadrightarrow \mathrm{Gal}(\mathbf{Q}(\sqrt{\alpha})/\mathbf{Q})$. It is natural to ask whether there are any $k/\mathbf{Q}$ unramified everwhere? For quadratic extensions, the answer is easily no: the only possible unramified extension is $\mathbf{Q}(\sqrt{-1})/\mathbf{Q}$, and this ramifies at 1. In fact, the Hermite-Minkowski theorem is that there exists no extension $k/\mathbf{Q}$ unramified everywhere.

The composite of all quadratic extensions of $\mathbf{Q}$ with $\{2, 3, 5, 7\}$ the only bad primes is finite. Indeed, it is $\mathbf{Q}(\sqrt{\pm 2}, \sqrt{\pm 3}, \sqrt{\pm 5}, \sqrt{\pm 7})$.

**Theorem 2.12.1.** *Let $k$ be a number field containing $\boldsymbol{\mu}_m$. Let $S$ be a finite set of places of $k$ including all those dividing $m$. Then the maximal abelian extension $L/k$ such that*

1. *all bad primes of $L/k$ are in $S$,*
2. $\mathrm{Gal}(L/k)$ *is killed by $m$,*

*is finite over $k$.*

*Proof.* This needs finiteness of class group and finite generation of the $S$-unit group. □

We're moving towards a proof of the Mordell-Weil theorem for elliptic curves $E_{/\mathbf{Q}}$. We have two steps:

1. Prove that $E(\mathbf{Q})/m$ is finitely generated for some $m \geqslant 2$.
2. Prove Proposition 2.12.2.
3. Define a height function $h : E(\mathbf{Q}) \to \mathbf{R}$ satisfying the hypotheses of Proposition 2.12.2.

**Proposition 2.12.2.** *Let $A$ be an abelian group with a function $h : A \to \mathbf{R}$ such that*

- *For $x \in A$, there exists a constant $c_x$ such that $h(x+y) \leqslant 2h(y) + c_x$ for all $y \in A$.*
- *There exists $m \geqslant 2, c_A$ such that for all $x \in A$, $h(m \cdot x) \geqslant m^2(h(x) - c_A$.*

- *For all $c$, the cardinality $\#\{h < c\} = \#\{x \in A : h(x) < c\} < \infty$.*

*Then $A$ is finitely generated.*

Let $E_{/\mathbf{Q}}$ be an elliptic curve. We'll start by defining $h : E(\mathbf{Q}) \to \mathbf{R}$. Let $P = (x(P), y(P)) \in E(\mathbf{Q})$. Then $h_x(P)$ is the logarithm of the maximum of the absolute values of the numerator and denominator of $x(P)$.

We'll start with the weak Mordell-Weil theorem, namely that $E(\mathbf{Q})/m$ is finitely generated.

**Lemma 2.12.3.** *Let $L/k$ be a Galois extension of number fields, $E_{/k}$ be an elliptic curve. If $E(L)/m$ is finitely generated, then so is $E(k)/m$.*

*Proof.* We plan to prove that $(E(k) \cap mE(L))/mE(k)$ is finite. Since it is the kernel of $E(k)/m \to E(L)/m$ and $E(L)/m$ is finite, we will conclude that $E(k)/m$ is finite. Let $x \in (E(k) \cap mE(L))/mE(k)$. Then there exists $y_x \in E(L)$ such that $m \cdot y_x = x$. Define $\lambda_x : \mathrm{Gal}(L/k) \to E[m]$ by $\lambda_x(\sigma) = \sigma(y_x) - y_x$. Let $x, x'$ be two points and assume $\lambda_x = \lambda_{x'}$. Then $\sigma(y_x) - x_y = \sigma(y_{x'}) - y_{x'}$ for all $\sigma \in \mathrm{Gal}(L/k)$, which implies $\sigma(y_x) - \sigma(y_{x'}) = y_x - y_{x'}$ for all $\sigma$. This in turn implies that $y_x - y_{x'} \in E(k)$. So $m \cdot (y_x - y_{x'}) = x - x' \in mE(k)$. So the map $x \mapsto \lambda_x$ is an injection from $(E(k) \cap mE(L))/mE(k)$ into the finite set of functions $\mathrm{Gal}(L/k) \to E[m]$. (This map isn't a homomorphism because it depends on the choice of $y_x$. That's okay – it's still an injection, and this gives the finiteness of $(E(k) \cap mE(L))/mE(k)$.) □

Thus, to prove that $E(\mathbf{Q})/m$ is finite, we can switch to the number field $k = \mathbf{Q}(E[m])$ generated by $E[m]$ over $\mathbf{Q}$. Formally, let $\rho_{E,m} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}/m)$ be the Galois representation associated to $E$; one puts $\mathbf{Q}(E[m]) = (\overline{\mathbf{Q}})^{\ker(\rho_{E,m})}$. We will prove that $E(k)/m$ is finite. So far we've had the Weil pairing $E[m] \times E[m] \to \boldsymbol{\mu}_m$ and the Kummer pairing. $k^\times/p \times G_k^{(p)} \to \boldsymbol{\mu}_p$. This should be thought of as a pairing $\mathbf{G}_{\mathrm{m}}(k) \times G_k \to \boldsymbol{\mu}_m(k)$. Mimic this with $E$ and $E[m]$. We get a pairing $E(k) \times G_k \to E[m](k)$. A similar pairing works for any commutative algebraic group.

[what group scheme generates all abelian extensions of a number field? General Kummer exact sequence]

Under the assumption $E[m] \subset k$, we define $E(k)/m \times G_k \to E[m]$ by $(x, \sigma) \mapsto \sigma(y) - y$ for any $y$ such that $m \cdot y = x$. This is well-defined. Indeed, $y$ is well-defined only up to some $z \in E[m]$. Note that

$$\begin{aligned}\sigma(y + z) - (y + z) &= \sigma(y) + z - y - z \\ &= \sigma(y) - z.\end{aligned}$$

It is trivial to check that this is bilinear. Let $L = k(\frac{1}{m}E(k))$. Then we have a perfect pairing $E(k)/m \times \mathrm{Gal}(L/k) \to E[m]$. So to prove $E(k)/m$ is finite, it suffices to prove that $\mathrm{Gal}(L/k)$ is finite. The extension $L/k$ is abelian, Galois, and killed by $m$. In fact, it has only finitely many ramified primes. By Theorem 2.12.1, the extension $L/k$ is finite, so we're done. To prove that $L/k$ is ramified at only finitely many primes, we need the fact that elliptic curves have bad reduction at only finitely many primes.

We won't prove Proposition 2.12.2. Instead, we will show that the height function we constructed on $E(\mathbf{Q})$ satifies the hypothese of this result.

If $k$ is a general number field and $A_{/k}$ is an abelian variety, the Mordell-Weil theorem tells us that $A(k)$ is a finitely generated abelian group. But given $E_{/\mathbf{Q}}$, there exists $k/\mathbf{Q}$ with $E(k)$ having rank $\geqslant 100$, or $N$ for any fixed integer $N$. If we fix $k$, is there $E_{/k}$ with arbitrarily large rank? Even if $k = \mathbf{Q}$, this is wide open. Heuristics suggest that $\sup\{\operatorname{rk} E(k) : E_{/k} \text{ an elliptic curve}\}$ is finite.

The height function $h_x : E(\mathbf{Q}) \to \mathbf{R}$ we have defined is "almost" a quadratic form. Tate observed that if $f : E \to \mathbf{P}^1$ is a morphism over $\mathbf{Q}$, set $h_f(P) = \log H(f(P))$, where $H : \mathbf{P}^1(\mathbf{Q}) \to \mathbf{R}$ is determined by $H(a : b) = \max\{|a|, |b|\}$ when $(a, b) = 1$. Set

$$\widehat{h}(P) = \frac{1}{\deg f} \lim_{N\to\infty} 4^{-N} h_f(2^N \cdot P).$$

This gives a quadratic form on $E(\mathbf{Q})$ which does not depend on $f$. One calls $\widehat{h}$ the *Néron-Tate canonical height*; it vanishes on $E(\mathbf{Q})_{\mathrm{tors}}$.

**Proposition 2.12.4.** *The height function $h_x : E(\mathbf{Q}) \to \mathbf{R}$ satisfies the conditions of Proposition 2.12.2.*

*Proof.* We check that $h_x$ satisfies the last three conditions. The fact that $\#\{h < c\} < \infty$ is trivial. Now we show that for all $Q \in E(\mathbf{Q})$, there exists a constant $C_Q$ such that $h(P + Q) \leqslant 2h(P) + C_Q$ for all $P \in E(\mathbf{Q})$. Write $Q = (\frac{a_0}{d_0^2}, \frac{b_0}{d_0^3})$ and $P = (\frac{a}{d^2}, \frac{b}{d^2})$, where all the variables are in $\mathbf{Z}$, and $a_0, b_0, d_0$ are fixed. Write $E$ as $y^2 = x^3 + Ax + B$ for fixed $A, B \in \mathbf{Z}$. Basic algebra tells us that

$$x(P + Q) = \frac{(aa_0 + Ad^2d_0^2)(ad_0^2 + a_0d^2) + 2Bd^4d_0^4 - 2bdb_0d_0}{(ad_0^2 - a_0d^2)^2}.$$

The numerator is

$$a^2 \cdot (\text{fixed stuff}) + d^4 \cdot (\text{fixed stuff}) + bd \cdot (\text{f. s.}) + ad^2 \cdot (\text{f. s.})$$

In general, $H(r + s + t + u) \leqslant 4 \max\{H(r), H(s), H(t), H(u)\}$ when $r, s, t, u \in \mathbf{Z}$. The denominator is

$$a^2 \cdot (\text{fixed stuff}) + d^4 \cdot (\text{f. s.}) + ad^2 \cdot (\text{f. s.}).$$

We have $h_x(P) = \max\{\log |a|, \log |d|^2\}$. Bound $ad^2$ using Cauchy-Schwarz. For $bd$, plug $P$ into the equation $y^2 = x^3 + Ax + B$. One gets $b^2 = a^3 + Aad^4 + Bd^6$, whence

$$|b| \leqslant C \max\{|a^{3/2}|, |a^{1/2}d^2|, |d|^3\}.$$

Some more annoying computations give the result. The remaining condition is left to the reader. □

For a more conceptual approach to heights, see the book [BG06].

**Proposition 2.12.5.** *Let $k$ be a number field, $E_{/k}$ an elliptic curve. Let $v$ be a finite place at which $E$ has good reduction. Let $\mathcal{E}$ be the Néron model for $E$ at $v$, and let $m$ be an integer with $v \nmid m$. Then $E(k)[m] \hookrightarrow \mathcal{E}(\kappa_v)[m]$.*

*Proof.* This is hard – it uses the theory of formal groups and minimal Weierstrass models. □

When $k = \mathbf{Q}$, this tells us that $E(\mathbf{Q})[m] \hookrightarrow E(\mathbf{F}_l)$ whenever $l \nmid m$.

