LECTURE NOTES: GARLAT 2026

DEBANJANA KUNDU

There is nothing original in these notes; either in terms of content or presentation. The only virtue of these notes is that I have tried to provide to a beginning graduate student clear statements of some main theorems and motivation to read the more comprehensive books and articles cited.

Motivation

A *Diophantine equation* is an equation given by a polynomial in r-many variables with integer coefficients, i.e.,

$$f(x_1, \dots, x_r) = 0 \text{ where } f(x_1, \dots, x_r) \in \mathbb{Z}[x_1, \dots, x_r].$$

We are often interested in the solutions of such equations and we can ask the following questions:

(1) Does $f(x_1, \dots, x_r)$ have *any* integral (or rational) solutions?
(2) If yes, can we determine *at least one* such solution?
(3) Can we find *all* the solutions and show that there are no more solutions?

In this direction, David Hilbert asked the following question[1]:

> *'Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: to devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.'*

In other words, Hilbert was asking for an *algorithm* to decide whether a given Diophantine equation has integral solutions. This problem has a negative answer; i.e., such a general algorithm cannot exist. This is the result of combined work of Martin Davis, Yuri Matiyasevich, Hilary Putnam, and Julia Robinson over two decades, with Matiyasevich completing the theorem in 1970 [11, 12, 34, 45].

The problem can be extended, and the same question(s) can be asked for many rings (e.g., rings of integers of number fields). Building on the work of Bjorn Poonen [44], Alexandra Shlapentokh reformulated this question to one on elliptic curves [50]. A complete (unconditional) proof of Hilbert's 10th Problem for rings of integers of number fields has been announced by Peter Koymans and Carlo Pagano [31] and Levent Alpöge, Manjul Bhargava, Wei Ho, and Ari Shnidman [1].

Note that Hilbert's question only deals with (1). Sometimes more can be said:

- *Polynomials in one variable:* In this case, we can use the Rational Root Theorem.
- *Linear equations in two (honest!) variables:* Such equations have infinitely many rational solutions. To determine the integral solutions, one can use the Euclid's algorithm.
- *Conics (quadratic equations):* Legendre's criterion says that rational (global) solutions exist on a conic if and only if it has points over $\mathbb{R}$ and over $\mathbb{Q}_p$ for all primes p (*local* solutions).
- *Cubic equations in two variables:* Such equations may have no rational solutions, exactly one rational solution, or infinitely many rational solutions. We will study (special cases of) these equations during these lectures.
- *Higher degree:* Usually[2], if a curve is defined by an equation of degree ≥ 4, it has genus ≥ 2. It was conjectured by Louis Mordell [39] and proved by Gerd Faltings [16] that all curves of genus ≥ 2 have finitely many rational points.

Date: July 9, 2026.

[1] This was the 10th problem in the list of 23 problems posed by Hilbert at the Second ICM in Paris in 1900.

[2] See exercise sheet

1. Lecture 1: Elliptic Curves over $\mathbb{Q}$

1.1. Definition and Examples.

Definition 1.1. An *elliptic curve* E over $\mathbb{Q}$ is a smooth cubic projective (algebraic) curve E of genus 1 defined over $\mathbb{Q}$ with at least one rational point $\mathcal{O} \in \mathsf{E}(\mathbb{Q})$, that is called the origin.

This means that an elliptic curve E in the projective plane is given by a cubic polynomial

$$F(X,Y,Z) = aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2Z + fXYZ + gY^2Z + hXZ^2 + jYZ^2 + kZ^3 = 0,$$

where the coefficients are in $\mathbb{Q}$, and such that at any point $\mathsf{P} \in \mathsf{E}$ the tangent vector

$$\left(\frac{\partial F}{\partial X}(\mathsf{P}), \frac{\partial F}{\partial Y}(\mathsf{P}), \frac{\partial F}{\partial Z}(\mathsf{P})\right) \neq 0.$$

However, when working over $\mathbb{Q}$ (or over any field K which is not of characteristic 2 or 3), we can perform a change of coordinates and rewrite the elliptic curve (in affine coordinates) as

$$\mathsf{E} : y^2 = x^3 + Ax + B$$

where $A, B \in \mathbb{Q}$ satisfying $4A^3 + 27B^2 \neq 0$. This is called the *short Weierstrass equation*. Note that when the Weierstrass equation is written in projective coordinates it has a unique point at infinity $[0:1:0]$; when rewriting it in affine coordinates we denote this point by $\mathcal{O}$ and call this the origin (or the point at infinity). Sometimes we might use the more *general Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \text{ with } a_i \in \mathbb{Q}. \tag{1}$$

1.2. Minimal Model.

Let us start with an elliptic curve over $\mathbb{Q}$ in its short Weierstrass form.

Definition 1.2. Define the *discriminant* Δ_{E} and the *j-invariant* $j(\mathsf{E})$ of the elliptic curve E as

$$\Delta_{\mathsf{E}} = -16(4A^3 + 27B^2) \text{ and } j(\mathsf{E}) = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

More generally, if we work with the long Weierstrass equation then

$$\Delta_{\mathsf{E}} = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_8 \quad \text{where} \quad \begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

Definition 1.3. Two elliptic curves $(\mathsf{E}, \mathcal{O})$ and $(\mathsf{E}', \mathcal{O}')$ are *isomorphic* over $\mathbb{Q}$ if there is an invertible change of variables $\psi : \mathsf{E} \to \mathsf{E}'$ defined via rational functions with rational coefficients such that $\mathcal{O} \mapsto \mathcal{O}'$.

Two elliptic curves which are isomorphic of $\mathbb{Q}$ (and hence $\mathbb{C}$) have the same j-invariant; see [52, Proposition III.1.4(b)]. However, the converse is not true. Two elliptic curves with the same j-invariant need not be isomorphic over $\mathbb{Q}$ (but they will be isomorphic over $\mathbb{C}$).

Definition 1.4. Now suppose that S is the set of all elliptic curves E' that are isomorphic to E over $\mathbb{Q}$. Consider the set

$$\mathfrak{S} \coloneqq \{|\Delta_{\mathsf{E}'}| \ : \ \mathsf{E}' \in S\}.$$

The *minimal discriminant* of E is the integer $\Delta_{\mathsf{E}'}$ that attains the minimum of $\mathfrak{S}$. We call E' the *minimal model*.

Example 1.5. Consider the elliptic curve $\mathsf{E} : y^2 = x^3 + 1$. This is 36.a4 in LMFDB. We can calculate the discriminant $\Delta_{\mathsf{E}} = -432$. Now, we consider the isomorphic curve $\mathsf{E}' : Y^2 = X^3 + 5^6$, Indeed, this is an isomorphism where the map $\mathsf{E} \to \mathsf{E}'$ is given by $(x, y) \mapsto (25x, 125y) = (X, Y)$. Notice that $|\Delta_{\mathsf{E}'}| > |\Delta_{\mathsf{E}}|$. So, $\Delta_{\mathsf{E}'}$ cannot be the minimal model.

Example 1.6. Consider the elliptic curve $\mathsf{E} : y^2 + y = x^3 - x^2 - 10x - 20$; this is 11.a2 in LMFDB. We calculate $\Delta_{\mathsf{E}} = -(11)^5$. We can perform a change of variables to obtain a model in the short Weierstrass form $\mathsf{E}' : y^2 = x^3 - 13392x - 1080432$ with discriminant $\Delta_{\mathsf{E}'} = -1 \cdot 2^{12} \cdot 3^{12} \cdot 11^5$. *Thus, the elliptic curve presented in the short Weierstrass model need not be minimal.*

Remark 1.7. Another definition is the following: a Weierstrass equation for $\mathsf{E}/\mathbb{Q}$ is said to be *minimal* if it is minimal at v for all places v of $\mathbb{Q}$. (This is also true more generally for number fields). Let K be a local field, complete with respect to a discrete valuation v; in our case $K = \mathbb{Q}_p$. Let E/K be an elliptic curve defined over K given by the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \text{ with } a_i \in K. \tag{2}$$

By a suitable change of variables, we may assume that $v(a_i) > 0$, i.e., $a_i \in \mathcal{O}_K$ where $\mathcal{O}_K$ is the ring of integers of K. Define the set

$$\mathcal{S} = \{v(\Delta) \ : \ \Delta \text{ is the discriminant of a Weierstrass equation for } \mathsf{E} \text{ and } v(\Delta) \geq 0\}.$$

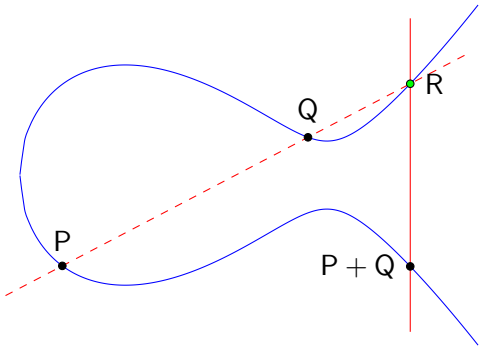
Since v is a discrete valuation, the set S is a set of non-negative integers, therefore it has a minimum value $m \in S$. If the equation is not minimal, then there is a coordinate change giving a new equation with discriminant $\Delta = u^{-12}\Delta$, so so the equations only differ by a 12-th power of a non-zero number in K. Thus $v(\Delta)$ can be changed only by multiples of 12, so we conclude that if $a_i \in \mathcal{O}_K$ and $v(\Delta) < 12$ then the equation is minimal. Note that this is *not* an if and only if condition. There is an algorithm of Tate which determines whether the model is minimal.

We will return to this topic again in Lecture 3.

1.3. **Group Law.** As explained in the 'Motivation', we want to find the rational solutions of $\mathsf{E}/\mathbb{Q}$. Let us record the notation for the rational points on E called the *Mordell–Weil group* of E:

$$\mathsf{E}(\mathbb{Q}) \coloneqq \{(x, y) \in \mathsf{E} \ : \ x, y \in \mathbb{Q}\} \cup \{\mathcal{O}\}.$$

1.3.1. *Adding Points.* If P and Q are two points on the curve, then we can uniquely describe a third point $\mathsf{P} + \mathsf{Q}$ in the following way.

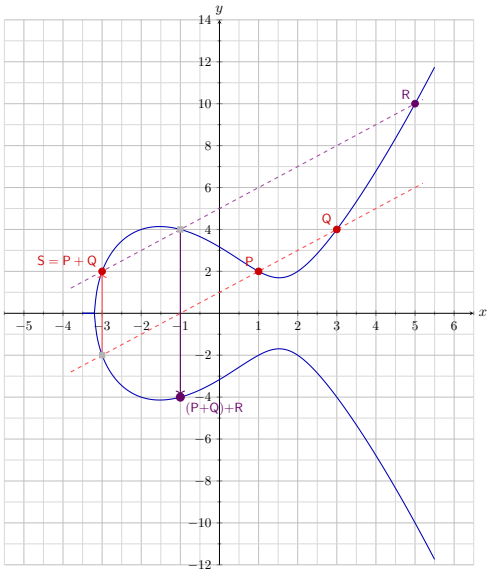


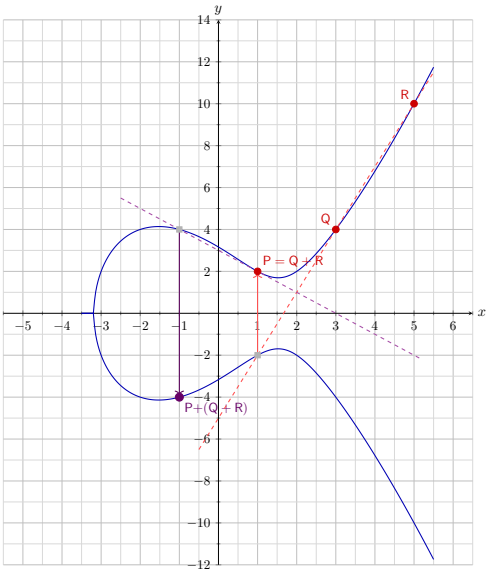
First, draw the line that intersects P and Q. This intersects the cubic at a third point, say R. Then define

$$\mathsf{P} + \mathsf{Q} = -\mathsf{R}$$

where by $-\mathsf{R}$, we mean the point opposite R.

In fact, $(\mathsf{E}, +)$ forms an abelian group[3] (when points of E are considered over any field, not just $\mathbb{Q}$) where $\mathcal{O}$ is the zero element.





Example 1.8. Consider the elliptic curve

$$\mathsf{E} : y^2 = x^3 - 7x + 10.$$

This is the curve 664.a1 in LMFDB. We can check that $\mathsf{P} = (1, 2)$ and $\mathsf{Q} = (3, 4)$ are rational (in fact, integral) points on the elliptic curve. First, we calculate the slope of the line joining P and Q. This is

$$m = \frac{4-2}{3-1} = 1.$$

The equation of the line $\overline{\mathsf{PQ}}$ is $y = x + 1$. To find the third point of intersection of $\overline{\mathsf{PQ}}$ and E, solve

$$y^2 = (x+1)^2 = x^3 - 7x + 10.$$

We factorize the polynomial $x^3 - x^2 - 9x + 9 = (x-1)(x-3)(x+3)$. From this we calculate

$$-\mathsf{R} = (-3, -3+1) = (-3, -2) \text{ and } \mathsf{P} + \mathsf{Q} = \mathsf{R} = (-3, 2).$$

1.3.2. *Doubling the Point.* If $\mathsf{P} = \mathsf{Q}$, then we construct the tangent line at P and let it intersect with the cubic. The rest of the procedure remains the same.