It remains to prove the weak Mordell-Weil theorem. Let $L = k(\frac{1}{m}E(k))$; then we have a pairing $E(k)/m \times \mathrm{Gal}(L/k) \to E[m]$. This is perfect if $E[m] \subset k$. Our job is to show that $\mathrm{Gal}(L/k)$ is finite. Note that $\mathrm{Gal}(L/k)$ is an $m$-torsion abelian group. If $mQ \in E(k)$, then $Q \in E(L)$. It follows that $k(Q)/k$ is unramified at those $v$ for which $E$ has good reduction at $v$ and $v \nmid m$. [...didn't write down whole proof. It's not hard...]

**Theorem 2.12.6.** *Let $k$ be a number field containing $\boldsymbol{\mu}_m$. Let $L/k$ be the maximal abelian extension killed by $m$ and ramified at a finite set. Then $[L : k] < \infty$.*

*Proof.* We will use the fact that $\mathrm{Cl}(k) = \mathrm{Pic}(\mathcal{O}_k)$ is finite. Moreover, each class is represented by a prime ideal $\mathfrak{p}$. So if we invert finitely many well chosen primes, we can kill the class group. That is, there is a finite set $S \subset \mathcal{O}_k \smallsetminus 0$ such that $\mathcal{O}_{k,S}$ is a principal ideal domain. For each fractional ideal $\mathfrak{a} \subset k$, we can talk about $v_\mathfrak{p}(\mathfrak{a})$, the $\mathfrak{p}$-adic valuation of $\mathfrak{a}$. This is the unique integer $n$ such that $\mathfrak{a}_\mathfrak{p} = \mathfrak{p}^n$ inside $\mathcal{O}_{k,\mathfrak{p}}$.

Note that $\mathcal{O}_k^\times = \{x \in \mathcal{O}_k : v_\mathfrak{p}(x) = 0 \text{ for all } \mathfrak{p}\}$. Note that we've excluded the archimedean places coming from the embeddings $k \hookrightarrow (\mathbf{R} \text{ or } \mathbf{C})$. There are $r_1 + r_2$ such embeddings, where $r_1$ (resp. $r_2$) is the number of real (resp. complex) places of $k$. If $S$ is a finite set of places of $k$, containing all archimedean places, put $\mathcal{O}_{k,S}^\times = \{x \in \mathcal{O}_k : v_\mathfrak{p}(x) = 0 \text{ for all } \mathfrak{p} \notin S\}$.

Since $\boldsymbol{\mu}_m \subset k$, Kummer theory tells us that any subextension $L \supset M \supset k$ with $M/k$ cyclic is of the for $M = k(\alpha^{1/m})$ for some $\alpha \in k^\times/m$. The extension $M/k$ is ramified exactly at those primes $\mathfrak{p}$ for which either $\mathfrak{p} \mid m$ or $v_\mathfrak{p}(\alpha) \not\equiv 0 \pmod m$. So if we let

$$T_S = \{\alpha \in k^\times/m : v_\mathfrak{p}(\alpha) \equiv 0 \pmod m \text{ for all } \mathfrak{p} \notin S\},$$

then $L = k(T_S^{1/m})$.

Let $S$ be the union of the set of places at which $L$ is ramified and the set of archimedean places. Enlarge $S$ as necessary to make $\mathrm{Pic}(\mathcal{O}_{k,S}) = 0$. Let $\alpha \in T_S$ be integral and consider $v_\mathfrak{p}(\alpha)$. At $\mathfrak{p} \in S$, we're a unit so we don't care about $v_\mathfrak{p}(\alpha)$. At $\mathfrak{p} \notin S$, $v_\mathfrak{p}(\alpha) \equiv 0 \pmod m$ so because $\mathrm{Pic}(\mathcal{O}_{k,S}) = 0$, $\alpha$ is an $m$-th power (up to unit). That is, $\alpha = \varepsilon\beta^m$ for some $\varepsilon \in \mathcal{O}_{k,S}^\times$. So $L$ is obtained by adjoining all $m$-th roots of elements of the finitely generated group $\mathcal{O}_{k,S}^\times$. □

**Theorem 2.12.7.** *Let $k$ be a number field, $S$ a finite set of places containing all archimedean places, then $\mathrm{rk}(\mathcal{O}_{k,S}^\times) = \#S - 1$.*

To summarize, the weak Mordell-Weil theorem states that for an elliptic curve $E_{/\mathbf{Q}}$, the group $E(\mathbf{Q})/m$ is finite. Via a Kummer pairing, we reduced this to showing that the extension $L/k$ is finite, where $k = \mathbf{Q}(E[m])$ and $L$ is the maximal abelian extension of $k$ killed by $m$ and unramified outside the (finite) set of places of bad reduction of $E$. We proved $L/k$ is finite by using classical Kummer theory, the finiteness of the class group, and the generalized Dirichlet unit theorem.

We used, but did not prove, two main ingredients in the proof of the Mordell-Weil theorem for elliptic curves:

1. The reduction map $E(k)[m] \to \mathcal{E}(\kappa_\mathfrak{p})[m]$ is injective for $\mathfrak{p} \nmid m$ of good reduction. This involves formal groups, the Néron-Ogg-Shafarevich criterion, and reduction theory.

2. An abstract height function on an abelian group satisfying certain axioms yields the finite generation of the group.

We did prove that the height function $h_x : E(\mathbf{Q}) \to \mathbf{R}_{\geqslant 0}$ satisfies (two of) the necessary axioms.

The theorem can generalize to arbitrary abelian varieties over arbitrary number fields. Besides the general theory of Néron models, no "really new" ideas are needed.

# 3 Main stuff

Let $k$ be a number field, $C_{/k}$ a smooth proper curve. Let $g$ be the genus of $C$. If $g = 0$, either $C(k) = \varnothing$, or $C \simeq \mathbf{P}^1_{/k}$. If $g > 1$, then Faltings gave an ineffective proof that $\#C(k) < \infty$. If $g = 1$, then either $C(k) = \varnothing$, or, if $C(k) \neq \varnothing$, then $C(k)$ is a finitely generated abelian group. Recall that the Birch and Swinnerton-Dyer conjecture is that $\operatorname{rk}(E(k)) = \operatorname{ord}_{s=1} L(E,s)$. The function $L(E,s)$ satisfies a functional equation $L(E,s) \sim \pm L(E, 2-s)$. We expect $(-1)^{\operatorname{rk}(E)} = \pm$ accordingly. This is the "sign conjecture." Kolyvagin and others have proved that if $L(E,s)$ has a pole of order at most 1 at 1, then BSD holds for $E$. A folklore question is: is $\sup_{E/\mathbf{Q}} \operatorname{rk}(E) < \infty$?

Any $E_{/\mathbf{Q}}$ can be written as $y^2 = x^3 + Ax + B$ where $A, B \in \mathbf{Z}$, and $p^6 \mid B \Rightarrow p^4 \nmid A$. The *height* of $E$ is $H(E) = \max(4|A|^3, 27B^2)$. This is asymptotically degree-six in the roots of $x^3 + Ax + B$. We could have ordered $E$ by (Galois-theoretic) conductor. The reason we use height is that the number of elliptic curves with height $\leqslant X$ is $CX^{5/6}$ + (error term) for some constant $C$. On the other hand, we have no idea how many elliptic curves there are with bounded conductor. So even though height isn't as conceptually elegant, we'll order elliptic curves by it.

Given $E_{/\mathbf{Q}}$ with algebraic rank 3, we could numerically show that the analytic rank is $\leqslant 3$, then use sign considerations to get t $r_{\text{an}} \in \{1, 3\}$. If $r_{\text{an}} = 1$, we know that $r_{\text{alg}} = 1$, a contradiction, hence $r_{\text{an}} = 3$. Thus, for (specific) elliptic curves with algebraic rank 3, it is possible to prove BSD. At the present, no one knows how to do this for a family of elliptic curves. From the Kummer exact sequence $0 \to E[p] \to E \xrightarrow{p} E \to 0$, one gets a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & E(\mathbf{Q})/p \arrow[r] & \mathrm{H}^1(\mathbf{Q}, E[p]) \arrow[r] & \mathrm{H}^1(\mathbf{Q}, E)[p] & 0. \end{tikzcd}$$

One has a similar short exact sequence for each place $v$. This yields a (now-familiar) commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & E(\mathbf{Q})/p \arrow[r] \arrow[d] & \mathrm{H}^1(\mathbf{Q}, E[p]) \arrow[r] \arrow[d] & \mathrm{H}^1(\mathbf{Q}, E)[p] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \prod E(\mathbf{Q}_v)/p \arrow[r] & \prod \mathrm{H}^1(\mathbf{Q}_v, E[p]) \arrow[r] & \prod \mathrm{H}^1(\mathbf{Q}_v, E)[p] \arrow[r] & 0.
\end{tikzcd}$$

Even better, we can write

$$\mathrm{Sel}_p(E) \ker\left(\mathrm{H}^1(\mathbf{Q}, E[p]) \to \mathrm{H}^1(\mathbf{A}, E)[p]\right),$$

where $\mathbf{A}$ is the ring of adeles over $\mathbf{Q}$ and "$\mathrm{H}^1$" denotes étale cohomology.

We'd like to give a geometric interpretation of $\mathrm{H}^1(\mathbf{Q}, E)$ and $\mathrm{H}^1(\mathbf{Q}, E[p])$. First, note that $\dim(E(\mathbf{Q})/p) = \mathrm{rk}(E) + \delta$, where $\delta = \dim E[p](\mathbf{Q}) \leqslant 2$. With respect to height, $\delta > 0$ on a density zero set, so we may as well assume $\delta = 0$. Recall there is a short exact sequence

$$0 \longrightarrow E(\mathbf{Q})/p \longrightarrow \mathrm{Sel}_p(E) \longrightarrow Ш[p] \longrightarrow 0.$$

Separating $\mathrm{Sel}_p(E)$ into its contributions from $E(\mathbf{Q})/p$ and $Ш[p]$ is very difficult. One conjectures that $Ш = \ker(\mathrm{H}^1(\mathbf{Q}, E) \to \mathrm{H}^1(\mathbf{A}, E))$ is finite for all $E$. This conjecture implies that $Ш[p] = 0$ for almost all $p$. Cassels has constructed a perfect pairing $Ш \times Ш \to \mathbf{Q}/\mathbf{Z}$. So if $\#Ш < \infty$, then $\#Ш$ should be a perfect square. The "Ш-part" of BSD can be computed in some examples, and it always turns out to be a perfect square.

[...recap of strategy for Bhargava's proof...]

$$\rho : \Gamma_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{T}_{\mathfrak{m}}).$$

## 3.1 Group cohomology

For the moment, let $G$ be a profinite group. By a $G$-module, we mean an abelian group $M$ with $G$-action, such that for all $m \in M$, the stabilizer $\mathrm{Stab}_G(m)$ is an open subgroup of $G$. The category of $G$-modules is an abelian category with enough injectives. Indeed, let $\mathcal{C}$ be the category of finite sets with continuous $G$-action. Then the category of $G$-modules is equivalent to the category of sheaves of abelian groups on $\mathcal{C}$. It is known in general that the category of abelian group objects in a Grothendieck topos has enough injectives.

**Definition 3.1.1.** *Let $M$ be a $G$-module. We define* $\mathrm{H}^i(G, M) = \mathsf{R}^i(-)^G(M)$.

That is, $\mathrm{H}^i(G, -)$ is the $i$-th derived functor of $(-)^G$. The group $\mathrm{H}^2(G, M)$ classifies central extensions $0 \to M \to X \to G \to 1$, up to isomorphism making the following diagram commute:

$$\begin{tikzcd}
1 \arrow[r] & M \arrow[r] \arrow[d, equal] & X \arrow[r] \arrow[d, "\wr"] & G \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & M \arrow[r] & Y \arrow[r] & G \arrow[r] & 1.
\end{tikzcd}$$

For $i \leqslant 2$, $\mathrm{H}^i(G,M)$ can be more readily computed directly. Let

$$\begin{aligned} Z^1(G,M) &= \{f : G \to M \text{ continuous, such that } f(\sigma\tau) = f(\sigma) + \sigma(f(\tau))\} \\ B^1(G,M) &= \{f : G \to M \text{ of the form } \sigma \mapsto \sigma(m) - m \text{ for some } m \in M\}. \end{aligned}$$

Then $\mathrm{H}^1(G,M) \simeq Z^1(G,M)/B^1(G,M)$.

If $H \subset G$, the restriction functor $\mathrm{res}^G_H(-)$ from $G$-modules to $H$-modules is exact, so the natural inclusion $\mathrm{H}^0(H, \mathrm{res}^G_H M) \hookrightarrow \mathrm{H}^0(G,M)$ extends canonically to a natural transformation $\mathrm{H}^\bullet(H, \mathrm{res}^G_H(-)) \to \mathrm{H}^\bullet(G,-)$.

**Theorem 3.1.2.** *If $G$ acts trivially on $M$, then $\mathrm{H}^1(G,M) = \hom(G,M)$.*

*Proof.* If $G$ acts trivially, then $B^1(G,M) = 0$. Also, $Z^1(G,M)$ consists of those $f : G \to M$ such that $f(\sigma\tau) = f(\sigma) + f(\tau)$. □

Let $k$ be a number field. If $v$ is a place of $k$, write $G_v \subset G_k$ for the Galois group $\mathrm{Gal}(\overline{k_v}/k_v)$. If $M$ is a $G_k$-module $v$ is a place of $k$, one puts

$$Ш(M) = \ker\left(\mathrm{H}^1(k,M) \to \prod_v \mathrm{H}^1(k_v,M)\right).$$

**Theorem 3.1.3.** *Let $k$ be a number field, $M$ a finite $G_k$-module. Then $Ш(M)$ is finite.*

*Proof.* Let $K = k(M)$; then $G_K$ acts trivially on $M$. If $f \in Ш(M)$, then $f|_{G_K}$ is a homomorphism cutting out an extension $L/K$. Since $f|_{G_v} = 0$ for all places $v$ of $K$, we know that all primes in $L$ split completely (hence are unramified) over $K$. By the Hermite-Minkowski thorem, there are only finitely many possibilities for $f$. □

Via the above proof, we see that cohomology relates to class groups (via Hermite-Minkowski). Let $M$ be a finite $\mathbf{F}_p[G_{\mathbf{Q}_l}]$-module. Put $M^* = \hom(M, \boldsymbol{\mu}_p)$. Then there is a perfect pairing $\mathrm{H}^\bullet(\mathbf{Q}_l, M) \times \mathrm{H}^{2-\bullet}(\mathbf{Q}_l, M^*) \to \mathrm{H}^2(\mathbf{Q}_l, \boldsymbol{\mu}_p)$, and

$$\sum_{i=0}^{2} (-1)^i \dim_{\mathbf{F}_p} \mathrm{H}^i(\mathbf{Q}_l, M) = \begin{cases} 0 & l \neq p \\ -\dim(M) & l = p \end{cases}$$

This is *Local Tate Duality*. It should be thought of as analogous to algebraic topology. In fact, étale cohomology is the “right” cohomology theory for varieties, and satisfies a good duality theory that resembles Poincaré duality. There is a duality theory for modules over $G_k$ when $k$ is a global field. You can compute $\dim \mathrm{H}^1(\mathbf{Q}, M) - \dim \mathrm{H}^2(\mathbf{Q}, M)$ when $M$ is a $\mathbf{F}_p[G_{\mathbf{Q}}]$-module. Getting either one of $\mathrm{H}^1$ or $\mathrm{H}^2$ involves computing the class group of $\mathbf{Q}(M)$.

## 3.2 Geometric interpretation of cohomology

The elliptic curves

$$\begin{aligned} E_1 &: y^2 = x^3 + x + 1 \\ E_2 &: 3y^2 = x^3 + x + 1, \end{aligned}$$

are isomorphic over $\mathbf{Q}(\sqrt{3})$ but not over $\mathbf{Q}$. Considering such pairs is a standard approach to the $r_{\text{an}} \leqslant 1$ cases of BSD.

In general, if $L/K$ is a field extension and $X_{/L}$ is some "arithmetic object" the set of $Y_{/K}$ giving rise to $X$ via base-change is classified by $\mathrm{H}^1(\mathrm{Gal}(L/K), \mathrm{Aut}\, X)$. Since $\mathrm{Aut}(X)$ might be nonabelian, this $\mathrm{H}^1(L/K, \mathrm{Aut}\, X)$ may only be a pointed set.

Let $E_{/\mathbf{Q}}$ be an elliptic curve. We'll realise $E[p]$ and $E(\overline{\mathbf{Q}})$ as automorphisms of pairs of objects, one entry of which is $E$. So $\mathrm{H}^1(\mathbf{Q}, E[p])$ and $\mathrm{H}^1(\mathbf{Q}, E)$ will classify descents of some type of object to $\mathbf{Q}$.

**Definition 3.2.1.** *Let $G$ be a profinite group, $N$ a (possibly nonabelian) group with continuous $G$-action. Then $Z^1(G, N)$ is the set of continuous $f : G \to N$ such that $f(\sigma\tau) = f(\sigma)\sigma(f(\tau))$ for all $\sigma, \tau \in G$. If $f, g \in Z^1(G, N)$, we say they are* cohomologous *if there exists $n \in N$ such that $f(\sigma) = n^{-1}g(\sigma)\sigma(n)$ for all $\sigma \in G$. Let $\mathrm{H}^1(G, N) = Z^1(G, N)/\sim$, where $f \sim g$ if $f$ is cohomologous to $g$.*

We'll find elements of $\mathrm{H}^1(\mathbf{Q}, E[p])$ that correspond bijectively to pairs $(C, D)$ where $C$ is a curve of genus 1 over $\mathbf{Q}$ and $D$ is a divisor of degree $p$ over $\mathbf{Q}$. These correspond to maps $C \to S \simeq_{\overline{\mathbf{Q}}} \mathbf{P}^{p-1}$, where $C \simeq_{\overline{\mathbf{Q}}} E$.

**Example 3.2.2.** Let $C_{/\mathbf{Q}}$ be the projective curve $3x^3 + 4y^3 + 5z^3 = 0$. Then $C(\mathbf{Q}) = \varnothing$. However, if we take some $x \in C(\overline{\mathbf{Q}})$ and let $D = \sum_{\sigma \in G_{\mathbf{Q}}} (\sigma(x))$, then $D$ is a divisor on $C$ defined over $\mathbf{Q}$. Essentially, the point is that even if $C(\mathbf{Q}) = \varnothing$, we will have $\mathrm{Pic}^\circ(C)(\mathbf{Q}) \neq \varnothing$. ▷

**Theorem 3.2.3.** *Let $E_{/\mathbf{Q}}$ be an elliptic curve. Then $\mathrm{Sel}_p(E)$ is finite.*

*Proof.* We essentially reprove weak Mordell-Weil. Recall that if $l \neq p$ is a prime of good reduction, then $E[p] \hookrightarrow E_{\mathbf{F}_l}(\overline{\mathbf{F}_l})$. Alternatively, the inertia group $I_l$ acts trivially on $E[p]$. So we'll prove that any $f \in \mathrm{Sel}_p E$ is unramified outside a (fixed) finite set, namely $p$ together with the set of bad primes for $E$. Let $S$ be that set. For $l \notin S$, the restriction $f|_{G_{\mathbf{Q}_l}}$ is a coboundary in $\mathrm{H}^1(\mathbf{Q}_l, E)$. So there exists $P \in E(\overline{\mathbf{Q}_l})$ such that $f(\sigma) = \sigma(P) - P$ for all $\sigma \in G_{\mathbf{Q}_l}$. But $\sigma(P) - P \in E[p]$. For $\sigma \in I_l$, $\sigma(P) - P = 0$ in $E(\overline{\mathbf{F}}_l)$. Since $E[p] \hookrightarrow E_{\mathbf{F}_l}[p]$, we have $\sigma(P) = P$, i.e. $f(I_l) = 0$. We have shown that all classes $f \in \mathrm{Sel}_p(E)$ are unramified outside of $S$, which yields the result. □

This proof depends on the finiteness of the class group.

**Lemma 3.2.4.** *Let $E_{/\mathbf{Q}}$ be an elliptic curve, $\phi : E \to E$ a nonconstant map such that $\phi(0) = 0$. Then $\phi$ is an isogeny. Moreover, if $\phi$ is an isomorphism ad commutes with all translations, then $\phi = 1$.*

*Proof.* We sketch a proof of the latter claim. If $E$ is non-CM, then $\phi = \pm 1$. Clearly $-1$ does not commute with translations, so $\phi = 1$. If $E$ has CM, think about $E_{/\mathbf{C}} \simeq \mathbf{Z}/\Lambda$ for $\Lambda$ an order in a quadratic imaginary field. Say $\Lambda = \langle 1, \tau \rangle$ for $\tau \in \mathbf{Q}(\sqrt{-d})$ where $d \in \{1, 3\}$. The only automorphisms are $\{\pm 1, \pm i\}$ or $\{\pm 1, \pm \omega, \pm \omega^2\}$. You can check directly that none of these commute with translations, except for 1.