Example 1.9. We continue with our example from before. Writing $\mathsf{E} = y^2 = f(x)$, to calculate $2\mathsf{P}$, we find the slope of the tangent line by implicit differentiation

$$m = \frac{dy}{dx} = \frac{f'(x)}{2y} = \frac{3x^2 - 7}{2y}.$$

At $\mathsf{P} = (1, 2)$, the slope is $m = -1$. The equation of the line is $y = -x + 3$ To find the x-coordinate of the third point of intersection, we solve

$$y^2 = (-x+3)^2 = x^3 - 7x + 10.$$

Therefore the $x(-\mathsf{R}) = -1$ and $y(-\mathsf{R}) = 4$. Thus, $2\mathsf{P} = (-1, -4)$.

[3]The associative property is tedious to prove [52, Proposition III.2.2(e)]. The fact that this associative property is non-trivial might become clear from a sample picture.

Exercise 1.10. Given an elliptic curve $\mathsf{E} : y^2 = x^3 + Ax + B$ and a point $\mathsf{P} = (x_0, y_0)$, find a general formula for $2\mathsf{P}$.

Exercise 1.11. Given an elliptic curve $\mathsf{E} : y^2 = x^3 + Ax + B$ and points $\mathsf{P} = (x, y)$ satisfying $3\mathsf{P} = \mathcal{O}$, find a polynomial in x with roots $x(\mathsf{P})$.

Exercise 1.12. Consider the elliptic curve $\mathsf{E} : y^2 = x^3 + 1$. This is 36.a4 in LMFDB. Starting with $\mathsf{P} = (2, 3)$, find $2\mathsf{P}, 3\mathsf{P}, 4\mathsf{P}, 5\mathsf{P}, 6\mathsf{P}$.

1.4. **Structure of the Mordell–Weil Group.** The next step in the study of the structure of $\mathsf{E}(\mathbb{Q})$ is the following theorem which was proved by Louis Mordell [39] in 1922. The assertion was later shown to be true for all abelian varieties over all number fields by André Weil [60] in 1928.

Theorem 1.13 (Mordell–Weil)**.** The group of rational points $\mathsf{E}(\mathbb{Q})$ is a finitely generated abelian group. In other words,

$$\mathsf{E}(\mathbb{Q}) \simeq \mathbb{Z}^{r_\mathsf{E}} \oplus \mathsf{E}(\mathbb{Q})_{\text{tors}}.$$

The group $\mathsf{E}(\mathbb{Q})$ is called the *Mordell–Weil group*. The integer r_E is called the *(algebraic) rank* of the elliptic curve and $\mathsf{E}(\mathbb{Q})_{\text{tors}}$ is the torsion part (and is always finite).

We emphasize that the decomposition of $\mathsf{E}(\mathbb{Q})$ into the direct sum of two abelian groups (namely, the free part and the torsion part) is *not* canonical. Consider the subset

$$\mathcal{S} = \{\mathsf{P} \in \mathsf{E}(\mathbb{Q}) \ : \ \mathsf{P} \text{ is of infinite order}\} \cup \{\mathcal{O}\}.$$

Note that this is *not* a subgroup of $\mathsf{E}(\mathbb{Q})$. Indeed, if P_0 is a point of infinite order and T is a torsion point, then $\mathsf{P}_0 + \mathsf{T} \in \mathcal{S}$. But $(\mathsf{P}_0 + \mathsf{T}) - \mathsf{P}_0 = \mathsf{T} \notin \mathcal{S}$. This shows that in general, it is not possible to choose the subgroup of $\mathsf{E}(\mathbb{Q})$ isomorphic to $\mathbb{Z}^{r_\mathsf{E}}$ in a unique way.

Example 1.14. We return to the curve $\mathsf{E} : y^2 = x^3 - 7x + 10$. It can be proved that the generators of $\mathsf{E}(\mathbb{Q})$ are

$$\mathsf{P} = (5, -10) \text{ and } \mathsf{Q} = (-2, 4).$$

We can check (for example) that the point $(3, 4) = 2\mathsf{P} + \mathsf{Q}$. Or that $(2, -2) = 4\mathsf{P} + 3\mathsf{Q}$.

1.4.1. *Proof of the Mordell–Weil Theorem.* We mention the fundamental ingredients of the proof. We do not give a proof but work through the key steps via an explicit example in the worksheet. For a rigorous proof, we refer the reader to [52, Chapter VIII].

- *Weak Mordell–Weil Theorem:* This statement asserts that $\mathsf{E}(\mathbb{Q})/m\mathsf{E}(\mathbb{Q})$ is finite for any positive integer $m \geq 2$.
- *Height Function:* Given an elliptic curve $\mathsf{E}/\mathbb{Q}$, there is a (canonical) height function

  $$\hat{h} : \mathsf{E}(\mathbb{Q}) \longrightarrow \mathbb{R}_{\geq 0}$$

  satisfying the following properties
  - $\hat{h}(\mathsf{P}) \geq 0$ for all $\mathsf{P} \in \mathsf{E}(\mathbb{Q})$.
  - there exists a constant c_0, such that

    $$\left| \frac{1}{2} h(\mathsf{P}) - \hat{h}(\mathsf{P}) \right| \leq c_0 \text{ for all } \mathsf{P}.$$

    We define $h(\mathsf{P})$ as follows: suppose that $x(\mathsf{P}) = \frac{r}{s}$ then $h(\mathsf{P}) = \log(\max\{|r|, |s|\})$.
  - given a constant c, there exist only finitely many points $\mathsf{P} \in \mathsf{E}(\mathbb{Q})$ with $\hat{h} \leq c$.
  - $\hat{h}(m\mathsf{P}) = m^2 \hat{h}(\mathsf{P})$ for all integers m and all P.
  - [parallelogram law] $\hat{h}(\mathsf{P} + \mathsf{Q}) + \hat{h}(\mathsf{P} - \mathsf{Q}) = 2\hat{h}(\mathsf{P}) + 2\hat{h}(\mathsf{Q})$ for all P, Q.
  - if $\mathsf{P} \in \mathsf{E}(\mathbb{Q})_{\text{tors}}$ then $\hat{h}(\mathsf{P}) = 0$.

  For a proof, we refer the reader to [59, Theorem 8.18].

- *Descent Theorem:* This step establishes that any finite abelian group G with height function $\hat{h}$ such that G/mG is finite for *some* $m \geq 2$, is in fact finitely generated.

A natural question to ask is what more can we say about the rank and the torsion part of $\mathsf{E}(\mathbb{Q})$. It is in general an open problem whether there is an absolute bound on the rank of all elliptic curves over $\mathbb{Q}$ [43, Section 3]. In fact, there is little consensus among the experts if the rank of an elliptic curve should be expected to be bounded uniformly. Finding elliptic curves of large rank is a difficult problem. In 2024, Noam Elkies and Zev Klagsbrun discovered a curve with a rank of at least 29 (under the Generalized Riemann Hypothesis, the rank is exactly 29); see announcement here. In addition, there is an infinite family of elliptic curves over $\mathbb{Q}$ each of rank at least 19.

Given an elliptic curve E in the short Weierstrass form, we can define another height function $H(\mathsf{E}) = \max\{4|A|^3, 27B^2\}$. Using this, we can 'order' elliptic curves and obtain a reasonable notion of 'average rank' as follows

$$\lim_{X\to\infty} \frac{\sum_{H(\mathsf{E})<X} r_{\mathsf{E}}}{\sum_{H(\mathsf{E})<X} 1},$$

but it is not known whether this limit exists. Much progress has been made towards the task of finding upper bounds for the average rank. The best result known in this direction is by Manjul Bhargava and Arul Shankar [6] where they have shown unconditionally that the average rank is bounded above by $7/6$.

1.4.2. *Mazur's Torsion Theorem.* We have concrete understanding of the torsion structure of the Mordell–Weil group over $\mathbb{Q}$. In this direction, we have the following result due to Barry Mazur [36].

Theorem 1.15 (Mazur)**.** Let $\mathsf{E}/\mathbb{Q}$ be an elliptic curve. Then $\mathsf{E}(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the following groups

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} \qquad &\text{with} \quad 1 \leq n \leq 10 \text{ or } n = 12, \text{or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} \quad &\text{with} \quad 1 \leq m \leq 4. \end{aligned}$$

Techniques employed by Mazur were generalized by Sheldon Kamienny [27] and Kamienny–Mazur [28], who obtained uniform boundedness for quadratic fields and number fields of degree at most 8, respectively. Finally, Loïc Merel [38] proved the uniform bounded conjecture for elliptic curves over any number field, which is the assertion that the torsion part of an elliptic curve is bounded (only) in terms of the degree of the number field.

One way Mazur's theorem is extremely useful is that if we can calculate the order of a rational point $\mathsf{P} \in \mathsf{E}(\mathbb{Q})$ to be more than 12, then it is automatically a point of infinite order.

1.4.3. *Nagell-Lutz.* In this section, we discuss a simple algorithm to determine $\mathsf{E}(\mathbb{Q})_{\text{tors}}$ discovered independently by Trygve Nagell [41] and Élisabeth Lutz [33].

Theorem 1.16 (Nagell–Lutz)**.** Let $\mathsf{E} : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{Q}$ such that $A, B \in \mathbb{Z}$. Then every $\mathsf{P} \in \mathsf{E}(\mathbb{Q}) \setminus \{\mathcal{O}\}$ satisfies the following conditions:

(1) $x(\mathsf{P})$ and $y(\mathsf{P})$ are both integers.
(2) If P has order ≥ 3, then $y(\mathsf{P})^2 \mid (4A^3 + 27B^2)$.
(3) If P has order 2, then $y(\mathsf{P}) = 0$.

Example 1.17. Let $\mathsf{E} : y^2 = x^3 - 2 = f(x)$. This is the elliptic curve 1728.o3 in LMFDB. Note that $f(x) = 0$ has no rational roots, so there is no rational point of order 2. We check that

$$4A^3 + 27B^2 = 27 \cdot 4 = 2^2 \cdot 3^3.$$

If we require that $y(\mathsf{P})^2 \mid (4A^3 + 27B^2)$, then

$$y(\mathsf{P}) \in \{\pm 1, \pm 2, \pm 3, \pm 6\} \text{ and } x(\mathsf{P})^3 = y(\mathsf{P})^2 + 2 \in \{3, 6, 11, 38\}.$$

There does not exist any integer $x(\mathsf{P})$ such that the cube is 3, 6, 11, or 38. So the torsion part of $\mathsf{E}(\mathbb{Q})$ is trivial.

1.5. **Integral Points on the Elliptic Curve.** We may ask about the size and structure of $\mathsf{E}(\mathbb{Z})$.

Exercise 1.18. Consider the elliptic curve

$$\mathsf{E} : y^2 = x^3 - 7x + 10,$$

as before. Starting with the point $\mathsf{P} = (1, 2)$, show that $\mathsf{E}(\mathbb{Z})$ is *not* a group.

Using the theory of *Diophantine approximation*, Carl Siegel proved the following theorem in 1929; see for example [52, Section IX.3].

Theorem 1.19. Let $\mathsf{E}/\mathbb{Q}$ be an elliptic curve given by $\mathsf{E} : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$, then $E(\mathbb{Z})$ is a finite set.

However, the proof is not effective, i.e., it provides no bound on $\#\mathsf{E}(\mathbb{Z})$. An alternative effective proof was found by Alan Baker in 1990 [52, Section IX.5].

Example 1.20. Consider the curve $\mathsf{E} : y^2 = x^3 + 7$. This is the curve 21168.ce2 in LMFDB. If we want to find $\mathsf{E}(\mathbb{Z})$, we can make the simple observation that $2 \nmid x$. This is because if x were even, then $y^2 = 8k + 7 \equiv 3 \pmod 4$ which cannot happen. Now we can rewrite

$$y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4).$$

Since x is odd,

$$x^2 - 2x + 4 \equiv x(x - 2) \equiv 3 \pmod 4.$$

Hence there is a prime $p \equiv 3 \pmod 4$ which divides $x^2 - 2x + 4$ and hence $y^2 + 1$. In other words,

$$y^2 + 1 \equiv 0 \pmod p.$$

We show that this is not possible. Observe that

$$y^2 \equiv (y^2)^{\frac{p-1}{2}} = y^{p-1} \equiv -1 \pmod p.$$

By Fermat's Little Theorem, $y^{p-1} \equiv 1 \pmod p$ since $\gcd(p, y) = 1$. This forces

$$2 \equiv 0 \pmod p,$$

which is a contradiction since p is an odd prime. *This example is not particularly interesting because* $\mathsf{E}(\mathbb{Q})$ *is trivial, as well.*

Example 1.21. Let $\mathsf{E} : y^2 = x^3 - 2$. This is the elliptic curve 1728.o3 in LMFDB. For this example we know from Example 1.17 that $\mathsf{E}(\mathbb{Q})_{\text{tors}}$ is trivial. *But for this example* $\mathsf{E}(\mathbb{Q}) \simeq \mathbb{Z}$*, so it is interesting to calculate* $\mathsf{E}(\mathbb{Z})$. Using reduction modulo 4, we can check that x, y must both be odd and in fact $x \equiv 3 \pmod 4$.

Consider the factorization in $\mathcal{R} = \mathbb{Z}[\sqrt{-2}]$, which we remind the reader is a PID,

$$(y + \sqrt{-2})(y - \sqrt{-2}) = x^3.$$

We claim that

$$y + \sqrt{-2} = \zeta^3 \text{ and } y - \sqrt{-2} = \overline{\zeta}^3 \text{ for some } \zeta \in \mathcal{R}.$$

To see this,

- Check that $\sqrt{-2}$ is prime in $\mathcal{R}$. Indeed, if $\sqrt{-2} \mid (a + b\sqrt{-2})(c + d\sqrt{-2})$ then taking norms, $2 \mid (a^2 + 2b^2)(c^2 + 2d^2)$ so either a or c is even.

- Suppose that $\gcd(y+\sqrt{-2}, y-\sqrt{-2}) > 1$. If d is a prime such that $d \mid (y+\sqrt{-2})$ and $d \mid (y-\sqrt{-2})$, then $d \mid 2\sqrt{-2} = -(\sqrt{-2})^3$. By the above calculation, we know $d = \sqrt{-2}$ (up to associates since $\mathcal{R}$ is a UFD).

  We can therefore write $y = (r + s\sqrt{-2})\sqrt{-2}$. This means $r = 0$ which forces $y = -2s$; but we know that y cannot be even. So, $y+\sqrt{-2}$ and $y-\sqrt{-2}$ are coprime to each other. This proves the claim.

Now, write $\zeta = R + S\sqrt{-2}$. Then

$$(y+\sqrt{-2}) - (y-\sqrt{-2}) = 2\sqrt{-2} = \zeta^3 - \overline{\zeta}^3 = (\zeta - \overline{\zeta})(\zeta^2 - \zeta\overline{\zeta} + \overline{\zeta}^2) = 2\sqrt{-2}S(3R^2 - 2S^2).$$

The only integral solutions for (R, S) are $(\pm 1, 1)$. We can then check $(x, y) = (3, \pm 5)$.

1.6. **Selmer Groups.** *In the worksheet, we explicitly compute the 2-Selmer group for a specific elliptic curve. This section gives the motivation for studying such objects, but uses the language of Galois cohomology for providing definitions.*

1.6.1. *Hasse Principle.* Helmut Hasse introduced a local-global principle which essentially says that that certain types of equations have a rational solution if and only if they have a solution in the real numbers and in the p-adic numbers for each prime p. In other words, one can find an integer solution of an equation by using the Chinese remainder theorem to piece together solutions modulo powers of each different prime number. For example, this was seen to be true for conics.

Given a polynomial equation with rational coefficients, it is straightforward to notice that if it has a rational solution, then it also has a real solution and a p-adic solution for each prime p. This is to say that a global solution yields always yields local solutions at each prime. But, the converse is not always true. An important example was first shown by Ernst Selmer in 1951 [48]. He showed that the cubic curve

$$C : 3x^3 + 4y^3 = 5$$

has no local obstruction (i.e., it has a non-zero solution over $\mathbb{R}$ and every $\mathbb{Q}_p$), but has no rational points. The Hasse principle asks when can the reverse be done, or what is the obstruction.

1.6.2. *Definition via Galois Cohomology.* Let $\mathsf{E}/\mathbb{Q}$ be an elliptic curve and consider the abelian group $\mathsf{E}(\overline{\mathbb{Q}})$ of all points on the elliptic curve, where $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$. Then $\mathsf{E}(\overline{\mathbb{Q}})$ is a module over $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and we may consider the Galois cohomology groups $H^i(\mathbb{Q}, \mathsf{E}(\overline{\mathbb{Q}}))$. For any positive integer n consider we have the multiplication by n-map (a surjective homomorphism of abelian groups)

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

So we have an exact sequence

$$0 \longrightarrow \mathsf{E}(\overline{\mathbb{Q}})[n] \longrightarrow \mathsf{E}(\overline{\mathbb{Q}}) \xrightarrow{[n]} \mathsf{E}(\overline{\mathbb{Q}}) \longrightarrow 0.$$

Henceforth, we write E *in place of* $\mathsf{E}(\overline{\mathbb{Q}})$ *and* $\mathsf{E}[n]$ *instead of* $\mathsf{E}(\overline{\mathbb{Q}})[n]$. The (beginning part of) associated long exact sequence of Galois cohomology is

$$0 \longrightarrow \mathsf{E}(\mathbb{Q})[n] \longrightarrow \mathsf{E}(\mathbb{Q}) \xrightarrow{[n]} \mathsf{E}(\mathbb{Q}) \longrightarrow H^1(\mathbb{Q}, \mathsf{E}[n]) \longrightarrow H^1(\mathbb{Q}, \mathsf{E}) \xrightarrow{[n]} H^1(\mathbb{Q}, \mathsf{E}) \to \cdots.$$

which can be re-written as

$$0 \longrightarrow \mathsf{E}(\mathbb{Q})/n\mathsf{E}(\mathbb{Q}) \longrightarrow H^1(\mathbb{Q}, \mathsf{E}[n]) \longrightarrow H^1(\mathbb{Q}, \mathsf{E})[n] \longrightarrow 0.$$

This short exact sequence is called the *Kummer sequence* associated to the elliptic curve. If v is either a rational prime or the real archimedean place (in which case $\mathbb{Q}_v = \mathbb{R}$), we can repeat the steps above and obtain the *local Kummer sequence*

$$0 \longrightarrow \mathsf{E}(\mathbb{Q}_v)/n\mathsf{E}(\mathbb{Q}_v) \longrightarrow H^1(\mathbb{Q}_v, \mathsf{E}[n]) \longrightarrow H^1(\mathbb{Q}_v, \mathsf{E})[n] \longrightarrow 0.$$

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

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathsf{E}(\mathbb{Q})/n\mathsf{E}(\mathbb{Q}) & \longrightarrow & H^1(\mathbb{Q},\mathsf{E}[n]) & \longrightarrow & H^1(\mathbb{Q},\mathsf{E})[n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & \overset{g}{\searrow} & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & \prod_v \mathsf{E}(\mathbb{Q}_v)/n\mathsf{E}(\mathbb{Q}_v) & \longrightarrow & \prod_v H^1(\mathbb{Q}_v,\mathsf{E}[n]) & \longrightarrow & \prod_v H^1(\mathbb{Q}_v,\mathsf{E})[n] & \longrightarrow & 0. \end{array}$$

The *n-Selmer group* of an elliptic curve $\mathsf{E}/\mathbb{Q}$ is

$$\mathrm{Sel}^{(n)}(\mathsf{E}/\mathbb{Q}) = \ker(g) = \ker\left(H^1(\mathbb{Q},\mathsf{E}[n]) \longrightarrow \prod_v H^1(\mathbb{Q}_v,\mathsf{E})[n]\right).$$

The *Shafarevich-Tate group* of an elliptic curve $\mathsf{E}/\mathbb{Q}$ is

$$Ш(\mathsf{E}/\mathbb{Q}) = \ker\left(H^1(\mathbb{Q},\mathsf{E}) \longrightarrow \prod_v H^1(\mathbb{Q}_v,\mathsf{E})\right).$$

In particular,

$$Ш(\mathsf{E}/\mathbb{Q})[n] = \ker(h).$$

From the commutative diagram we obtain the *n-descent sequence*

$$0 \longrightarrow \mathsf{E}(\mathbb{Q})/n\mathsf{E}(\mathbb{Q}) \longrightarrow \mathrm{Sel}^{(n)}(\mathsf{E}/\mathbb{Q}) \longrightarrow Ш(\mathsf{E}/\mathbb{Q})[n] \longrightarrow 0.$$

The key step in the proof of the (weak) Mordell–Weil theorem involves showing that $\mathrm{Sel}^{(n)}(\mathsf{E}/\mathbb{Q})$ is finite for all n. This implies that $\mathsf{E}(\mathbb{Q})/n\mathsf{E}(\mathbb{Q})$ and $Ш(\mathsf{E}/\mathbb{Q})[n]$ are also finite.

A big open question in the theory of elliptic curves is the following: let $\mathsf{E}/\mathbb{Q}$ be an elliptic curve. Then the Shafarevich–Tate group $Ш(\mathsf{E}/\mathbb{Q})$ is finite. *We will mention some progress towards this conjecture in Lecture 4.*

2. Lecture 2: Elliptic Curves over $\mathbb{C}$

2.1. **Lattice.**

Definition 2.1. Let $\omega_1 = u_1 + v_1 i$ and $\omega_2 = u_2 + v_2 i$ be two non-zero complex numbers such that (u_1, v_1) and (u_2, v_2) are linearly independent in $\mathbb{R}^2$. The set

$$\Lambda = \{m\omega_1 + n\omega_2 \ : \ m, n \in \mathbb{Z}\}$$

is a lattice. Moreover, every lattice is given in this way.

As a matter of convention, we require that ω_1/ω_2 lies in $\mathbb{H} = \{a + bi \in \mathbb{C} \ : \ b > 0\}$. We use the notation $\Lambda = [\omega_1, \omega_2]$ to mean that the lattice is generated by ω_1, ω_2.

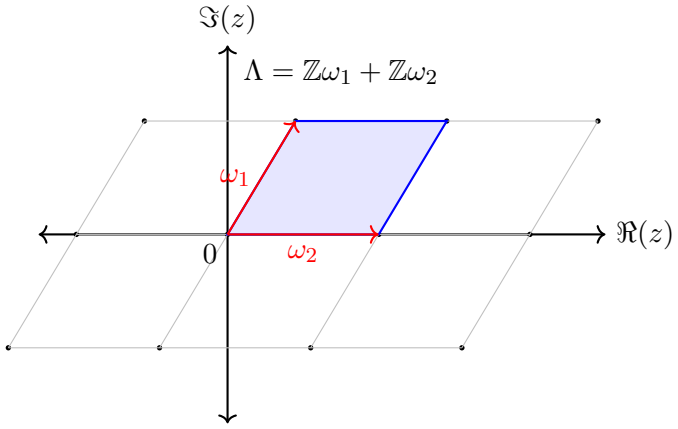
Exercise 2.2. Show that $\mathbb{Z}[i]$ forms a lattice but $\mathbb{Z}[\sqrt{2}]$ does not.

Given a lattice $\Lambda = [\omega_1, \omega_2]$, we can define a quotient group $\mathbb{C}/\Lambda$. The equivalence relation defining $\mathbb{C}/\Lambda$ is the one that says z_1, z_2 are equivalent if $z_1 - z_2 \in \Lambda$.

The *fundamental domain* for $\mathbb{C}/\Lambda$ is the parallelogram

$$\mathcal{F} = \{\lambda\omega_1 + \mu\omega_2 \ : \ 0 \leq \lambda, \mu < 1\}.$$

The elements of $\mathcal{F}$ form a complete set of representatives for $\mathbb{C}/\Lambda$. Further note that $\mathbb{C}/\Lambda$ is a torus since the sides of the fundamental parallelogram are identified with the opposite side modulo Λ.



Exercise 2.3. Consider the lattice $\Lambda = [\sqrt{-3}, 1]$. Draw the fundamental parallelogram for $\mathbb{C}/\Lambda$.

Exercise 2.4. Let $\Lambda = [\omega_1, \omega_2]$ be a lattice. Show that $\Lambda = [\omega_1', \omega_2']$ if and only if there exists a matrix $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$\gamma \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix} = \begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix}.$$

Definition 2.5. Given two lattices Λ and Λ', any map between quotients $\phi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ are given by complex numbers $\alpha \in \mathbb{C}$ such that $\alpha\Lambda \subseteq \Lambda'$ and the map $\phi = \phi_\alpha$ sends z to $\alpha z \pmod{\Lambda'}$. Two lattices Λ and Λ' are called *homothetic* if $\Lambda = \alpha\Lambda'$ for some $\alpha \in \mathbb{C} \setminus \{0\}$.

Exercise 2.6. Homothety is an equivalence relation between lattices in $\mathbb{C}$.

2.2. **Functions on Lattices.**

2.2.1. *Elliptic Functions.* We will be interested in special kinds of elliptic functions, but first we introduce the general notion.

Definition 2.7. A meromorphic function[4] $f(z)$ is called an *elliptic function* if there are two complex numbers ω_1, ω_2 which are linearly independent and for all $z \in \mathbb{C}$,

$$f(z + \omega_1) = f(z) \text{ and } f(z + \omega_2) = f(z).$$

Such functions have two periods, and are therefore called *doubly periodic functions*. The lattice $\Lambda = [\omega_1, \omega_2]$ is called the *period lattice*. The fact that an elliptic function is periodic with respect to Λ means that it can also be viewed as a function on $\mathbb{C}/\Lambda$.

We now mention some useful facts about elliptic functions [59, Theorem 9.1]

- A holomorphic elliptic function is constant.
- Every elliptic function has finitely many poles in $\mathbb{C}/\Lambda$ and the sum of its residues is zero.
- A non-constant elliptic function takes on every value the same number of times in $\mathbb{C}/\Lambda$ counted with multiplicity.

2.2.2. *Eisenstein Series of a Lattice.*

Definition 2.8. Let Λ be a lattice and fix an integer $k > 2$. The *weight-k Eisenstein series* for Λ is the sum

$$G_k(\Lambda) = \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^k}.$$

[4] A meromorphic function $f(z)$ is a complex valued function of the form $f(z) = g(z)/h(z)$ where $g(z), h(z)$ are entire and $h(z) \neq 0$.

We note that the sum converges absolutely for all $k > 2$; see [52, Theorem VI.3.1(a)].

Exercise 2.9. If k is odd, then $G_k(\Lambda) = 0$ for any lattice Λ.

The above exercise implies that the only interesting Eisenstein series are those of even weight.

Exercise 2.10. Suppose that $\Lambda = [\tau, 1]$ where $\tau \in \mathbb{H}$. Writing $G_k(\tau)$ to mean $G_k(\Lambda)$, show that

$$G_k(\tau + 1) = G_k(\tau) \text{ and } G_k(-1/\tau) = \tau^k G_k(\tau).$$

2.2.3. *Weierstrass $\wp$-Function.* We now give an example of a non-trivial elliptic function.