Alternatively, just plug $x = 0$ into $\phi(x + y) = \phi(x) + y$. □

**Definition 3.2.5.** *Let $k$ be a field of characteristic zero, $C_{/k}$ a curve. A* twist *of $C$ is a curve $D_{/k}$ together with an isomorphism $\phi : C_{\overline{k}} \xrightarrow{\sim} D_{\overline{k}}$.*

The philosophy is that $\mathrm{H}^1(G_{\mathbf{Q}}, \mathrm{Aut}(E_{\overline{\mathbf{Q}}}))$ classifies twists of $E$ over $\mathbf{Q}$. More generally, if "$X_{/\mathbf{Q}}$ is an object," then $\mathrm{H}^1(G_{\mathbf{Q}}, \mathrm{Aut}(X_{\overline{\mathbf{Q}}}))$ classifies twists of $X$."

**Theorem 3.2.6.** *Let $X_{/\mathbf{Q}}$ be a twist of $\mathbf{P}^n_{/\mathbf{Q}}$. Then $X \simeq \mathbf{P}^n$ if and only if $X(\mathbf{Q}) \neq \varnothing$. Moreover, if $X(\mathbf{A}) \neq \varnothing$, then $X(\mathbf{Q}) \neq \varnothing$.*

We will use this theorem because $\alpha \in \mathrm{Sel}_p\, E$ gives rise to a map $C \to S$, where $C$ is a twist of $E$ and $S$ is a twist of $\mathbf{P}^{p-1}_{/\mathbf{Q}}$. But elements of $\mathrm{Sel}_p(E)$ are locally trivial. This will imply $C(\mathbf{A}) \neq \varnothing$. Thus $S(\mathbf{A}) \neq \varnothing$, so $S \simeq \mathbf{P}^{p-1}$. We end up with a curve $C \subset \mathbf{P}^{p-1}$. We hope to write such curves as the zero-locus of a single function, or a small managable set of functions. For $p \in \{2, 3, 5\}$, this can be done.

Suppose we are given a twist $C'$ of $C_{/\mathbf{Q}}$ with $\phi : C'_{\overline{\mathbf{Q}}} \xrightarrow{\sim} C_{\overline{\mathbf{Q}}}$. Define $f : G_{\mathbf{Q}} \to \mathrm{Aut}(C_{\overline{\mathbf{Q}}})$ by $f(\sigma) = \phi^\sigma \circ \phi^{-1}$. Here, $\phi^\sigma(x) = \sigma(\phi(x))$.

**Proposition 3.2.7.** *As constructed above, $f$ is a 1-cocycle. Moreover, adjusting $f$ by a 1-coboundary preserves the isomorphism class of $C'$. So $C \mapsto f$ induces a bijection between the set of isomorphism classes of twists of $C$ and $\mathrm{H}^1(G_{\mathbf{Q}}, \mathrm{Aut}(C_{\overline{\mathbf{Q}}}))$.*

*Proof.* We begin with a computation:

$$\begin{aligned} f(\sigma\tau) &= \phi^{\sigma\tau}\phi^{-1} \\ &= \phi^{\sigma\tau}(\phi^\tau)^{-1}\phi^\tau\phi^{-1} \\ &= (\phi^\sigma\phi^{-1})^\tau\phi^\tau\phi^{-1} \\ &= {}^\tau f(\sigma) f(\tau). \end{aligned}$$

The rest is relatively trivial. Showing surjectivity is a bit tricky – this ends up being a special case of descent (étale descent, to be precise). □

We'll begin with the easier case of a discrete $G_{\mathbf{Q}}$-module. Let $f \in \mathrm{H}^1(G_{\mathbf{Q}}, \mathrm{Aut}(M))$; we need to build a twist of $M$. Put $\sigma \cdot_f m = f(\sigma)(\sigma(m))$. Check that $\cdot_f$ gives a well-defined action of $G_{\mathbf{Q}}$ on $M$. Write $f^* M$ for the twist of $M$ that we have defined. Check that if $f$ is a coboundary, then $M \simeq f^* M$.

**Theorem 3.2.8** (Bhargava-Shankar). *Set $E : y^2 = x^3 - \frac{I}{3}x - \frac{J}{27}$ for $I, J \in k$. Then $E(k)/2$ is naturally in bijection with $\mathrm{PGL}_2$-orbits of $k$-soluble binary quartic forms having invariants $I$ and $J$, via*

$$(\varepsilon, \eta) \mapsto \frac{x^4}{4} - \frac{3}{2}\varepsilon x^2 y^2 + 2\eta x y^3 + \left(\frac{I}{3} - \frac{3}{4}\varepsilon^2\right) y^4.$$

## 3.3 Torsors

**Definition 3.3.1.** *Let $E_{/\mathbf{Q}}$ be an elliiptic curve. A* torsor *under $E$ is a curve $C_{/\mathbf{Q}}$ with $E$-action such that $C_{\overline{\mathbf{Q}}} \simeq E_{\overline{\mathbf{Q}}}$ as $E$-varieties.*

That is, we are given a map $\mu : E \times C \to C$ defined over $\mathbf{Q}$ satisfying the appropriate associativity conditions. Given any $x \in C(\overline{\mathbf{Q}})$, the map $\mu(-, x) : E_{\overline{\mathbf{Q}}} \to C_{\overline{\mathbf{Q}}}$ will be an isomorphism of varieties over $\overline{\mathbf{Q}}$.

**Definition 3.3.2.** *Two $E$-torsors $C_1, C_2$ are isomorphic if there exists an $E$-equivariant isomorphism $\phi : C_1 \xrightarrow{\sim} C_2$ defined over $\mathbf{Q}$.*

So we need the following diagram to commute:

$$\begin{tikzcd}
E \times C_1 \arrow[r, "\mu_1"] \arrow[d, "1\times\phi"] & C_1 \arrow[d, "\phi"] \\
E \times C_2 \arrow[r, "\mu_2"] & C_2.
\end{tikzcd}$$

The *trivial torsor* is $E \times E \xrightarrow{+} E$. Note that by definition, every torsor is a twist of the trivial torsor. Recall that $\mathrm{Aut}_E(E)$, the group of $E$-equivariant automorphisms of $E$, is $E$. Thus $\mathrm{H}^1(\mathbf{Q}, E)$ classifies $E$-torsors up to isomorphism. In general, let $G_{/k}$ be a group scheme. Then $\mathrm{H}^1(\mathbf{Q}, G)$ classifies $G$-torsors up to isomorphism.

The papers [Cre+08; Cre+09; Cre+14] give many different descriptions of elements of $\mathrm{H}^1(\mathbf{Q}, E[p])$ for $p$ not necessarily prime.

**Definition 3.3.3.** *A torsor divisor class pair (of degree $p$) is an $E$-torsor with a divisor $D$ of degree $p$, defined over $\mathbf{Q}$.*

Two torsor divisor class pairs $(C_1, D_1)$, $(C_2, D_2)$ are isomorphic if there is an isomorphism $\phi : C_1 \to C_2$ of $E$-torsors such that $\phi^* D_2 \sim D_1$ in $\mathrm{Pic}(C_1)$. The trivial torsor divisor class pair is $(E, p \cdot 0)$.

**Lemma 3.3.4.** *Every torsor divisor class pair is a twist of $(E, p \cdot 0)$.*

*Proof.* Let $\phi : C_{\overline{\mathbf{Q}}} \xrightarrow{\sim} E_{\overline{\mathbf{Q}}}$. We need $\phi^*(p \cdot 0) \sim 0$. Equivilantly, we need $p \cdot 0 - (\phi^{-1})^* D \sim 0$. It is sufficient to show that the sum of points (with multiplicities) in $\phi^{-1*} D$ equal to 0 on $E$? Say the sum is $x \in E(\overline{\mathbf{Q}})$. Let $py = x$ and compose $\phi$ with "translate by $-y$." This gives the result. □

**Lemma 3.3.5.** $\mathrm{Aut}_{E_{\overline{\mathbf{Q}}}}(E, p \cdot 0) = E[p]$.

*Proof.* Any automorphism of a torsor divisr class pair must be translation by some element, and the condition $\phi * D_2 \sim D_1$ forces that point to be $p$-torsion. □

It follows that $\mathrm{H}^1(\mathbf{Q}, E[p])$ is in bijection with the set of isomorphism classes of torsor divisor class pairs. Note that $\mathrm{H}^1(\mathbf{Q}, E[p]) \supset \mathrm{Sel}_p E \supset E(\mathbf{Q})/p$. The latter set corresponds to those $(C, D)$ for which $C(\mathbf{Q}) \neq \varnothing$, while $\mathrm{Sel}_p E$ corresponds to the set of $(C, D)$ for which $C(\mathbf{A}) \neq \varnothing$.

**Definition 3.3.6.** *A* Brauer-Severi diagram *$C \to S$ is a morphism from $C$, an $E$-torsor, to $S$, a twist of $\mathbf{P}^{p-1}$.*

Twoo Brauer-Severi diagrams $C_1 \to S_1$ and $C_2 \to S_2$ are isomorphic if there isomorphisms $\phi : C_1 \xrightarrow{\sim} C_2$ and $\psi : S_1 \to S_2$ making the following diagram commute:

$$\begin{tikzcd} C_1 \arrow[r] \arrow[d, "\phi"] & S_1 \arrow[d, "\psi"] \\ C_2 \arrow[r] & S_2. \end{tikzcd}$$

The trivial Brauer-Severi diagram is the map $E \to \mathbf{P}^{p-1}$ coming from the divisor $p \cdot 0$.

**Lemma 3.3.7.** *The trivial Brauer-Severi diagram $E \to \mathbf{P}^{p-1}$ satisfies* $\operatorname{Aut}(E \to \mathbf{P}^{p-1}) = E[p]$.