Definition 2.11. The Weierstrass $\wp$-function of a lattice Λ is defined by

$$\wp(z) \coloneqq \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Its derivative is given by

$$\wp'(z) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3}.$$

The $\wp$-function is a meromorphic function on $\mathbb{C}$ with double poles at each lattice point $\omega \in \Lambda$. Moreover, it is holomorphic[5] at each $z_0 \notin \Lambda$. On the other hand, the derivative $\wp'$ is a meromorphic function on $\mathbb{C}$ with triple poles at each lattice point $\omega \in \Lambda$.

Exercise 2.12. Show that $\wp(z) = \wp(-z)$; i.e., the Weierstrass $\wp$-function is an even function. Further show that the derivative is an odd function.

Exercise 2.13. Show that the derivative $\wp'(z)$ is an elliptic function of order 3 for Λ.

Given a lattice $\Lambda = [\omega_1, \omega_2]$, every fundamental region of Λ contains exactly one lattice point, so $\wp(z)$ has two poles in each fundamental region. We showed in the above exercise that $\wp'(z)$ is periodic; so $\wp'(z + \omega_j) = \wp'(z)$ where $j = 1, 2$. Upon integrating, we obtain $\wp(z + \omega_j) - \wp(z) = c_j$. Choosing $z = -\omega_j/2$ and using the fact that $\wp(z)$ is an even function implies that $c_j = 0$. This shows that $\wp(z)$ is an elliptic function of order[6] 2 for Λ.

Lemma 2.14. Given a lattice Λ, the Laurent series for $\wp(z)$ about $z = 0$ is given by

$$\wp(z) = \frac{1}{z^2} + \sum_{k \geq 1} (2k+1) G_{2k+2}(\Lambda) z^{2k}.$$

Sketch of proof. Recall that the power series expansion of $f(x) = \frac{1}{(1-x)^2}$ in $|x| < 1$ is

$$\frac{1}{(1-x)^2} = \sum_{n \geq 0} (n+1) x^n.$$

Set $x = z/\omega$ and assume that $|x| < 1$ (this holds for all $\omega \in \Lambda \setminus \{0\}$ when z is near 0), then

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \sum_{n \geq 0} \frac{(n+1) z^n}{\omega^{n+2}}.$$

Summing over ω, changing the order of summation (via absolute convergence), and using the fact that $\wp$ is an even function gives the result. □

[5] A holomorphic function is a complex-valued function that is complex differentiable in a neighbourhood of each point in a domain in complex coordinate space.

[6] Recall that the *order* of an elliptic function is the sum of the orders of the poles it has in any fundamental parallelogram (the number of poles counted with multiplicity).

2.3. **Lattices Define Elliptic Curves.**

Exercise 2.15. Let Λ be a lattice. Show that the first few terms of the Laurent series expansions for $\wp(z)$, $\wp'(z)$, and their powers at $z = 0$ are as follows:

$$\wp(z) = \frac{1}{z^2} + 3G_4(\Lambda)z^2 + 5G_6(\Lambda)z^4 + \dots$$
$$\wp'(z) = \frac{-2}{z^3} + 6G_4(\Lambda)z + 20G_6(\Lambda)z^3 + \dots$$
$$\wp(z)^3 = \frac{1}{z^6} + \frac{9G_4(\Lambda)}{z^2} + 15G_6(\Lambda) + \dots$$
$$\wp'(z)^2 = \frac{4}{z^6} - \frac{24G_4(\Lambda)}{z^2} - 80G_6(\Lambda) + \dots.$$

Lemma 2.16. Let Λ be a lattice. The function $\wp(z)$ satisfies the differential equation

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4(\Lambda)\wp(z) - 140G_6(\Lambda).$$

Sketch of proof. Define

$$f(z) = \wp'(z)^2 - 4\wp(z)^3 - 60G_4(\Lambda)\wp(z) - 140G_6(\Lambda).$$

Using the previous exercise, we can compute the Laurent series expansion for $f(z)$ at $z = 0$. We obtain that $f(0) = 0$.

We have seen previously that $\wp, \wp'$ have poles only at the lattice points of Λ, so $f(z)$ is holomorphic in the fundamental parallelogram. Since, with respect to the lattice, $f(z)$ is a periodic function, it is holomorphic on all of $\mathbb{C}$. But this forces $f(z)$ to be constant (and hence identically 0). □

We simplify the notation and set

$$y = \wp'(z); \quad x = \wp(z); \quad -4A = g_2(\Lambda) = 60G_4(\Lambda); \quad -4B = g_3(\Lambda) = 140G_6(\Lambda).$$

The differential equation can then be rewritten as

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda). \tag{3}$$

If we want to re-write the equation in Weierstrass form, we may use the notation in terms of A, B. If we can further show that the projective curve defined by the differential equation is smooth, this would show that every lattice defines an elliptic curve over $\mathbb{C}$.

The following exercise might remind you of the fact that points of order 2 *on the elliptic curve are points of the form* (x, y) *such that* $y = 0$*. Here of course* $(x, y) = (\wp(z), \wp'(z))$*. The condition that* $z_0 \notin \Lambda$ *corresponds to saying that* (x, y) *is not the point at infinity.*

Exercise 2.17. Given a lattice Λ and $z_0 \notin \Lambda$, show that $\wp'(z_0) = 0$ if and only if $2z_0 \in \Lambda$. Moreover, the only such points z in the fundamental parallelogram are $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$, and $\frac{\omega_1+\omega_2}{2}$.

Set $r_1 = \omega_1/2$, $r_2 = \omega_2/2$, and $r_3 = r_1 + r_2$. Consider the cubic equation

$$f(x) = 4x^3 - g_2(\Lambda)x - g_3(\Lambda).$$

The above exercise shows that $\wp(r_i)$ are the three zeroes of the cubic equation. We now check that the zeroes are distinct. For this, define $f_i(z) = \wp(z) - \wp(r_i)$. This order 2 elliptic function has exactly 2 zeroes, and r_i is a double root (because $f_i'(r_i) = \wp'(r_i) = 0$). Since $f_i(z)$ has no other roots, it forces that $\wp(r_i) \neq \wp(r_j)$ when $i \neq j$. Therefore, the discriminant of the polynomial

$$\Delta(f) = \prod_{i<j}(\wp(r_i) - \wp(r_j))^2 = 16(g_2(\Lambda)^3 - 27g_3(\Lambda)^3) \neq 0. \tag{4}$$

Now, we return to the projective curve defined by the differential equation

$$zy^2 = 4x^3 - g_2(\Lambda)xz^2 - g_3(\Lambda)z^3.$$

Taking partial derivatives with respect to the variables x, y, and z, we note that if they were to simultaneously vanish then

$$\begin{aligned} 12x^2 - g_2(\Lambda)z^2 &= 0 \\ 2zy &= 0 \\ y^2 + 2g_2(\Lambda)xz + 3g_3(\Lambda)z^2 &= 0. \end{aligned}$$

We may assume that $z = 1$, else $x = y = z = 0$. This force

$$y = 0 \text{ and } x = \frac{-3g_3(\Lambda)}{2g_2(\Lambda)}.$$

In particular,

$$12x^2 = \frac{-27g_3(\Lambda)^2}{g_2(\Lambda)^2} = g_2(\Lambda).$$

Rearranging the terms, we see that the last equality cannot be satisfied because of (4). Since (3) is non-singular, we have shown that a lattice Λ gives rise to an elliptic curve.

2.4. **Uniformization Theorem.** So far we have constructed a map

$$\begin{aligned} \Phi : \mathbb{C}/\Lambda &\longrightarrow \mathsf{E}_\Lambda(\mathbb{C}) \\ z &\longmapsto \begin{cases} (\wp(z), \wp'(z)) & \text{if } z \notin \Lambda \\ 0 & \text{if } z \in \Lambda. \end{cases} \end{aligned}$$

where $\mathsf{E}_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$.

In this section, we will show that Φ is a group isomorphism. *This is the* Uniformization Theorem *which asserts that a lattice $\Lambda = [\omega_1, \omega_2]$ in $\mathbb{C}$ gives rise to an elliptic curve E_Λ, and every elliptic curve over $\mathbb{C}$ arises from a lattice.*

We make some observations

- Φ preserves the identity, since $0 \mapsto 0$.
- $\Phi(-z) = -\Phi(z)$, so the map is compatible with taking inverses.

Exercise 2.18. Show that the restriction of Φ to $(\mathbb{C}/\Lambda)[2]$ defines a bijection $(\mathbb{C}/\Lambda)[2] \to \mathsf{E}_\Lambda[2]$. Conclude that this must be a group isomorphism.

Claim: The map Φ is surjective.

Justification: Start with a point $(x_0, y_0) \in \mathsf{E}_\Lambda(\mathbb{C})$. Consider the elliptic function $f(z) = \wp(z) - x_0$ of order 2; it has two zeros in the fundamental parallelogram. Let $z_0 \neq 0$ be one such root (note that f has a pole at $z_0 = 0$); i.e., $\wp(z_0) = x_0$. The pre-images of (x_0, y_0) under the map Φ are $\pm z_0$.

Claim: The map Φ is injective.

Justification: Suppose that $\Phi(z_1) = \Phi(z_2)$ for two complex numbers z_1, z_2 in the fundamental parallelogram. In view of Exercise 2.18 we may assume that $2z_1 \notin \Lambda$. As in the previous argument, we work with $f = \wp(z) - \wp(z_1)$ and we know that the roots are $\pm z_1$. Thus $z_2 \equiv \pm z_1 \pmod{\Lambda}$. But our additional assumption $\wp'(z_1) = \wp'(z_2)$ forces that $z_2 \equiv z_1 \pmod{\Lambda}$ since $\wp'(z)$ is an odd function and $\wp'(z_1) \neq 0$.

We are still left to prove that Φ is in fact a homomorphism. This argument is not difficult, but requires revisiting results in complex analysis, so we outline the steps without giving the details.

Let z_1, z_2 in the fundamental domain. To show $\Phi(z_1 + z_2) = \Phi(z_1) + \Phi(z_2)$, it suffices to prove the case that $z_1, z_2, z_1 + z_2 \notin \Lambda$. Consider the line $y = mx + c$ joining $\mathsf{P}_1 = \Phi(z_1)$ and $\mathsf{P}_2 = \Phi(z_2)$. If P_3 is the third point where the line intersects E_Λ then $\mathsf{P}_3 = \Phi(z_3)$ where z_3 is the third zero of the

elliptic function $f(z) = -\wp'(z) + m\wp(z) + c$ in the fundamental domain. Using complex analysis, one can show that $z_1 + z_2 + z_3 \in \Lambda$. This implies

$$\Phi(z_1 + z_2) = \Phi(-z_3) = -\Phi(z_3) = -\mathsf{P}_3 = \mathsf{P}_1 + \mathsf{P}_2 = \Phi(z_1) + \Phi(z_2).$$

2.5. **Complex Multiplication.** To complete our understanding of the categorical equivalence of complex tori and elliptic curves, we want to relate morphisms of complex tori to isogenies[7] of elliptic curves. We state without proof that

$$\mathrm{Hom}(\mathbb{C}/\Lambda, \mathbb{C}/\Lambda) = \mathrm{End}(\mathsf{E}_\Lambda) \simeq \{\alpha \in \mathbb{C} \ : \ \alpha\Lambda \subseteq \Lambda\},$$

where the complex conjugation $\alpha \mapsto \overline{\alpha}$ in $\mathrm{End}(\mathbb{C}/\Lambda)$ corresponds to involution $\phi \mapsto \hat{\phi}$ in $\mathrm{End}(\mathsf{E}_\Lambda)$. When $\mathrm{End}(\mathsf{E}_\Lambda)$ is bigger than $\mathbb{Z}$, the extra endomorphisms in $\mathrm{End}(\mathsf{E}_\Lambda)$ correspond to multiplication-by-α maps in $\mathrm{End}(\mathbb{C}/\Lambda)$, where α is a non-real algebraic integer in an imaginary quadratic field. *The reader might benefit from looking at the worksheet for additional information.*

This begs the following question. Let $\mathfrak{O}$ be an order in an imaginary quadratic field K. It is a lattice, and we would like to understand for which lattices Λ do we have $\mathrm{End}(\mathsf{E}_\Lambda) = \mathfrak{O}$?

Without getting into technicalities we state the following theorem which shows the deep connections between the theory of elliptic curves and class field theory.

Theorem 2.19. Let $\mathfrak{O}$ be an order in an imaginary quadratic field. There is a one-to-one correspondence between elements of the ideal class group $\mathrm{cl}(\mathfrak{O})$ and homothety classes of lattices $\Lambda \subseteq \mathbb{C}$ for which $\mathrm{End}(\mathsf{E}_\Lambda) \simeq \mathfrak{O}$.

The main theorem of complex multiplication asserts that for any elliptic curve E over $\mathbb{C}$ with complex multiplication by an order inside K, the j-invariant $j(E)$ is algebraic, and generates an abelian extension over K. Moreover, for a torsion point $t \in \mathsf{E}(\mathbb{C})$, the extension $K(h(t))/K$ is abelian where $h(\cdot)$ is a Weber function.

3. Lecture 3: Elliptic Curves over Finite Fields

In this section, p always denotes a prime and $q = p^r$ for some $r \geq 1$.

3.1. **Reduction Types.** Since $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a field, we may talk about elliptic curves defined over $\mathbb{F}_p$. The elliptic curve must be given by a cubic equation and must be smooth.

Example 3.1. Let $\mathsf{E} : y^2 \equiv x^3 + 2 \pmod 5$. Write $F \equiv zy^2 - x^3 - 2z^3 \pmod 5$. We calculate the partial derivatives modulo 5

$$\frac{\partial F}{\partial x} \equiv -3x^2, \quad \frac{\partial F}{\partial y} \equiv 2yz, \quad \frac{\partial F}{\partial z} \equiv y^2 - z^2.$$

The partial derivatives vanish precisely when $x \equiv y \equiv z \equiv 0 \pmod 5$. Since $[0,0,0]$ is not a point in the projective plane, $\mathsf{E}/\mathbb{F}_5$ has no singular points and defines an elliptic curve.

Now consider $C : y^2 \equiv x^3 + 2 \pmod 3$. By calculating the partial derivatives modulo 3, we see that the point $\mathsf{P} = (\overline{1}, \overline{0})$ is a point of singularity. Hence $C/\mathbb{F}_3$ is *not* an elliptic curve.

3.1.1. *Minimal Model.* We continue our discussion on minimal models from Lecture 1.

Example 3.2. We return to our Example 1.5. As in the previous example, we can readily check by taking partial derivatives modulo 5 that the curve $\mathsf{E} : y^2 = x^3 + 1$ is an elliptic curve over $\mathbb{F}_5$. However, when we consider the model $C : y^2 = x^3 + 5^6$ then it is not smooth over $\mathbb{F}_5$. This again has to do with the fact that $y^2 = x^3 + 5^6$ is *not* the minimal model for the elliptic curve over $\mathbb{Q}$.

[7] An isogeny $\phi : \mathsf{E} \to \mathsf{E}'$ of elliptic curves defined over any field K is a surjective morphism of curves that induces a group homomorphism $\mathsf{E}(\overline{K}) \to \mathsf{E}'(\overline{K})$.

Definition 3.3. Let $\mathsf{E}/\mathbb{Q}$ be an elliptic curve given by minimal model. Let p be a prime and $\widetilde{\mathsf{E}}$ be the reduction curve of E modulo p. If $\widetilde{\mathsf{E}}$ is smooth then we say $\mathsf{E}/\mathbb{Q}$ has *good reduction* at the prime p. Else, we say that $\mathsf{E}/\mathbb{Q}$ has *bad reduction* at p.

We have the following important observation: let $\mathsf{E} : y^2 = f(x) = (x-\alpha)(x-\beta)(x-\gamma)$ be an elliptic curve over $\mathbb{Q}$ with integer coefficients (where α, β, γ are in $\overline{\mathbb{Q}}$) given by its minimal model. We know from Lecture 2 that

$$\frac{\Delta_{\mathsf{E}}}{16} = \Delta(f) = (\alpha-\beta)^2(\beta-\gamma)^2(\gamma-\alpha)^2.$$

The elliptic curve E has bad reduction at p precisely when $p \mid \Delta_{\mathsf{E}}$. Indeed, a singularity for $\widetilde{\mathsf{E}} : y^2 \equiv f(x) \pmod{p}$ occurs at $\mathsf{P} = (\delta, 0)$ where $f(\delta) = 0$ precisely when δ is a double root of $f(x)$.

3.1.2. *Types of bad reduction.* Given a finite field $\mathbb{F}_p$, let $\widetilde{\mathsf{E}}$ be a cubic curve with Weierstrass equation

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

If $\mathsf{P} = (x_0, y_0)$ is a point of singularity, then

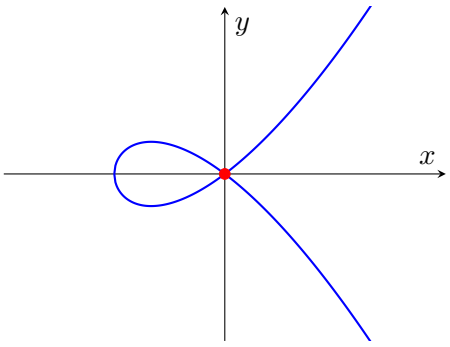
$$f(x,y) - f(x_0,y_0) = \delta_1(x-x_0)^2 + \delta_2(x-x_0)(y-y_0) + \delta_3(y-y_0)^2 - (x-x_0)^3,$$

where $\delta_i \in \mathbb{F}_p$. But there exist $\alpha, \beta \in \overline{\mathbb{F}_p}$ such that

$$f(x,y) - f(x_0,y_0) = ((y-y_0) - \alpha(x-x_0))((y-y_0) - \beta(x-x_0)) - (x-x_0)^3.$$

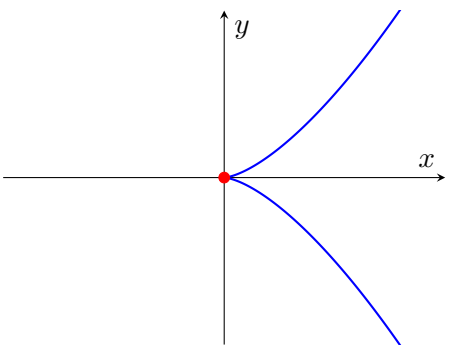
If $\alpha \neq \beta$, then P is called a *node*. In this case, there are two different tangent lines at P. If $\alpha = \beta$ then P is called a *cusp* and there is a unique tangent line at P.

Node



$y^2 = x^2(x+1)$

Cusp



$y^2 = x^3$

Definition 3.4. If $\widetilde{\mathsf{E}}$ has a cusp at P, then E has *additive/unstable* reduction. If $\widetilde{\mathsf{E}}$ has a node at P, then E has *multiplicative/stable* reduction. If $\alpha, \beta \in \mathbb{F}_p$ then the reduction is said to be *split multiplicative*, else it is called *non-split* multiplicative.

3.2. **Group Order and Structure.** Since $\mathbb{F}_q$ is a finite field, it is clear that $\mathsf{E}(\mathbb{F}_q)$ is always finite.

Example 3.5. Let $\mathsf{E} : y^2 = x^3 + x + 1$ be an elliptic curve over $\mathbb{F}_5$. We check that

$$\mathsf{E}(\mathbb{F}_5) = \{\mathcal{O}, (0,1), (0,4), (2,1), (2,4), (3,1), (3,4), (4,2), (4,3)\}.$$

Setting $\mathsf{P} = (0,1)$, we can calculate using the technique of adding points from Lecture 1

$$2\mathsf{P} = (4,2),\ 3\mathsf{P} = (2,1);\ 4\mathsf{P} = (3,4);\ 5\mathsf{P} = (3,1),\ 6\mathsf{P} = (2,4),\ 7\mathsf{P} = (4,3),\ 8\mathsf{P} = (0,4),\ 9\mathsf{P} = \mathcal{O}.$$

In other words, we check that $\mathsf{E}(\mathbb{F}_5) \simeq \mathbb{Z}/9\mathbb{Z}$.

Example 3.6. Let $\mathsf{E} : y^2 = x^3 + 2$ be an elliptic curve over $\mathbb{F}_7$. We check that

$$\mathsf{E}(\mathbb{F}_5) = \{\mathcal{O}, (0,3), (0,4), (3,1), (3,6), (5,1), (5,6), (6,1), (6,6)\}.$$

However, we check that there is no element of order 9 and hence $\mathsf{E}(\mathbb{F}_7) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

3.2.1. *Frobenius map.* Before the next example, let us discuss what happens in characteristic 2.

Recall that we may not work with the short Weierstrass equation in this case. Working with the general Weierstrass equation (1), depending on whether $a_1 = 0$ or not, we may perform change of variables and re-write the equation of the elliptic curve as

$$y^2 + xy = x^3 + a_2'x^2 + a_6' \text{ where } a_6' \neq 0$$
$$y^2 + a_3'y = x^3 + a_4'x + a_6' \text{ where } a_3' \neq 0.$$

If we want to find points of order 2, we need to ensure that the partial derivative with respect to y vanishes. In the first case this means $x = 0$, equivalently there is exactly one non-trivial point of order 2. In the second case, the partial derivative with respect to y can never vanish, so $\mathsf{E}[2] = \{\mathcal{O}\}$.

Example 3.7. Consider $\mathsf{E} : y^2 + xy = x^3 + 1$ defined over $\mathbb{F}_2$. We can calculate

$$\mathsf{E}(\mathbb{F}_2) = \{\mathcal{O}, (0,1), (1,0), (1,1)\}.$$

Now, consider the field $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/\langle X^2 + X + 1\rangle = \{0, 1, \omega, \omega^2\}$ where $1 + \omega + \omega^2 = 0$. Then

$$\mathsf{E}(\mathbb{F}_4) = \{\mathcal{O}, (0,1), (1,0), (1,1), (\omega,0), (\omega,\omega), (\omega^2,0), (\omega^2,\omega^2)\} \simeq \mathbb{Z}/8\mathbb{Z} = \langle(\omega,0)\rangle.$$

Exercise 3.8. Consider the map $\phi_2 : \mathsf{E}(\mathbb{F}_4) \to \mathsf{E}(\mathbb{F}_4)$ given by $(x,y) \mapsto (x^2, y^2)$. Show that ϕ_2 permutes the elements of $\mathbb{F}_4$.

Definition 3.9. Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$. The the map

$$\begin{aligned} \phi_q : \mathsf{E}(\overline{\mathbb{F}_q}) &\longrightarrow \mathsf{E}(\overline{\mathbb{F}_q}) \\ (x,y) &\longmapsto (x^q, y^q) \end{aligned}$$

is an endomorphism of E called the *Frobenius endomorphism*.

Let us record some statements about the Frobenius endomorphism [59, Theorem 4.10]

- $\phi_q^n = \phi_{q^n}$.
- The characteristic polynomial of the Frobenius endomorphism is given by
$$\phi_q^2 - a_q(\mathsf{E})\phi_q + q = 0.$$
The quantity $a_q(\mathsf{E}) = q + 1 - \#\mathsf{E}(\mathbb{F}_q)$ is the *trace of the Frobenius*.
- The group of q-rational points $\mathsf{E}(\mathbb{F}_q)$ is the kernel of the separable endomorphism $\phi_q - 1$. Thus,
$$\#\mathsf{E}(\mathbb{F}_q) = \deg(\phi_q - 1) = (\phi_q - 1)(\hat{\phi}_q - 1) = q + 1 - \text{trace}(\phi_q),$$
where we use the fact that $\hat{\phi}_q$ is the dual of ϕ_q and $\phi_q\hat{\phi}_q = \deg(\phi_q) = q$.

Fix an elliptic curve E defined over the finite field $\mathbb{F}_q$. Consider the factorization of the polynomial

$$X^2 - a_q(\mathsf{E})X + q = (X - \alpha)(X - \beta). \tag{5}$$

Exercise 3.10. Show that $s_n = \alpha^n + \beta^n$ is always an integer for $n \geq 1$. In particular, show that $s_0 = 2$, $s_1 = a_q(\mathsf{E})$, and $s_{n+1} = a_q(\mathsf{E})s_n - qs_{n-1}$.

With this description, define

$$f(X) \coloneqq (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n.$$

By construction $(X - \alpha)(X - \beta) \mid f(X)$. In particular,

$$0 = f(\phi_q) = (\phi_q^n)^2 - (\alpha^n + \beta^n)\phi_q^n + q^n = (\phi_{q^n})^2 - (\alpha^n + \beta^n)\phi_{q^n} + q^n.$$

It follows from the facts stated above that

$$a_{q^n}(\mathsf{E}) = \alpha^n + \beta^n = q^n + 1 - \#\mathsf{E}(\mathbb{F}_{q^n}).$$

Example 3.11. Consider the curve $\mathsf{E} : y^2 = x^3 + 4x - 1$ over $\mathbb{F}_7$. We may check by direct computation that $\#\mathsf{E}(\mathbb{F}_7) = 11$ or use Problem 3.1 from the Worksheet. We calculate $a_7(\mathsf{E}) = -3$.

Now if we want to compute $\mathsf{E}(\mathbb{F}_{7^3})$ we write

$$X^2 + 3X + 7 = (X - \alpha)(X - \overline{\alpha}) \text{ with } \alpha = \frac{-3 + i\sqrt{19}}{2}.$$

Then for $\overline{\alpha} = \beta$, we have

$$\#\mathsf{E}(\mathbb{F}_{7^3}) = 343 + 1 - (\alpha^3 + \beta^3) = 343 + 1 - (a_7(\mathsf{E})^2 - 3 \cdot 7)a_7(\mathsf{E}) = 308 = 2^2 \times 7 \times 11.$$

3.2.2. *Group Structure.* First we discuss the torsion part. For a field of characteristic 0, such as $\mathbb{Q}$, we can show[8] that $\mathsf{E}(\overline{\mathbb{Q}})[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. If $\mathbb{F}$ is a (finite) field of characteristic p and $p \nmid n$ then again $\mathsf{E}(\overline{\mathbb{F}})[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. However, if $p \mid n$ the structure is different. More precisely if n' is the largest p-free part of n, then

$$\mathsf{E}(\overline{\mathbb{F}})[n] \simeq \mathbb{Z}/n'\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z} \text{ or } \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}.$$

For a proof, we refer the reader to [59, Theorem 3.2].

Definition 3.12. An elliptic curve E in characteristic p is called *ordinary* if $\mathsf{E}[p] \simeq \mathbb{Z}/p\mathbb{Z}$ and is called *supersingular* if $\mathsf{E}[p]$ is trivial.