*Proof.* Let $\phi : E_{\overline{\mathbf{Q}}} \xrightarrow{\sim} E_{\overline{\mathbf{Q}}}$. We need $\phi^*(p \cdot 0) = (p \cdot 0)$. We know $\phi = (-) + x$ for some $x$, and $\phi^*(p \cdot 0) \sim (p \cdot 0)$ implies $x \in E[p]$. We need an automorphism of projective space making the following diagram commute:

$$\begin{tikzcd} E \arrow[r, "p\cdot 0"] \arrow[d, "+x"] & \mathbf{P}^{p-1} \arrow[d, dashed] \\ E \arrow[r, "\phi^*(p\cdot 0)"] & \mathbf{P}^{p-1}. \end{tikzcd}$$

Such an automorphism exists because $\operatorname{Aut}(\mathbf{P}^{p-1}) = \mathrm{GL}(p)$ acts transitively on $\mathbf{P}^{p-1}$. □

**Definition 3.3.8.** *An $n$-*covering *of $E$ is a curve $C_{/\mathbf{Q}}$ together with $\pi : C \to E$, such that there is an isomorphism $\phi : C_{\overline{\mathbf{Q}}} \xrightarrow{\sim} E_{\overline{\mathbf{Q}}}$ making the following diagram commute:*

$$\begin{tikzcd} C \arrow[d, "\phi"] \arrow[dr, "\pi"] & \\ E \arrow[r, "n"] & E. \end{tikzcd}$$

The trivial $n$-covering is $\cdot n : E \to E$.

**Lemma 3.3.9.** *All $n$-coverings are twists of the trivial $n$-covering. Moreover, the trivial $n$-covering has automorphism group $E[n]$.*

Thus isomorphism classes of $n$-coverings of $E$ are in bijection with $\mathrm{H}^1(\mathbf{Q}, E[n])$.

**Definition 3.3.10.** *Let $\pi : C \twoheadrightarrow E$ be an $n$-covering. Then $(C, \pi)$ is* solvable *if $C(\mathbf{Q}) \neq \varnothing$, and* locally soluble *if $C(\mathbf{A}) \neq \varnothing$.*

Let $x_0 \in E(\mathbf{Q})/p \subset \operatorname{Sel}_p E \subset \mathrm{H}^1(\mathbf{Q}, E[p])$. Consider $\pi(x) = p \cdot x + x_0$. Then $\phi(x) = x + (\text{some } \frac{1}{p}x_0)$. So $\pi$ is trivial if and only if $x_0 = 0$ in $E(\mathbf{Q})/p$.

Let $\alpha \in \operatorname{Sel}_p(E)$. We know that $\alpha = 0$ in $\mathrm{H}^1(\mathbf{A}, E)$. Thus, if $C$ is the corresponding $p$-covering, we have $C(\mathbf{A}) \neq \varnothing$. Finally, $\alpha$ will correspond to a Brauer-Severi embedding which is locally soluble. Since projective spaces satisfy the Hasse principle, locally soluble Brauer-Severi embeddings look like $C \to \mathbf{P}^{p-1}$.

## 3.4 Review and plan of attack

Let $E_{/\mathbf{Q}}$ be an elliptic curve. So far, we've (mostly) proved that $E(\mathbf{Q})$ is finitely generated. The one thing we skipped was the fact that $E[n] \hookrightarrow \mathcal{E}_{\mathbf{F}_l}(\overline{\mathbf{F}_l})$ so long as $l \nmid n$ and $l$ is a prime of good reduction. We can write $E(\mathbf{Q}) \simeq \mathbf{Z}^r \oplus T$, where $T$ is a finite group. Due to Mazur's work in [Maz77], we completely understand $T$. Mazur's proof requires some extremely delicate algebraic geometry. The rank $r = \operatorname{rk}(E)$ is still poorly understood.

One way to bound $r$ is to look at the canonical short exact sequence

$$0 \longrightarrow E(\mathbf{Q})/p \longrightarrow \operatorname{Sel}_p(E) \longrightarrow \text{Ш}(E)[p] \longrightarrow 0.$$

It gives us the bound $p^r \leqslant \# \operatorname{Sel}_p(E)$, or equivalently $r \leqslant \dim \operatorname{Sel}_p(E)$. We interpreted elements of $\operatorname{Sel}_p(E)$ as locally soluble $p$-coverings of $E$, and elements of $E(\mathbf{Q})/p \subset \operatorname{Sel}_p(E)$ as those coverings which are actually globally soluble. Both these groups live inside $\mathrm{H}^1(\mathbf{Q}, E[p])$, which classifies *all* $p$-coverings of $E$. Recall that a $p$-covering is a map $\psi : C \twoheadrightarrow E$ defined over $\mathbf{Q}$, for which there exists an isomorphism $\phi : C_{\overline{\mathbf{Q}}} \to E_{\overline{\mathbf{Q}}}$ making the following diagram commute:

$$\begin{tikzcd}
C_{\overline{\mathbf{Q}}} \arrow[d, "\phi"] \arrow[dr, "\psi"] & \\
E_{\overline{\mathbf{Q}}} \arrow[r, "p"] & E.
\end{tikzcd}$$

For such a covering to be locally soluble, one needs $C(\mathbf{A}) \neq \varnothing$, and to be globally soluble, one needs $C(\mathbf{Q}) \neq \varnothing$. The group $\mathrm{H}^1(\mathbf{Q}, E[p])$ classifies diagrams $C \to S$, where $S$ is a twist of $\mathbf{P}^{p-1}_{/\mathbf{Q}}$. The group $\operatorname{Sel}_p(E)$ classifies diagrams $C \to S$, where $S \simeq \mathbf{P}^{p-1}$.

Note that everything we have done with $\operatorname{Sel}_p(E)$ and $\mathrm{H}^1(\mathbf{Q}, E[p])$ works for $p = n$ a composite number. Bhargava and Shankar find $\operatorname{avg}(\# \operatorname{Sel}_n)$ for $n \in \{2, 3, 4, 5\}$. It's

$$\sigma(n) = \sum_{d \mid n} d.$$

These sorts of sums show up in Eisensterin series, which are used extensively in Mazur's classification of the possible torsion in $E(\mathbf{Q})$.

Let $p = 2$. Then $\operatorname{Sel}_2 E$ classifies degree-two maps $C \to \mathbf{P}^1$. From Riemann-Hurwitz, we get

$$\chi(C) = 2\chi(\mathbf{P}^1) - \sum (e_x - 1),$$

which shows that there must be four branch points. So $C$ comes from a binary quartic $ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$.

If we set $p = 3$, we are looking at maps $C \hookrightarrow \mathbf{P}^2$ whose image is the zero locus of a ternary cubic. Such cubics live in a 10-dimensional space.

For $n = 4$, we classify maps $C \hookrightarrow \mathbf{P}^3$. The image is no longer the zero locus of one function, but rather a complete intersection of two quadrics.

When $p = 5$, we have maps $C \hookrightarrow \mathbf{P}^4$. The image is not a complete intersection. It will be defined by five quadrics coming from $4 \times 4$ submatrices of a skew-symmetric $5 \times 5$ matrix (all thought of as quadratic forms). The moral of the story is that the geometry is getting a *lot* harder.

**Theorem 3.4.1.** *If, for all $p$, $\operatorname{avg}(\# \operatorname{Sel}_p) = p + 1$, then BSD holds $100\%$ of the time.*

The curves in the above theorem will all have $r_{\text{an}}, r_{\text{alg}} \leqslant 1$.

The group $E(\mathbf{Q})/2$ corresponds to globally soluble diagrams $C \to \mathbf{P}^1$, which in turn correspond to binary quartics. The point $(\varepsilon, \eta)$ on the elliptic curve $E : y^2 = x^3 - \frac{I}{3}x - \frac{J}{27}$ corresponds to the quartic

$$\frac{x^4}{4} - \frac{3}{2}\eta^2 x^2 y^2 + 2\eta x y^3 + \left(\frac{I}{3} - \frac{3}{4}\varepsilon^2\right) y^4.$$

The point $0 \in E(\mathbf{Q})/2$ corresponds to a quartic having a linear factor.

**Example 3.4.2.** Let $(I, J) = (3, -27)$. Then our curve is $E : y^2 = x^3 - x + 1$. The point $(1, 1) \in E(\mathbf{Q})$ has $(1, 1) + (1, 1) = (-1, 1) = (\varepsilon, \eta)$. So the corresponding quartic should have a linear factor. This quartic is

$$\frac{1}{4}x^4 + \frac{3}{2}x^2y^2 + 2xy^3 + \frac{1}{4}y^4 \sim \frac{1}{4}(x^4 + 6x^2 + 8x + 1),$$

which has the integer $x = 1$ is a root. The quartic corresponding to $(1, 1)$ is

$$\frac{1}{4}x^4 - \frac{3}{2}x^2y^2 + 2xy^3 + \frac{1}{4}y^4 \sim \frac{1}{4}(x^4 - 6x^2 + 8x + 1),$$

which has no rational roots. ▷

**Theorem 3.4.3.** *Let $E_{/\mathbf{Q}}$ be the affine curve given by $y^2 = x^3 + Ax + B$. Then $\# E(\mathbf{Z}) < \infty$.*

Looking ahead: our job now is to count binary quartic forms. They live in the space $V_R = \{(a, b, c, d, e) \in R^5\}$ where $R$ is some commutative ring (probably just $\mathbf{Z}$, $\mathbf{Q}$, or some $\mathbf{Q}_v$). Write an element of $V_R$ as $f = ax^4 + \cdots + ey^4$. The group $\mathrm{GL}_2(R)$ acts on $V_R$ by

$$(\gamma \cdot f)(x, y) = f\left(\begin{pmatrix} x & y \end{pmatrix} \gamma\right).$$

Set

$$\begin{aligned} I &= 12ae - 3bd + c^2 \\ J &= 72ace + 9bcd - 27cd^2 - 27eb^2 - 2c^3. \end{aligned}$$

Then $\mathbf{Q}[a, b, c, d, e]^{\mathrm{SL}_2^{\pm}(\mathbf{Q})} = \mathbf{Q}[I, J]$ is a polynomial ring. We'll count binary quartics with given invariant $(I, J)$. That will correspond to elliptic curves $E_{/\mathbf{Q}}$ of the form $y^2 = x^3 + \frac{I}{?} + \frac{J}{*}$, where $?$ and $*$ are fixed constants only involving powers of 2 and 3. For given $(I, J)$, there are only finitely many equivalence classes of quartics.

If we studied binary quadratics $ax^2 + bxy + cy^2$, the ring of invariants is generated by the discriminant $b^2 - 4ac$. The crucial property is: is $b^2 - 4ac \equiv 0 \pmod 4$ for $f \in V_{\mathbf{Z}}$?

**Theorem 3.4.4.** *A pair $(I,J)$ occurs as the invariant of a binary quartic form if and only if*

1. $(I,J) \equiv (0,0) \mod (3,27)$,
2. $(I,J) \equiv (1,\pm 2) \mod (9,27)$,
3. $(I,J) \equiv (4,\pm 16) \mod (9,27)$,
4. $(I,J) \equiv (7,\pm 7) \mod (9,27)$,

Modulo $(9,27)$, there are 9 pairs. So $\frac{1}{27}$ of pairs occur.