Now, suppose we want to go a step further and understand the full structure of $\mathsf{E}(\mathbb{F}_q)$. A finite abelian group is isomorphic to a direct sum of cyclic groups

$$\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z},$$

where $m_i \mid m_{i+1}$ for all $i \geq 1$. It is immediate that there are m_1^r many elements of order m_1 but we just saw that there can be at most m_1^2 many such points. This forces

$$\mathsf{E}(\mathbb{F}_q) \simeq \mathbb{Z}/m\mathbb{Z} \text{ or } \mathsf{E}(\mathbb{F}_q) \simeq \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \text{ where } m_1 \mid m_2.$$

Using some basic properties of the Frobenius map ϕ_q that we have unfortunately not discussed in these lectures, we can get an upper bound on $\#\mathsf{E}(\mathbb{F}_q)$. This result is attributed to Helmut Hasse:

Theorem 3.13 (Hasse)**.** Let E be an elliptic curve over the finite field $\mathbb{F}_q$. Then the order of $\#\mathsf{E}(\mathbb{F}_q)$ satisfies the following inequality satisfies

$$\left|a_q(\mathsf{E})\right| = \left|q + 1 - \#\mathsf{E}(\mathbb{F}_q)\right| \leq 2\sqrt{q}.$$

Intuition: Suppose that $\mathsf{E}/\mathbb{Q}$ is an elliptic curve given in its short Weierstrass form with integer coefficients. Further suppose that $q = p$. This means we have p many choices for $x \in \mathbb{F}_p$. For each $x = x_0$, we have $y^2 = f(x_0) \in \mathbb{F}_p$. The probability that a random element in $\mathbb{F}_p$ is (or is not) a square is $1/2$. If $f(x_0)$ is a square modulo p, then there are *two* corresponding values of y which satisfy the equation, else there are none. Finally, we need to account for the point $\mathcal{O}$. This means

$$\#\mathsf{E}(\mathbb{F}_p) \approx p\left(\frac{1}{2} \times 2 + \frac{1}{2} \times 1\right) + 1 = p + 1.$$

The following two results completely describe the structure of $\mathsf{E}(\mathbb{F}_q)$; see [59, Theorems 4.3–4.4]

Theorem 3.14. Let $q = p^n$ be a power of a prime p and set $N = q + 1 - a$. There exists an elliptic curve E defined over $\mathbb{F}_q$ with $\#\mathsf{E}(\mathbb{F}_q) = N$ if and only if $|a| \leq 2\sqrt{q}$ and a satisfies one of the following:

[8] See Problem 2.1 of the Worksheet.

(1) $\gcd(a,p)=1$,
(2) n is even and $a=\pm 2\sqrt{q}$
(3) n is even, $p\not\equiv 1 \pmod 3$, and $a=\pm\sqrt{q}$
(4) n is odd, $p=2$ or 3, and $a=\pm p^{(n+1)/2}$
(5) n is even, $p\not\equiv 1 \pmod 4$, and $a=0$
(6) n is odd and $a=0$.

Theorem 3.15. Let N be an integer that occurs as the order of an elliptic curve over a finite field $\mathbb{F}_q$, as in Theorem 3.14 above. Suppose that $p^e \,||\, N$ and $N=p^e m_1 m_2$ with $m_1 \mid m_2$ (note that m_1 may be 1). There is an elliptic curve $\mathsf{E}/\mathbb{F}_q$ satisfying

$$\mathsf{E}(\mathbb{F}_q) \simeq \mathbb{Z}/p^e\mathbb{Z} \times \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$$

if and only if

(1) $m_1 \mid (q-1)$ in cases (1), (3)–(6) of Theorem 3.14.
(2) $m_1 = m_2$ in cases (2) of Theorem 3.14.

Example 3.16. We return to Example 3.11. First we note that $a_{7^3}(\mathsf{E})=36$ which is coprime to 7. We check that the cubic polynomial x^3+4x-1 factorizes into three linear factors in $\mathbb{F}_{7^3}$. This means there are three non-trivial points of order 2 in $\mathsf{E}(\mathbb{F}_{343})$, and no points of order 4. By the previous result, we conclude that

$$\mathsf{E}(\mathbb{F}_{343}) \simeq \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/22\mathbb{Z}.$$

Let $\mathsf{E}/\mathbb{F}_q$ be an elliptic curve and suppose that

$$\mathsf{E}(\mathbb{F}_q) \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},$$

for some n. We know from our above discussion that $\gcd(q,n)=1$. Moreover, it follows from the Weil pairing[9] on elliptic curves that the n-th roots of unity must be contained in $\mathbb{F}_q$. In particular, $n \mid (q-1)$. Therefore,

$$a_q(\mathsf{E}) = q+1-n^2 \equiv 2 \pmod n.$$

Exercise 3.17. Show that q is either of the form n^2+1 or $n^2 \pm n+1$ or $(n\pm 1)^2$.

We make one final remark. So far, we discussed the case that $\mathsf{E}/\mathbb{F}_p$ is an elliptic curve. In other words, there are no singular points when we consider the reduced curve $\mathsf{E} \pmod p$. However, there are techniques to count the number of *non-singular points* even when $\mathsf{E}/\mathbb{Q}$ has bad reduction at p. In particular,

$$\#\mathsf{E}^{\mathrm{ns}}(\mathbb{F}_p) = \begin{cases} p-1 & \text{if } p \text{ is a prime of split multiplicative reduction} \\ p+1 & \text{if } p \text{ is a prime of non-split multiplicative reduction} \\ p & \text{if } p \text{ is a prime of additive reduction.} \end{cases}$$

3.3. **Supersingular Curves.** We begin by giving a precise criterion for an elliptic curve over a finite field to be supersingular.

Lemma 3.18. Let $\mathsf{E}/\mathbb{F}_q$ be an elliptic curve. The elliptic curve E is supersingular if and only if $p \mid a_q(\mathsf{E})$; i.e. if and only if $\#\mathsf{E}(\mathbb{F}_q) \equiv 1 \pmod p$.

[9]The Weil pairing is a pairing (bilinear form with multiplicative notation) on the points of order dividing n of an elliptic curve E, taking values in n-th roots of unity [52, Section III.8].

Sketch of proof. Suppose that $a_q(\mathsf{E}) \equiv 0 \pmod{p}$. We know by Exercise 3.10 that

$$s_1 = a_q(\mathsf{E}) \equiv 0 \pmod{p} \text{ and } s_n \equiv 0 \pmod{p} \text{ for all } n \geq 1.$$

It follows that

$$\#\mathsf{E}(\mathbb{F}_{q^n}) = q^n + 1 - s_n \equiv 1 \pmod{p}.$$

This means there are no points of order p in $\mathsf{E}(\mathbb{F}_{q^n})$ for any $n \geq 1$ and hence also in $\mathsf{E}(\overline{\mathbb{F}_q})$. Thus, by definition, E is supersingular.

On the other hand, suppose that $a_q(\mathsf{E}) \not\equiv 0 \pmod{p}$. Then

$$s_n \equiv a_q(\mathsf{E})^n \pmod{p} \text{ for all } n \geq 1.$$

In particular,

$$\#\mathsf{E}(\mathbb{F}_{q^n}) = q^n + 1 - s_n \equiv 1 - a_q(\mathsf{E})^n \pmod{p}.$$

By Fermat's Little Theorem, $p \mid \#\mathsf{E}(\mathbb{F}_{q^{p-1}})$. Thus, E is ordinary. □

Exercise 3.19. Suppose that $p \geq 5$. Then $\mathsf{E}/\mathbb{F}_p$ is supersingular if and only if $a_p(\mathsf{E}) = 0$.

If E is an elliptic curve defined over $\mathbb{Q}$ (such that the Weierstrass equation has integer coefficients) with complex multiplication by a subring of $\mathbb{Q}(\sqrt{-d})$, and p is an odd prime number such that $p \nmid d$ and $\widetilde{\mathsf{E}} \pmod{p}$ is an elliptic curve, then $\widetilde{\mathsf{E}} \pmod{p}$ is supersingular if and only if $-d$ is not a square modulo p. Therefore, the reduced curve is supersingular for approximately half of the primes.

If E does *not* have complex multiplication, then the set of primes for which $\widetilde{\mathsf{E}} \pmod{p}$ is supersingular is infinite but of zero density [15, 49]. It was conjectured by Serge Lang and Hale Trotter [32] that the number of supersingular p is asymptotic to $\frac{C\sqrt{x}}{\ln x}$ for some constant $C = C(\mathsf{E})$ as $x \to \infty$.

3.4. **Sato–Tate Conjecture.** This is a statistical statement about the family of elliptic curves $\widetilde{\mathsf{E}}$ modulo p for almost all primes p posed by Mikio Sato and John Tate [54] independently in the 1960's. This is now a theorem for rational elliptic curves (and more generally for elliptic curves defined over any totally real number field) by the work of Tom Barnet-Lamb, Laurent Clozel, Michael Harris, David Geraghty, Nicholas Shepherd-Barron, and Richard Taylor [4, 8, 22, 55].

Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. In view of Hasse's theorem, we know that for a prime number p, we can define $0 \leq \theta_p \leq \pi$ as the solution to the equation

$$p + 1 - \#\mathsf{E}(\mathbb{F}_p) = 2\sqrt{p}\cos(\theta_p)$$

Then the conjecture predicts that for any $0 \leq \alpha < \beta \leq \pi$,

$$\lim_{X\to\infty} \frac{p \leq X \ : \ \alpha \leq \theta_p \leq \beta}{\#\{p \leq X\}} = \frac{2}{\pi}\int_\alpha^\beta \sin^2(\theta)d\theta.$$

The reader may refer to [40] *for a gentle introduction to the subject and related questions.*

4. Lecture 4: Modular Forms and L-Functions

This is a brief introduction to the subject with no proofs. The main goal of the lecture is to discuss the Birch and Swinnerton-Dyer Conjecture. In the process, we will discuss notions to make sense of the terms arising in the conjecture.

4.1. Definition and Examples.

4.1.1. *Congruence Subgroup.* Fix a positive integer N. Define the following subgroups of $\mathrm{SL}_2(\mathbb{Z})$

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

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ c \equiv 0 \pmod{N} \text{ and } a \equiv d \equiv 1 \pmod{N} \right\},$$

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ b \equiv c \equiv 0 \pmod{N} \text{ and } a \equiv d \equiv 1 \pmod{N} \right\}.$$

Exercise 4.1. If $M \mid N$, show that $\Gamma_0(N) \subseteq \Gamma_0(M)$.

Let Γ be a fixed congruence subgroup. Recall that

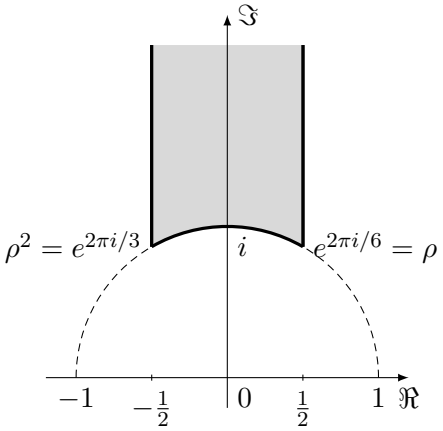
$$\mathbb{P}^1(\mathbb{Q}) = \{[x, y] \ \ x, y \in \mathbb{Q} \text{ with } (x, y) \neq (0, 0)\}.$$

Set $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$. We say $\tau, \tau' \in \mathbb{H}^*$ are Γ-equivalent if there exists $M \in \Gamma$ such that $\tau' = M\tau$. This is an equivalence relation. Define $X(\Gamma) = \mathbb{H}^*/\Gamma$ to be the set of all equivalence classes; this space $X = X(\Gamma)$ is called the *modular curve*. The *cusps* of X are the elements in the quotient that have representative in $\mathbb{P}^1(\mathbb{Q})$.

Example 4.2. Let $\Gamma = \Gamma_0(p)$. Suppose that there is one cusp in $X_0(p) = \mathbb{H}^*/\Gamma_0(p)$. Then there is a matrix $M \in \Gamma_0(p)$ such that $M \cdot \infty = 0$ and $a/c = M \cdot \infty = 0$. In particular, $a = 0$ and using the formula of the determinant of a matrix we must have $ad - bc = -bc = 1$. Since $p \mid c$, this is not possible. It follows that $\infty \not\sim 0$ in $X_0(p)$. On the other hand, if $\frac{r}{s} \in \mathbb{Q}$ such that s is divisible by p then there is a matrix $M \cdot \infty = \frac{r}{s}$ where $\gcd(r, s) = 1$. We obtain this matrix by choosing $a = r$ and $c = p$. If $\frac{r}{s} \in \mathbb{Q}$ such that $p \nmid s$ then there is a matrix $M \cdot 0 = \frac{r}{s}$ which we obtain by choosing $b = r$ and $d = s$. This shows that there are precisely two cusps.

Exercise 4.3. Show that $X(1) = \mathbb{H}^*/\Gamma(1)$ has one cusp.

We can make sense of the notion of *fundamental domains* even in this context. We draw the picture for the fundamental domain of $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$ (this is the non-compact version of $X(1)$ where we make the observation that $\mathrm{SL}_2(\mathbb{Z}) = \Gamma(1)$).



In view of the Uniformization Theorem and Exercise 2.4, we can make the following observation: non-cuspidal points in $X(1)$ classify elliptic curves (up to isomorphism) over $\mathbb{C}$. Indeed, if $[\tau] \in X(1)$

is non-cuspidal then it corresponds to $\mathsf{E}/\mathbb{C} \simeq \mathbb{C}/\Lambda$ where $\Lambda = [\tau, 1]$, and conversely. For more general Γ, one can show similar correspondence between the modular curve $X(\Gamma)$ and elliptic curves with additional structure.

The modular curve for $\Gamma_0(N)$ is a compact Riemann surface with a rational model as a projective algebraic curve. The model may not always be an elliptic curve, it can have higher genus for example. It is also possible that the model is highly singular. For any elliptic curve $\mathsf{E}/\mathbb{Q}$ there exists a positive integer N and a surjective morphism $\varphi : X_0(N) \to \mathsf{E}$ defined over $\mathbb{Q}$. This map is called the *modular parameterization of* E. More generally, any elliptic curve (not necessarily defined over $\mathbb{Q}$) that admits a modular parameterization is called a *modular elliptic curve*. Note that this is not the same as saying that $X_0(N)$ is itself an elliptic curve.

Example 4.4 (Digression)**.** *In this example we try to showcase one area where the study of modular curves played a major role. Using vast generalizations of the ideas mentioned in this example, Barry Mazur proved the theorem classifying the possible structures of the torsion subgroup for* $\mathsf{E}/\mathbb{Q}$.

Consider the example $\Gamma = \Gamma_0(11)$.

Define a *modular pair* over a field K to be a pair (E, C) where E/K is an elliptic curve and C is a cyclic subgroup of $\mathsf{E}(\overline{K})$ of order 11. Two modular pairs (E, C) and (E', C') are isomorphic if $\mathsf{E} \simeq \mathsf{E}'$ are isomorphic over K and this isomorphism respects $C \simeq C'$.

Thus over the complex numbers, the pair $(\mathbb{C}/\Lambda_\tau, C)$ is isomorphic to $(\mathbb{C}/\Lambda_{\tau'}, C')$ precisely when there exists α satisfying $\alpha\Lambda_\tau = \Lambda_{\tau'}$ and $\alpha C = C' \pmod{\Lambda_{\tau'}}$.

Suppose we start with $(\mathbb{C}/\Lambda, C)$ where C has order 11. We can associate with this pair a complex number $\tau \in \mathbb{H}$ such that $(\mathbb{C}/\Lambda, C) \simeq (\mathbb{C}/\Lambda_\tau, \mathbb{Z}/11\mathbb{Z})$. But this τ is not unique. There is a one-to one correspondence between $\tau \in \mathbb{H}/\Gamma_0(11)$ and modular pairs $(\mathbb{C}/\Lambda_\tau, \mathbb{Z}/11\mathbb{Z})$ which we denote by $\mathrm{Ell}_0(\mathbb{C})$. Upon adding cusps, $X_0(11)$ can be given the structure of a compact Riemann surface and we have a bijection

$$X_0(11) \longleftrightarrow \mathrm{Ell}_0(\mathbb{C}) \cup \mathbb{C}.$$

Since every Riemann surface corresponds to a complex algebraic curve, the same holds for $X_0(11)$. We write this curve as $X_0(11)_{\mathbb{C}}$. However, this curve can be defined over $\mathbb{Q}$; i.e., it has a rational model. In other words, the Riemann surface $X_0(11)$ – which can be shown to be a torus – can be represented by an algebraic curve $X_0(11)_{\mathbb{Q}}$ over $\mathbb{Q}$. It follows that $X_0(11)_{\mathbb{Q}}$ is an elliptic curve and has a Weierstrass equation. *However, it is pertinent to point out that* $X_0(11)_{\mathbb{Q}}(\mathbb{Q})$ *is not the same as* $\mathrm{Ell}_0(\mathbb{Q})$. The equation of the elliptic curve is given by

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

This can be shown to have rank 0 and the torsion subgroup has order 5. More precisely,

$$X_0(11)_{\mathbb{Q}}(\mathbb{Q}) = \{\mathcal{O}, (5,5), (16,-61), (16,60), (5,-6)\}.$$

Two of these points come from cusps. But, we do not have a good understanding of the other three points. *Even if these points correspond to* (E, C) *in* $\mathrm{Ell}_0(\mathbb{Q})$*, it would only produce an elliptic curve* $\mathsf{E}/\mathbb{Q}$ *and a point* $\mathsf{P} \in \mathsf{E}[11]$ *such that* $\sigma(\mathsf{P})$ *is a multiple of* P *for all* $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

But one can repeat the same argument with $\Gamma = \Gamma_1(11)$. This time we need to work with *refined modular pairs* over a field K which are pairs of the form (E, P) where E/K and $\mathsf{P} \in \mathsf{E}(K)$ has exact order 11. With *much more work* one can show a bijection

$$X_1(11) \longleftrightarrow \mathrm{Ell}_1(\mathbb{C}) \cup \mathcal{C},$$

where $\mathcal{C}$ is a set of ten cusps *but not all cusps lie in* $X_1(11)_{\mathbb{Q}}(\mathbb{Q})$. For every number field $K/\mathbb{Q}$ there is a bijection

$$X_1(11)_{\mathbb{Q}}(K) \longleftrightarrow \mathrm{Ell}_1(K) \cup \mathcal{C}(K),$$

with $\#\mathcal{C}(K) \in \{5, 10\}$ dependent on if $\mathbb{Q}(\zeta_{11})^+ \subseteq K$. The Weierstrass equation for $X_1(11)_{\mathbb{Q}}$ is

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

This again has rank 0 and one can compute

$$X_0(11)_{\mathbb{Q}}(\mathbb{Q}) = \{\mathcal{O}, (0,0), (1,-1), (1,0), (0,-1)\}.$$

But all these points correspond to cusps so there is no rational elliptic curve with 11-torsion.

4.1.2. *Modular Function.*

Definition 4.5. Fix a congruence subgroup Γ. A function $f : \mathbb{H}^* \to \mathbb{C} \cup \{\infty\}$ is called a *modular function for* Γ if it satisfies the following properties:

- f is meromorphic on $\mathbb{H}^*$.
- $f(z) = f(Mz)$ for all $M \in \Gamma$.

Exercise 4.6. Show that $\mathrm{SL}_2(\mathbb{Z})$ is generated by the matrices $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Conclude that any modular function f for $\mathrm{SL}_2(\mathbb{Z})$ must satisfy $f(z) = f(z+1)$ and $f(z) = f(-1/z)$.

Let $\Lambda = [\tau, 1]$ be a lattice. Previously, we have seen the functions $g_2(\tau)$, $g_3(\tau)$. We now look at some reinterpretations of these functions. Write $\sigma_k(n) = \sum_{d|n} d^k$ and fix $q = e^{2\pi i \tau}$. Then

$$g_2(\tau) = \frac{4\pi^4}{3}\left(1 + 240\sum_{n\geq 1}\sigma_3(n)q^n\right)$$
$$g_3(\tau) = \frac{8\pi^6}{3}\left(1 - 504\sum_{n\geq 1}\sigma_5(n)q^n\right)$$
$$\Delta(\tau) = g_2^3(\tau) - 27g_3^2(\tau) = (2\pi)^{12}q\sum_{n\geq 1}(1-q^n)^{24}.$$

For a proof, we refer the reader to [59, pp. 273–4].

Exercise 4.7. Recall that

$$j(\tau) = 1728\frac{g_2^3(\tau)}{\Delta(\tau)}.$$

Show that $j(\tau) = \frac{1}{q} + 744 + \sum_{n\geq 1} a_n q^n$ with $a_n \in \mathbb{Z}$. Thus, $j(\tau)$ is a modular function for $\Gamma(1)$.

Does it now make sense why the definition of the j-function has a factor of 1728?

4.1.3. *Modular Form.*

Definition 4.8. Fix a congruence subgroup Γ and an integer k. A function $f : \mathbb{H}^* \to \mathbb{C} \cup \{\infty\}$ is called a *modular form of weight k for* Γ if it satisfies the following properties:

- f is holomorphic on $\mathbb{H}^*$.
- $f(Mz) = (cz + d)^k f(z)$ for all $M \in \Gamma$.

If the modular form vanishes at the cusp, then it is called a *cusp form of weight k for* Γ.

Exercise 4.9. Suppose that $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. Show that a modular form $f(z)$ has a Taylor expansion

$$f(z) = \sum_{n\geq 0} a_n q^n \text{ where } a_n \in \mathbb{Z} \text{ and } q = e^{2\pi i z}.$$

If $f(z)$ is a cusp form, show that $a_0 = 0$. *The integers a_n are called the Fourier coefficients of f.*

If we work with $\Gamma(N) \subseteq \Gamma(1)$, then we can check that $f(z) = f(T^N z) = f(z+N)$ for all $z \in \mathbb{H}$. In this case, the Taylor series expansion of the modular form $f(z)$ becomes

$$f(z) = \sum_{n \geq 0} a_n q_N^n \text{ where } q_N = e^{2\pi i z/N}.$$

More generally, if Γ is any congruence subgroup, we can always find $M \geq 1$ such that $\Gamma(M) \subseteq \Gamma$. Once again in this case, $f(z) = \sum_{n \geq 0} a_n q_M^n$.

Example 4.10. Set $k > 2$. Recall the definition of the Eisenstein series

$$G_k(\tau) = \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(m\tau + n)^k}.$$

Observe that

$$G_k(S\tau) = G_k(-1/\tau) = \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(-\frac{m}{\tau} + n)^k} = \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{\tau^k}{(-m + n\tau)^k} = \tau^k G_k(\tau)$$

$$G_k(T\tau) = G_k(\tau + 1) = 1^k G_k(\tau).$$

In addition, when k is even,

$$\lim_{\Im(\tau) \to \infty} G_k(\tau) = \lim_{\Im(\tau) \to \infty} \sum_{m,n} \frac{1}{(m\tau + n)^k} = 2 \sum_{m \geq 1} \frac{1}{m^k} = 2\zeta(k) < \infty.$$

We use the absolute convergence of $G_k(\tau)$. Thus, G_{2k} is a weight-$2k$ modular form with $k > 1$.

4.2. L-Functions.

4.2.1. *L-functions of modular forms.* Fix integers $N, k \geq 1$. Let $f(z)$ be a cusp form of weight k for the congruence subgroup $\Gamma_0(N)$. Since the matrix $T \in \Gamma_0(N)$, we know that $f(z) = f(z+1)$ for all $z \in \mathbb{H}$. Since $f(z)$ is a cusp form, it must have a q-expansion

$$f(z) = \sum_{n \geq 1} a_n q^n \text{ where } a_n \in \mathbb{C}.$$

Given a cusp form $f(z)$ of weight k, the *L-function of* $f(z)$ is defined as

$$L(f, s) = \sum_{n \geq 1} a_n n^{-s}.$$

The L-function $L(f, s)$ converges uniformly for $\Re(s) > 1 + k/2$.

By the work of Erich Hecke, the L-function $L(f, s)$ of a cusp form f for $\Gamma_0(N)$ has an analytic continuation and a functional equation.

Theorem 4.11 (Hecke)**.** Let $L(f, s)$ be the L-series of a weight-k cusp form $f(z)$ for the congruence subgroup $\Gamma_0(N)$. Then $L(f, s)$ extends analytically to a holomorphic function on $\mathbb{C}$, and the normalized[10] function $\tilde{L}(f, s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(f, s)$ satisfies a functional equation of the form

$$\tilde{L}(f, s) = \pm \tilde{L}(f, k - s).$$

An important class of cusp forms are *newforms*. A cusp form $f(z)$ for the congruence subgroup $\Gamma_0(N)$ which is also a cusp form for the congruence subgroup $\Gamma_0(M)$ for some $M \mid N$ $(M < N)$ is called an *old form*. On the other hand, one that does not arise in this way is called a *newform*.

When f is a newform, we can write the series as an Euler product; see [13, Section 5.9].

[10]The $\Gamma(s)$ appearing in the normalization denotes the Γ function defined as $\Gamma(s) = \int_0^\infty t^{s-1} e^{-t} dt$.

Theorem 4.12 (Hecke)**.** Let $L(f,s)$ be the L-series of a weight-k newform $f(z)$ for the congruence subgroup $\Gamma_0(N)$. Then

$$L(f,s) = \sum_{n\geq 1} a_n n^{-s} = \prod_p (1 - a_p p^{-s} + \chi(p) p^{k-1} p^{-2s})^{-1},$$

where $\chi(p) = 0$ for $p \mid N$ and $\chi(p) = 1$ otherwise,

4.2.2. *L-functions of elliptic curves.* Let $\mathsf{E}/\mathbb{Q}$ be an elliptic curve. Recall the notation

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

where $\widetilde{\mathsf{E}}$ is the reduced elliptic curve modulo p. Define *local L-factor* at p as follows

$$L_p(X) = \begin{cases} 1 - a_p(\mathsf{E})X + pX^2 & \text{if } \mathsf{E} \text{ has good reduction at } p, \\ 1 - X & \text{if } \mathsf{E} \text{ has split multiplicative reduction at } p, \\ 1 + X & \text{if } \mathsf{E} \text{ has non-split multiplicative reduction at } p, \\ 1 & \text{if } \mathsf{E} \text{ has additive reduction at } p. \end{cases}$$

The *Hasse–Weil L-function* of the elliptic curve $\mathsf{E}/\mathbb{Q}$ is then defined as

$$L(\mathsf{E},s) = \prod_p \frac{1}{L_p(p^{-s})}.$$

Note that the local L-factor of $L(\mathsf{E},s)$ and $L(f,s)$ have similar shape exactly when $k = 2$.

Exercise 4.13. Consider the elliptic curve $\mathsf{E} : y^2 + y = x^3 - x^2 - 10x - 20$ (which is its minimal model). This is the curve 11.a2 in LMFDB. Calculate Δ_{E} and find the reduction type at the primes of bad reduction of E. Write the L-series attached to E as a sum $\sum_{n\geq 1} a_n n^{-s}$.

The Fourier coefficients a_n can be made precise. Let $\mathsf{E}/\mathbb{Q}$ be an elliptic curve with L-function $L(\mathsf{E},s)$. Set $a_1 = 1$ and for $p \geq 2$ a prime, define

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

If $n = p^r$ for $r \geq 2$, define

$$a_{p^r} \coloneqq \begin{cases} a_p \cdot a_{p^{r-1}} - p \cdot a_{p^{r-2}} & \text{if } \mathsf{E} \text{ has good reduction at } p, \\ (a_p)^r & \text{if } \mathsf{E} \text{ has bad reduction at } p. \end{cases}$$

If $\gcd(m,n) = 1$, define $a_{mn} = a_m \cdot a_n$. Then

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

Using the theory of Hecke operators it is possible to show that the n-th Fourier coefficients of $L(f,s)$ have similar recursive formula as above when $f(z)$ is an eigenform. This raises a natural question: given an elliptic curve $\mathsf{E}/\mathbb{Q}$, is there a modular form f for which $L(\mathsf{E},s) = L(f,s)$?