**Theorem 3.4.5.** *Let $h^{(i)}(I,J)$ be the number of* $\mathrm{GL}_2(\mathbf{Z})$*-equivalence classes of irreducible binary quartic forms having invariants $(I,J)$, and having $4-2i$ real roots. Then*

$$\sum_{H(I,J)<X} h^{(0)}(I,J) = \frac{4}{135}\zeta(2)X^{5/6} + O(X^{3/4+\epsilon})$$

$$\sum_{H(I,J)<X} h^{(1)}(I,J) = \frac{32}{135}\zeta(2)X^{5/6} + O(X^{3/4+\epsilon})$$

$$\sum_{H(I,J)<X} h^{(2)}(I,J) = \frac{8}{135}\zeta(2)X^{5/6} + O(X^{3/4+\epsilon}),$$

*where $H(I,J) = \max(|I|^3, J^2)$ [with some constants].*

We have to omit the $(I,J)$ corresponding to singular curves, but that's a thin set with size $O(X^{1/3})$.

We need to understand $\mathrm{GL}_2(\mathbf{Z})\backslash V_{\mathbf{Z}}$. We'll also be interested in $\mathrm{GL}_2(\mathbf{R})\backslash V_{\mathbf{R}}$ or $\mathrm{GL}_2(\mathbf{Z})\backslash V_{\mathbf{R}}$. We'll find a fundamental domain for something like $\mathrm{GL}_2(\mathbf{Z})\backslash V_{\mathbf{R}}$, and count lattice points inside the domain. The fundamental domain will have a cusp and a "main body." You can estimate the volume of the main body; this gives (roughly) the number of integral points. To handle the cusp, we first thicken it slightly, then find that far out lattice points have linear factors, so they correspond to $0 \in \mathrm{Sel}_2 E$.

## 3.5 The case $p = 2$

For any ring $R$, let $V_R$ be the set of binary quartic forms over $R$. We're especially interested in $V_{\mathbf{Z}}$, $V_{\mathbf{R}}$, and $V_{\mathbf{Q}}$. Recall that $\mathrm{GL}_2(R)$ acts on $V_R$. We'd like to count elements of $\mathrm{GL}_2(\mathbf{Z})\backslash V_{\mathbf{Z}}$.

In general, if a discrete group $G$ acts on a manifold $X$, it is useful to find a fundamental domain $\mathcal{F} \subset X$ for the action of $G$ on $X$. The example we care about is $\mathrm{GL}_2(\mathbf{Z})$ acting on $V_{\mathbf{R}}$.

The group $\mathrm{SL}_2(\mathbf{R})$ acts on the upper half-plane $\mathfrak{H} = \{z \in \mathbf{C} : \Im z > 0\}$ in the standard way via fractional linear transformations:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}.$$

The action is transitive, because

$$\begin{pmatrix} \sqrt{x} & x/\sqrt{y} \\ & 1/\sqrt{y} \end{pmatrix} \cdot i = x + iy.$$

Let's compute the stabilizer. If $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot i = i$, then $a = d, b = -c$. But the matrix lies in $\mathrm{SL}_2(\mathbf{R})$, so $\det = a^2 + b^2 = 1$, whence $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathrm{SO}_2(\mathbf{R})$. It easily follows that $\mathrm{Stab}_{\mathrm{SL}_2(\mathbf{R})}(i) = \mathrm{SO}_2(\mathbf{R})$. So we can think of $\mathrm{SL}_2(\mathbf{R}) / \mathrm{SO}_2(\mathbf{R}) \simeq \mathfrak{H}$.

One conceptual picture here is: $\mathrm{GL}_2(\mathbf{R})$ acts on $\mathbf{C}/\mathbf{R}$, and elements with negative determinant swap $\mathfrak{H}$ with $\mathfrak{H}^- = \{z \in \mathbf{Z} : \Im z < 0\}$. Connected components, symmetric spaces, ....

[K. Conrad notes, maybe NAK decomposition.

Serre's *Arithmetic*

Bump

Gelbart: *Automorphic forms an adele groups*]

A couple elements of $\mathrm{SL}_2(\mathbf{Z})$ act in easily computable ways:

$$\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \cdot z = z + 1$$
$$\begin{pmatrix} & -1 \\ 1 & \end{pmatrix} \cdot z = -\frac{1}{z}.$$

**Theorem 3.5.1.** *A fundamental domain for the action of* $\mathrm{SL}_2(\mathbf{Z})$ *on* $\mathfrak{H}$ *is*

$$\mathcal{F} = \{z \in \mathfrak{H} : |z| \geqslant 1 \text{ and } -1/2 \leqslant \Im z \leqslant 1/2\}[fudgeonboundary].$$

*Proof.* This proof is [p. 77 of Serre]. Let $\gamma \in \mathrm{SL}_2(\mathbf{Z})$, and write $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then

$$\gamma \cdot z = \frac{az + b}{cz + d} = \frac{(az + b)(c\bar{z} + d)}{|cz + d|^2},$$

which has imaginary part $|cz + d|^{-2} \Im(z)$. Fix $z_0 \in \mathfrak{H}$. Note that $\Im(\gamma \cdot z_0) > \Im(z_0)$ if and only if $|cz_0 + d|$. The set $\{cz_0 + d : c, d \in \mathbf{Z}\} \subset \mathbf{C}$ is a lattice, so its intersection with $\{z \in \mathbf{C} : |z| < 1\}$. It follows that in $\mathrm{SL}_2(\mathbf{Z}) \cdot z_0$, there is an element which attains the largest possible size for $\Im(\gamma \cdot z_0)$. As $\begin{pmatrix} 1 & b \\ & 1 \end{pmatrix} z_0 = z_0 + b$, we can choose a representative $z_1$ of $\mathrm{SL}_2(\mathbf{Z}) \cdot z_0$ with maximal imaginary part, which also has real part in $[-1/2, 1/2)$. Furthermore, $|z_1| \geqslant 1$. Indeed, otherwise $\begin{pmatrix} & -1 \\ 1 & \end{pmatrix} \cdot z_1 = -z_1^{-1}$, which either has size $> 1$ or bigger imaginary part. We've shown that every orbit $\mathrm{SL}_2(\mathbf{Z}) \cdot z_0$ intersects $\mathcal{F}$. All we need to do is show that if $z_1, z_2 \in \mathcal{F}$ are in the same $\mathrm{SL}_2(\mathbf{Z})$-orbit, then

1. $z_2 = z_1 + 1$, or

2. $z_2 = -1/z_1$ and $|z_1| = |z_2| = 1$.

Without loss of generality, suppose $z$ and $\gamma z$ are both in $\overline{\mathcal{F}}$ and have $\Im(\gamma z) \geqslant \Im(z)$. So for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we have $|cz + d| \leqslant 1$ and $|z| \geqslant 1$. If $|c| \geqslant 2$, then $|cz + d| \geqslant 1$. So $c \in \{0, -1, 1\}$.

If $c = 0$, we need only consider the case $\gamma = \begin{pmatrix} 1 & b \\ & 1 \end{pmatrix}$, which translates to the right by $b \in \mathbf{Z}$.

If $c = -1$, this is similar to $c = 1$.

If $c = 1$, $|cz + d| = |z + d| \leqslant 1$. Then $d \in \{-1, 0, 1\}$. Suppose $d = 0$; we look at $\begin{pmatrix} a & -1 \\ 1 & \end{pmatrix} z = a - z^{-1}$, which is not in $\overline{\mathcal{F}}$ unless $|z| = 1$. We get $z = e^{2\pi i/3}$ or $e^{\pi i/3}$. The other cases are similar. □

For the moment, let's study binary quadratic forms $f = ax^2 + bxy_cy^2$ over $\mathbf{Z}$, up to $\mathrm{GL}_2(\mathbf{Z})$-equivalence. We'll assume the fact that $\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$ and $\begin{pmatrix} & -1 \\ 1 & \end{pmatrix}$ generate $\mathrm{SL}_2(\mathbf{Z})$. We compute:

$$\begin{aligned} \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} f(x,y) &= f\left( \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \right) \\ &= f(x, x + y) \\ &= ax^2 + bx(x + y) + c(x + y)^2 \\ &= (a + b + c)x^2 + (b + 2c)xy + cy^2. \end{aligned}$$

Similarly, if $z$ is a root of the dehomogenization $ax^2 + bx + c$, then $z - 1$ is a root of $\begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix} \cdot f$, and $-1/z$ is a root of $\begin{pmatrix} & -1 \\ 1 & \end{pmatrix} \cdot f$. Thus the action of $\mathrm{SL}_2(\mathbf{Z})$ on binary quadratic forms over $\mathbf{Z}$ induces the standard action on the roots. Let's work with positive definite forms (this is the easy case: on the same level as negative definite). So $a > 0$ and $b^2 - 4ac < 0$. Thus roots $z, \bar{z}$ live in an imaginary quadratic field. Indefinite quadratic forms have real roots, so we're working with real quadratic fields, whose rings of integers have infinite unit groups.

So we're trying to classify positive-definite binary quadratic forms over $\mathbf{Z}$ with $a, c > 0$, up to equivalence. They have roots $\bar{z}$, $z \in \mathfrak{H}$. Given a positive-definite binary quadratic form $f$, find $\gamma \in \mathrm{SL}_2(\mathbf{Z})$ such that the root of $\gamma \cdot f$ is in $\mathcal{F}$. The new form equivalent to $f$ is $ax^2 + bxy + cy^2$, where $\Delta = b^2 - 4ac < 0$. We care about the root $z = \frac{-b + i\sqrt{|\Delta|}}{2a}$. Since $z \in \mathcal{F}$, we have $|b| \leqslant a$. Moreover, $|z| \geqslant 1$ implies $c \geqslant a$. Now $3a^2 + b^2 \leqslant 4ac$, so $a^2 \leqslant \frac{|\Delta|}{3}$, whence $a \leqslant \sqrt{|\Delta|/3}$. How do we count inequivalent positive-definite binary quadratic forms over $\mathbf{Z}$ with discriminant $\Delta$? We need $a, b, c$ with $0 \leqslant |b| \leqslant a \leqslant \sqrt{|\Delta|/3}$. Given fixed $\Delta$, there are only finitely many such $a, b$, and $c$ is determined by $a, b$. We'll proceed to do this with indefinite quadratic forms.

## 3.6 Binary quartic forms

Let $R \subset \mathbf{R}$ be a ring. We want to understand the action of $\mathrm{GL}_2(R)$ on the space $V_{\mathbf{R}}$ of real binary quartic forms. Write such a form as

$$f = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4.$$

Given $f \in V_{\mathbf{R}}$, define

$$\begin{aligned} I &= 12ac - 3bd + c^2 \\ J &= 72ace + 9bcd - 27ad^2 - 27b^2e - 2c^3. \end{aligned}$$

We can think of $I, J$ as functions on the scheme $V_{/\mathbf{Z}}$. Any $\gamma \in \mathrm{GL}(2)$ acts on $V$ by

$$\gamma \cdot f = f\left(\begin{pmatrix} x & y \end{pmatrix} \gamma\right).$$

We have, for $\gamma \in \mathrm{GL}(2)$, the identities:

$$\begin{aligned} I(\gamma \cdot f) &= (\det \gamma)^4 I(f) \\ J(\gamma \cdot f) &= (\det \gamma)^6 J(f). \end{aligned}$$

Thus $I$ and $J$ are $\mathrm{SL}^{\pm}(2)$-invariant functions on $V$. The *height* of $f \in V_{\mathbf{R}}$ is

$$H(f) = \max\{|I|^3, J^2/4\}.$$

Our goal is to count the number of $f \in \mathrm{GL}_2(\mathbf{Z})\backslash V_{\mathbf{R}}$ with $H(f) \leqslant X$. As with binary quadratic forms, we'll have to treat the different possible signatures of $f$ separately. Put, for $R \subset \mathbf{R}$:

$$\begin{aligned} V_R^{(0)} &= \{f \in V_R : f \text{ has four real roots}\} \\ V_R^{(1)} &= \{f \in V_R : f \text{ has two real roots}\} \\ V_R^{(2-)} &= \{f \in V_R : f \text{ is negative definite}\} \\ V_R^{(2+)} &= \{f \in V_R : f \text{ is positive definite}\}. \end{aligned}$$

**Proposition 3.6.1.** *The fundamental domains for $V_{\mathbf{R}}^{(*)}$ with $\mathrm{GL}_2(\mathbf{R})$-action are:*

$$\begin{aligned} L_{\mathbf{R}}^{(0)} &= \left\{x^3y - \frac{xy^3}{3} - \frac{Jy^4}{27} : -2 < J < 2\right\} \\ L_{\mathbf{R}}^{(1)} &= \dots \\ L_{\mathbf{R}}^{(2\pm)} &= \dots \end{aligned}$$

The fundamental domains $L_{\mathbf{R}}^{(1)}$ and $L_{\mathbf{R}}^{(2\pm)}$ have similarly explicit fundamental domains. An all of the $L_{\mathbf{R}}^{(*)}$, the coefficients are bounded. In other words, $V_{\mathbf{R}}/\,\mathrm{GL}_2(\mathbf{R})$ has finite volume. It will be convenient to choose a compact subgroup $G_0 \subset \mathrm{GL}_2(\mathbf{R})$, and consider, for $h \in G_0$, the coset $hL_{\mathbf{R}}^{(*)}$. These cosets will be contained in some compact set which depends only on $G_0$. We care about $\mathrm{GL}_2(\mathbf{Z})\backslash V_{\mathbf{Z}}$. This leads us to study $\mathrm{GL}_2(\mathbf{Z})\backslash \mathrm{GL}_2(\mathbf{R})$. In the previous subsection, we got a pretty good understanding of $\mathrm{SL}_2(\mathbf{Z})\backslash \mathrm{SL}_2(\mathbf{R})/\mathrm{SO}(2)$. We have

$$\mathrm{GL}_2(\mathbf{Z})\backslash \mathrm{GL}_2(\mathbf{R}) = \mathrm{SL}_2(\mathbf{Z})\backslash \mathrm{GL}_2^+(\mathbf{R}) = \mathrm{SL}_2(\mathbf{Z})\backslash NAK\Lambda,$$

in which

$$\begin{aligned} N &= \begin{pmatrix} 1 & \\ * & 1 \end{pmatrix} \\ A &= \left\{ \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} : t > 0 \right\} \\ K &= \mathrm{SO}(2) \\ \Lambda &= \left\{ \begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix} : \lambda > 0 \right\} \end{aligned}$$

**Proposition 3.6.2.** *The multiplication map $N \times A \times K \times \Lambda \to \mathrm{GL}_2(\mathbf{R})^+$ is a homeomorphism.*

*Proof.* This is standard. □

So $\mathrm{GL}_2(\mathbf{Z})\backslash \mathrm{GL}_2(\mathbf{R})$ has the same fundamental domain

$$\mathcal{G} = \left\{ \begin{pmatrix} 1 & \\ u & 1 \end{pmatrix} \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} k \begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix} : u \in [-1/2, 1/2], t \geqslant \sqrt{\frac{\sqrt{3}}{2}} \right\},$$

where we fudge the bounds for $u$ appropriately to be in one or two intervals, depending on $t$. Let $h \in G_0$, our compact subgroup of $\mathrm{GL}_2(\mathbf{R})$. Then $\mathcal{G}hL_{\mathbf{R}}^{(*)}$ is not compact (moreover, it is a multiset – some elements of $V_{\mathbf{R}}$ occur with multiplicities $> 1$).

If $x \in V_{\mathbf{R}}^{(*)}$, how many times does the $\mathrm{GL}_2(\mathbf{Z})$-orbit of $x$ intersect $\mathcal{G}h \cdot L_{\mathbf{R}}^{(*)}$? There exists a unique $x_L \in hL_{\mathbf{R}}^{(*)}$ that is $\mathrm{GL}_2(\mathbf{R})$-equivalent to $x$. If $g \cdot x_L = x$, then $g' x_L \sim_{\mathrm{GL}_2(\mathbf{Z})} x$ if and only if $g' = \gamma g \tilde{g}$ for some $\gamma \in \mathrm{GL}_2(\mathbf{Z})$ and $\tilde{g} \in \mathrm{Stab}(x_L)\,\mathrm{GL}_2(\mathbf{R})$. Thus $g$ and $g'$ represent the same double coset in

$$\mathrm{GL}_2(\mathbf{Z})\backslash \mathrm{GL}_2(\mathbf{R})/\mathrm{Stab}_{\mathrm{GL}_2(\mathbf{R})}(x_L).$$

The number of such cosets is:

$$\frac{\#(g\,\mathrm{Stab}_{\mathrm{GL}_2(\mathbf{R})}(x_L)g^{-1})}{\#(\mathrm{SL}_2(\mathbf{Z}) \cap g\,\mathrm{Stab}_{\mathrm{GL}_2(\mathbf{R})}(x_L)g^{-1})} = \frac{\#\,\mathrm{Stab}_{\mathrm{GL}_2(\mathbf{R})}(x)}{\#\,\mathrm{Stab}_{\mathrm{GL}_2(\mathbf{Z})}(x)}.$$

Both stabilizers contain $\boldsymbol{\mu}_2$. In fact, $\mathrm{Stab}_{\mathrm{GL}_2(\mathbf{Z})}(x) = \{\pm 1\}$ away from a set of measure zero. On the other hand,

$$\#\,\mathrm{Stab}_{\mathrm{GL}_2(\mathbf{R})}(x) = \begin{cases} 8 & * \neq 1 \\ 4 & * = 1 \end{cases},$$

again, away from a set of measure zero.

**Definition 3.6.3.** *$R_X(h\cdot L^{(*)})$ is the multiset of $w \in \mathcal{G}h\cdot L^{(*)}$ such that $H(w) \leqslant X$.*

Let $N(V_{\mathbf{Z}}^{(*)}, X)$ be the number of integral irreducible binary quartic forms with signature of type $*$ and height $\leqslant X$. Let $n_{(*)} = \frac{1}{2}\#\operatorname{Stab}_{\mathrm{GL}_2(\mathbf{R})}(*)$. Then

$$n_{(*)}N(V_{\mathbf{Z}}^{(*)}, X) = \#\{\text{irred. int. points in } R_X(h\cdot L^{(*)}) \text{ weighted by } 1/r\},$$

in which $2r = \#\operatorname{Stab}(*)$. Let $h \in G_0$. Then the number of reducible integral binary quartic forms in $R_X(h\cdot L^{(*)}$ is $O(X^{2/3+\epsilon})$. There are roughly $O(X^{5/6})$ forms with height $\leqslant X$.

For $n \in \mathbf{N}$, let $d(n)$ be the number of divisors of $n$. So if $n = \prod p^{e_p}$, we have $d(n) = \prod(e_p + 1)$.

**Lemma 3.6.4.** $\limsup_{n\to\infty} \frac{\log d(n)}{\log n/\log\log n} = \log 2$.

As a corollary, $d(n) = o(n^\epsilon)$ for all $\epsilon > 0$. We'll count quartics that have a factor $px + qy$. This will tell us $p \mid a$ and $q \mid e$.

## 3.7 Responses to questions

We're interested in the local-global principle for Brauer-Severi varieties. That is, if $k$ is a global field, a twist $X_{/k}$ of $\mathbf{P}^{n-1}_{/k}$ satisfies the local-global principle.

**Theorem 3.7.1** (Hilbert 90). *Let $k$ be a field. Then $\mathrm{H}^1(k, \mathrm{GL}_n) = 1$.*

When $n = 1$, this is the more classical Hilbert 90, a theorem of Emmy Noether.

**Theorem 3.7.2.** *Let $X_{/k}$ be a Brauer-Severi variety over a global field. The following are equivalent:*

1. *$X \simeq \mathbf{P}^{n-1}_k$.*

2. *$X$ is birational to $\mathbf{P}^{n-1}_k$.*

3. *$X(k) \neq \varnothing$.*

*Proof.* Clearly $1 \Rightarrow 3$. We'll also prove the converse. Let $x_0 \in X(k)$. So $(X, x_0)$ is a twist of $(\mathbf{P}^{n-1}, (1:0:\cdots:0))$. These twists are classified by $\mathrm{H}^1(k, \operatorname{Aut}(\mathbf{P}^{n-1}, (1:0:\cdots:0))$. Recall that $\operatorname{Aut}(\mathbf{P}^{n-1}) = \mathrm{PGL}(n)$. We want automorphisms fiximg a point. These correspond to $(\mathbf{G}_{\mathrm{m}} \times \mathrm{GL}(n))/\mathbf{G}_{\mathrm{m}} \simeq \mathbf{G}_{\mathrm{a}}^n \ltimes \mathrm{GL}(n-1)$. So we have a short exact sequence

$$1 \to \mathbf{G}_{\mathrm{a}}^n \to \operatorname{Aut}(\mathbf{P}^n, p) \to \mathrm{GL}(n-1) \to 1.$$

It is well-known that $\mathrm{H}^1(k, \mathbf{G}_{\mathrm{a}}) = 0$. There is a long exact sequence for non-abelian Galois cohomology; it tells us that $\mathrm{H}^1(k, \operatorname{Aut}(\mathbf{P}^n, p)) = 1$. This tells us that the only twist of $(\mathbf{P}^n, p)$ is trivial, hence $X \simeq \mathbf{P}^n$. □

**Theorem 3.7.3.** *For $k$ a global field, the map*

$$\mathrm{H}^2(k, \mathbf{G}_\mathrm{m}) \to \bigoplus_v \mathrm{H}^2(k_v, \mathbf{G}_\mathrm{m})$$

*is an injection.*

This is a fundamental result of class field theory. Now we can prove the local-global principle for Brauer-Severi varieties. We have a short exact sequence

$$1 \to \mathbf{G}_\mathrm{m} \to \mathrm{GL}(n) \to \mathrm{PGL}(n) \to 1.$$

Since $\mathrm{H}^1(k, \mathrm{GL}_n) = 1$, the map $\mathrm{H}^1(k, \mathrm{PGL}_n) \to \mathrm{H}^2(k, \mathbf{G}_\mathrm{m})$ is an injection. Let $X_{/k}$ be a brauer-Severi variety. This corresponds to a unique cohomology class $c \in \mathrm{H}^1(k, \mathrm{PGL}_n) \subset \mathrm{H}^2(k, \mathbf{G}_\mathrm{m})$. We know that $X(k) \neq \varnothing$ if and only if $c \neq 0$. This holds if and only if $c|_v \neq 0$ in $\mathrm{H}^2(k_v, \mathbf{G}_\mathrm{m})$ for all $v$, which is equivalent to $X(\mathbf{A}) \neq \varnothing$. In other words, we have proved that $X(k) \neq \varnothing \Leftrightarrow X(\mathbf{A}) \neq \varnothing$, or equivalently that $X \simeq \mathbf{P}^n_{/k}$ if and only if $X_{k_v} \simeq \mathbf{P}^n_{/k_v}$ for all $v$.

This proof is from Poonen's notes, with file name `Qpoints.pdf`.

The other question asked concerned the Hermite-Minkowski theorem. Let $k$ be a number field, $S$ a finite set of primes of $k$. Let $K/k$ be the maximal abelian $p$-extension of $k$. We will use the fact that $[K : k] < \infty$.

**Theorem 3.7.4** (Dirichlet)**.** *Let $k$ be a number field. Then $\operatorname{rk} \mathcal{O}_k^\times = r + s - 1$, where $r$ is the number of real places of $k$ and $s$ is the number of complex places of $k$. More generally, $\operatorname{rk} \mathcal{O}_{k,S}^\times = \#S - 1$ for $S$ any finite set of places containing the infinite places.*

[Other way around: use Dirichlet's theorem to prove Hermite-Minkowski.]

*Proof.* To prove the finiteness of $K/k$, we'll prove the finiteness of $K(\boldsymbol{\mu}_p)/k(\boldsymbol{\mu}_p)$. So we may as well assume $\boldsymbol{\mu}_p \subset k$. We'll also assume $S$ contains all primes above $p$. Now we can use Kummer theory to classify $\mathbf{Z}/p$-extensions of $k$ as splitting fields of $x^p - \alpha$ for $\alpha \in k^\times/p$. Work locally at some $v \in S$. Then $\alpha = \pi^e \cdot u$, for $\pi$ a uniformizer at $v$ and $u \in \mathcal{O}_{k,v}$ a unit. Roots of $x^p - \alpha$ are conjugates of $\pi^{e/p} u^{1/p}$. The measure of ramification is $v(p) + r \cdot \frac{p-1}{p}$, unless $r \equiv 0 \pmod p$, in which case we take $\alpha = u$. In other words, $k(\sqrt[p]{\alpha})/k$ is ramified at $v$ unless $\alpha$ is (equivalent to) a $v$-unit. So we are interested in $\mathbf{G}_\mathrm{m}(\mathcal{O}_{k,S}) \otimes \mathbf{Z}/p \simeq (\mathbf{Z}/p)^{\#S-1}$, a finite group. □

The local-global principle is false in general. We could prove it for $\mathbf{P}^n$ because $\mathrm{Aut}(\mathbf{P}^{n-1}) = \mathrm{GL}(n)$, and we know the Galois cohomology of $\mathrm{GL}_n$. For a general curve, the automorphism group is much more complicated, so the Galois cohomology may not satisfy a local-global principle.

## 3.8 What we've done

Let $V_\mathbf{R}$ be the space of binary quartic forms over $\mathbf{R}$. The group $G_\mathbf{R} = \mathrm{GL}_2(\mathbf{R})$ acts on $V_\mathbf{R}$. The action of $G_\mathbf{R}$ changes the heights of quartic forms, but the change of height is determined by $\det(g)^2$. So $\mathrm{SL}_2(\mathbf{Z})$ and $\mathrm{GL}_2(\mathbf{Z})$ do not change heights. We had a fundamental domain $\mathcal{F} = NAK\Lambda$. We constructed fundamental domains for $\mathrm{GL}_2(\mathbf{Z})\backslash V_{\mathbf{R}}^{(i)}$.

[…stopped taking notes…]

# References

[BSa] Manjul Bhargava and Arul Shankar. *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*. arXiv: 1006.1002 [math.NT].

[BSb] Manjul Bhargava and Arul Shankar. *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*. arXiv: 1007.0052 [math.NT].

[BSc] Manjul Bhargava and Arul Shankar. *The average number of elements in the 4-Selmer groups of elliptic curves is 7*. arXiv: 1312.7333 [math.NT].

[BSd] Manjul Bhargava and Arul Shankar. *The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1*. arXiv: 1312.7859 [math.NT].

[BSe] Manjul Bhargava and Christopher Skinner. *A positive proportion of elliptic curves over $\mathbb{Q}$ have rank one*. arXiv: 1401.0233 [math.NT].

[BSZ] Manjul Bhargava, Christopher Skinner, and Wei Zhang. *A majority of elliptic curves over $\mathbb{Q}$ satisfy the Birch and Swinnerton-Dyer conjecture*. arXiv: 1407.1826 [math.NT].

[BG06] Enrico Bombieri and Walter Gubler. *Heights in Diophantine geometry*. Vol. 4. New Mathematical Monographs. Cambridge University Press, 2006.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*. Vol. 21. Ergebnisse der Mathematik und ihrer Grenzgebiete (3). Berlin: Springer-Verlag, 1990.

[Bru67] Armand Brumer. “On the units of algebraic number fields”. In: *Mathematika* 14 (1967), pp. 121–124.

[Bru92] Armand Brumer. “The average rank of elliptic curves. I”. In: *Invent. Math.* 109.3 (1992), pp. 445–472.

[Cas62] J. W. S. Cassels. “Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung”. In: *J. Reine Angew. Math.* 211 (1962), pp. 95–112.

[Cre+08] J. E. Cremona et al. “Explicit $n$-descent on elliptic curves. I. Algebra”. In: *J. Reine Angew. Math.* 615 (2008), pp. 121–155.

[Cre+09] J. E. Cremona et al. “Explicit $n$-descent on elliptic curves. II. Geometry”. In: *J. Reine Angew. Math.* 632 (2009), pp. 63–845.

[Cre+14] J. E. Cremona et al. “Explicit $n$-descent on elliptic curves. III. Algorithms”. In: *Math. of Computation* (2014). Published electronically.

[SGA $4\frac{1}{2}$] Pierre Deligne. *Cohomologie étale*. Lecture Notes in Mathematics, Vol. 569. Séminaire de Géométrie Algébrique du Bois-Marie SGA $4\frac{1}{2}$, Avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie, et J. L. Verdier. Springer-Verlag, 1977.

[Del80] Pierre Deligne. “La conjecture de Weil. II”. In: *Inst. Hautes Études Sci. Publ. Math.* 52 (1980), pp. 137–252.

[Fon85] Jean-Marc Fontaine. “Il n’y a pas de variété abélienne sur $\mathbf{Z}$”. In: *Invent. Math.* 81.3 (1985), pp. 515–538.

[GEM14] Gerard van der Geer, Bas Edixhoven, and Ben Moonen. *Abelian varieties*. 2014. URL: http://www.math.ru.nl/personal/bmoonen/research.html (visited on 09/03/2014).

[Har] Michael Harris. *Galois representations, automorphic forms, and the Sato-Tate conjecture*. URL: https://www.imj-prg.fr/~michael.harris/Clay.pdf (visited on 09/09/2014).

[HB04] D. R. Heath-Brown. “The average analytic rank of elliptic curves”. In: 122.3 (2004), pp. 591–623.

[Kle05] Steven Kleiman. “The Picard scheme”. In: *Fundamental algebraic geometry*. Vol. 123. Math. Surveys Monogr. Amer. Math. Soc., 2005, pp. 235–321.

[Lor96] Dino Lorenzini. *An invitation to arithmetic geometry*. Vol. 9. Graduate Studies in Mathematics. American Mathematical Society, 1996.

[Maz77] Barry Mazur. “Modular curves and the Eisenstein ideal”. In: *Inst. Hautes Études Sci. Publ. Math.* 47 (1977), pp. 33–186.

[Maz11] Barry Mazur. “How can we construct abelian Galois extensions of basic number fields?” In: *Bull. Amer. Math. Soc. (N.S.)* 48.2 (2011), pp. 155–209.

[Mor12] Masanori Morishita. *Knots and primes*. Universitext. Springer, 2012.

[Neu99] Jürgen Neukirch. *Algebraic number theory*. Vol. 322. Grundlehren der Mathematischen Wissenschaften. Berlin: Springer-Verlag, 1999.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*. Second. Vol. 323. Grundlehren der Mathematischen Wissenschaften. Springer-Verlag, 2008.

[Och99] Tadashi Ochiai. “$l$-independence of the trace of monodromy”. In: *Math. Ann.* 315.2 (1999), pp. 321–340.

[Rib76] Kenneth Ribet. “A modular construction of unramified $p$-extensions of $\mathbf{Q}(\mu_p)$”. In: *Invent. Math.* 34.3 (1976), pp. 151–162.

[Ser68] Jean-Pierre Serre. *Abelian $l$-adic representations and elliptic curves*. McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute. New York-Amsterdam: W. A. Benjamin, Inc., 1968.

[ST68] Jean-Pierre Serre and John Tate. “Good reduction of abelian varieties”. In: *Ann. of Math. (2)* 88 (1968), pp. 492–517.

[Sil09] Joseph Silverman. *The arithmetic of elliptic curves*. Second. Vol. 106. Graduate Texts in Mathematics. Dordecht: Springer, 2009.

[Sza09] Tamás Szamuely. *Galois groups and fundamental groups*. Vol. 117. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2009.

[You06] Matthew P. Young. “Low-lying zeros of families of elliptic curves”. In: *J. Amer. Math. Soc.* 19.1 (2006), pp. 205–250.