Let $\mathsf{E}/\mathbb{Q}$ be an elliptic curve. Write $L(\mathsf{E},s)=\sum_{n\geq 1}a_n(\mathsf{E})n^{-s}$ and define $f_{\mathsf{E}}(z)=\sum_{n\geq 1}a_n(\mathsf{E})q^n$. Define the *conductor of the elliptic curve* N_{E} as follows

$$N_{\mathsf{E}}=\prod_{p \text{ bad}} p^{f_p} \text{ where } f_p=\begin{cases} 1 & \text{if } \mathsf{E} \text{ has multiplicative reduction at } p,\\ 2 & \text{if } \mathsf{E} \text{ has additive reduction at } p\neq 2,3,\\ 2+\delta_p & \text{if } \mathsf{E} \text{ has additive reduction at } p=2,3.\end{cases}$$

We will not define δ_p here; see [51, Section IV.10]. If $f_{\mathsf{E}}(z)$ is a modular form of weight 2 for $\Gamma_0(N_{\mathsf{E}})$ then we say that $\mathsf{E}/\mathbb{Q}$ is *modular*. By the work of Richard Taylor and Andrew Wiles [56, 61] we know that every semi-stable elliptic curve is modular. Subsequent work by Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor [7] showed that every rational elliptic curve is modular. Thus, $L(\mathsf{E},s)$ converges uniformly for $\Re(s)>3/2$, has analytic continuation to the entire complex plane, and satisfies a functional equation. If the order of vanishing[11] of $L(\mathsf{E},1)$ is r, then we say that the elliptic curve $\mathsf{E}/\mathbb{Q}$ has analytic rank $r_{\mathsf{E}}^{\text{an}}$.

4.3. **Birch and Swinnerton-Dyer Conjecture.** We now explain the conjectural link between the algebraic rank r_{E} introduced in Lecture 1 and $r_{\mathsf{E}}^{\text{an}}$.

Conjecture. Let $\mathsf{E}/\mathbb{Q}$ be a rational elliptic curve and $L(\mathsf{E},s)$ be the associated L-function.

- $L(\mathsf{E},s)$ has a zero at $s=1$ of order $r=r_{\mathsf{E}}^{\text{an}}$ equal to the (algebraic) rank r_{E} of $\mathsf{E}(\mathbb{Q})$.
- The residue of $L(\mathsf{E},s)$ at $s=1$ has an explicit expression in terms of invariants of $\mathsf{E}/\mathbb{Q}$. More precisely,

$$\frac{L^{(r)}(\mathsf{E},1)}{r!}=\frac{\#Ш(\mathsf{E}/\mathbb{Q})\cdot\Omega_{\mathsf{E}}\cdot \mathrm{Reg}_{\mathsf{E}}\cdot\prod_{p \text{ bad}} c_p}{\#(\mathsf{E}(\mathbb{Q})_{\text{tors}})^2}.$$

  Here, Ω_{E} is the real period of E multiplied by the number of connected components of $\mathsf{E}(\mathbb{R})$. The elliptic regulator $\mathrm{Reg}_{\mathsf{E}}$ is defined via the canonical heights of a basis of rational points. Finally, $\prod_{p|N_{\mathsf{E}}} c_p$ is the Tamagawa number and is calculated by Tate's Algorithm.

4.3.1. *Progress towards BSD.*

(1) John Coates and Andrew Wiles [10] used Iwasawa Theory to prove that if E/F is an elliptic curve with complex multiplication by an imaginary quadratic field K of class number 1, i.e., $F=K$ or $\mathbb{Q}$, and $L(\mathsf{E},s)\neq 0$ then $\mathsf{E}(F)$ is finite. This was extended to the case where F/K is a finite abelian extension by Nicole Arthaud [3].
(2) The Gross–Zagier Theorem [21] asserts that if a modular elliptic curve over $\mathbb{Q}$ has a first-order zero at $s=1$, then it has a rational point of infinite order.
(3) Victor Kolyvagin [30] showed that a modular elliptic curve $\mathsf{E}/\mathbb{Q}$ for which $L(\mathsf{E},1)\neq 0$ has algebraic rank 0 and if $L(\mathsf{E},1)$ has a first order zero then it has algebraic rank 1.
(4) Karl Rubin [47] showed that for CM elliptic curves E/K (with complex multiplication by imaginary quadratic field K), if $L(\mathsf{E},1)\neq 0$, then the p-part of the Shafarevich–Tate group has the order predicted by BSD.
(5) Work of Manjul Bhargava and Arul Shankar [5, 6] (combined with that of Jan Nekovář [42], Tim and Vlad Dokchitser [14], Chris Skinner and Eric Urban [53]) implies that BSD is true for a positive proportion of rational elliptic curves.

5. Lecture 5: p-adic L-Functions and Iwasawa Theory of Elliptic Curves

Classical Iwasawa theory was introduced in the 1950's by Kenkichi Iwasawa [23, 24, 25, 26] in the context of class groups of $\mathbb{Z}_p$-extensions of number fields. The Iwasawa Main Conjecture proposed

[11] If $L^{(r)}(\mathsf{E},1)\neq 0$ but $L^{(k)}(\mathsf{E},1)=0$ for all $k<r$.

a connection between the p-adic L-functions of Tobio Kubota and Heinrich-Wolfgang Leopoldt and these class groups. This Main Conjecture was proved by Barry Mazur and Andrew Wiles [37].

In the 1970's, Barry Mazur [35] extended the ideas of Iwasawa theory to elliptic curves and recast it in the language of Selmer groups. Since then, Ralph Greenberg extended these ideas to other p-adic Galois representations [17]. In each setting, there is a Main Conjecture (often conjectural) that relates Galois cohomology groups (the algebraic side) with p-adic L-functions (the analytic side). Furthermore, these Main Conjectures have consequences for the (expected) related special value formulas. For elliptic curves, this include the p-part of the Birch and Swinnerton-Dyer formula when the analytic rank is at most one.

5.1. **Iwasawa Theory.** *Here, we will only treat the simplest setting.* Fix a prime[12] $p > 2$. We write $\mathbb{Q}_{\text{cyc}}$ to denote the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. This is the maximal totally real pro-p subfield of $\bigcup_n \mathbb{Q}(\zeta_{p^n})$ where ζ_{p^n} denotes a primitive p^n-th root of unity. In particular, there is a tower

$$\mathbb{Q} = \mathbb{Q}_{(0)} \subset \mathbb{Q}_{(1)} \subset \ldots \subset \mathbb{Q}_{\text{cyc}}$$

such that each $\mathbb{Q}_{(n)}$ is the totally real subfield of $\mathbb{Q}(\zeta_{p^{n+1}})$ with $\text{Gal}(\mathbb{Q}_{(n)}/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$. By infinite Galois theory,

$$\Gamma = \text{Gal}(\mathbb{Q}_{\text{cyc}}/\mathbb{Q}) \simeq \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p.$$

5.1.1. *Iwasawa algebra.* Define the *Iwasawa algebra* $\Lambda = \Lambda(\Gamma)$ as the completed group algebra $\mathbb{Z}_p[\![\Gamma]\!] := \varprojlim_n \mathbb{Z}_p[\Gamma/\Gamma^{p^n}]$. Fix a topological generator γ of Γ; this gives an isomorphism of rings

$$\begin{aligned} \Lambda &\xrightarrow{\sim} \mathbb{Z}_p[\![x]\!] \\ \gamma &\mapsto 1 + x. \end{aligned}$$

Let M be a finitely generated torsion Λ-module. The *structure theorem of Λ-modules* [58, Theorem 13.12] asserts that M is pseudo-isomorphic[13] to a finite direct sum of cyclic Λ-modules,

$$M \sim \left(\bigoplus_{i=1}^{s} \Lambda/\langle p^{m_i} \rangle \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/\langle f_j(x) \rangle \right).$$

Here, $m_i > 0$ and $f_j(x)$ is a distinguished polynomial (i.e. a monic polynomial with non-leading coefficients divisible by p). The *characteristic ideal* of M denoted by $\text{char}_\Lambda(M)$ is (up to a unit) generated by the characteristic element,

$$f_M^{(p)}(x) := p^{\sum_i m_i} \prod_j f_j(x).$$

For ease of notation, we often write $f(x) = f_M^{(p)}(x)$. The μ-invariant of M is defined as the power of p in $f_{\text{M}}^{(p)}(x)$. More explicitly,

$$\mu(M) = \mu_p(M) := \begin{cases} 0 & \text{if } s = 0 \\ \sum_{i=1}^{s} m_i & \text{if } s > 0. \end{cases}$$

The λ-invariant of M is the degree of the characteristic element, i.e.

$$\lambda(M) = \lambda_p(M) := \sum_{j=1}^{t} \deg f_j(x).$$

[12] Many definitions require slight modification when $p = 2$ and some of the claims made in this section are known/expected to be true only when p is odd.

[13] By this we mean we have a homomorphism $M \to N$ with finite kernel and cokernel.

5.1.2. *Selmer groups.* For our purposes, the object of interest will be the p-primary Selmer group of E over $\mathbb{Q}_{\text{cyc}}$. We defined the p-Selmer group in §1.6.2. Let F be any number field. The p^∞-Selmer group of E is obtained by taking the direct limits over n of the p-power Selmer groups

$$\text{Sel}_{p^\infty}(\mathsf{E}/F) \coloneqq \varinjlim_n \text{Sel}^{(p^n)}(\mathsf{E}/F).$$

Equivalently, it can be defined directly

$$\text{Sel}_{p^\infty}(\mathsf{E}/F) \coloneqq \ker\left(H^1(F, \mathsf{E}[p^\infty]) \longrightarrow \prod_v H^1(F_v, \mathsf{E})[p^\infty]\right).$$

Write Σ to denote the set of primes in F containing the primes above p, the primes above those of bad reduction of $\mathsf{E}/\mathbb{Q}$, and the archimedean primes. Set $G_{F,\Sigma} = \text{Gal}(F_\Sigma/F)$ where F_Σ is the maximal unramified outside Σ extension of F and denote the local Kummer map by κ_v. Then the p^∞-Selmer group can be written as

$$\text{Sel}_{p^\infty}(\mathsf{E}/F) \coloneqq \ker\left(H^1(G_{F,\Sigma}, \mathsf{E}[p^\infty]) \longrightarrow \prod_{\substack{v\in\Sigma \\ v\nmid p}} H^1(F_v, \mathsf{E}[p^\infty]) \times \prod_{v|p} H^1(F_v, \mathsf{E}[p^\infty])/\,\text{image}(\kappa_v)\right).$$

Taking the direct limit over the fundamental exact sequences for the multiplication-by-p^n maps yields the fundamental exact sequence for the p^∞-Selmer groups

$$0 \longrightarrow \mathsf{E}(F)\otimes\mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \text{Sel}_{p^\infty}(\mathsf{E}/F) \longrightarrow Ш(\mathsf{E}/F)[p^\infty] \longrightarrow 0.$$

The most natural way to define the Selmer group over $\mathbb{Q}_{\text{cyc}}$ is

$$\text{Sel}_{p^\infty}(\mathsf{E}/\mathbb{Q}_{\text{cyc}}) \coloneqq \varinjlim_n \text{Sel}_{p^\infty}(\mathsf{E}/\mathbb{Q}_{(n)}).$$

We often drop the notation p^∞ since p is fixed. Define the Pontryagin dual of the Selmer group as

$$X(\mathsf{E}/\mathbb{Q}_{\text{cyc}}) = \text{Hom}_{\text{cts}}(\text{Sel}(\mathsf{E}/\mathbb{Q}_{\text{cyc}}), \mathbb{Q}_p/\mathbb{Z}_p).$$

It follows from a standard argument using the topological Nakayama's Lemma that $X(\mathsf{E}/\mathbb{Q}_{\text{cyc}})$ is finitely generated as a Λ-module. When p is a prime of good ordinary reduction, then $X(\mathsf{E}/\mathbb{Q}_{\text{cyc}})$ is Λ-torsion [19, Theorem 1.5]. However, when p is a prime of good supersingular reduction, then $X(\mathsf{E}/\mathbb{Q}_{\text{cyc}})$ is not Λ-torsion [9, Theorem 2.6] and to obtain arithmetic information it becomes pertinent to work with modified Selmer groups.

5.1.3. *Algebraic Aspects.* We fix an elliptic curve $\mathsf{E}/\mathbb{Q}$ and a prime p of good ordinary reduction. By the discussion in the previous section, we may use the Structure Theorem to define the characteristic ideal $\text{char}_\Lambda(X)$, where we write $X = X(\mathsf{E}/\mathbb{Q}_{\text{cyc}})$. Write $f_{\mathsf{E}}(x)$ to denote the generator of this characteristic ideal. Then

Lemma 5.1. Fix a rank 0 elliptic curve $\mathsf{E}/\mathbb{Q}$ and a prime p of good ordinary reduction. Suppose that $Ш(\mathsf{E}/\mathbb{Q})[p^\infty]$ is finite. Then

$$f_{\mathsf{E}}(0) \sim_p \frac{\#Ш(\mathsf{E}/\mathbb{Q})[p^\infty]\cdot(\#\widetilde{\mathsf{E}}(\mathbb{F}_p)[p^\infty])^2\cdot\prod_{\ell|N_{\mathsf{E}}} c_\ell^{(p)}}{(\#\mathsf{E}(\mathbb{Q})[p^\infty])^2},$$

where the notation $a \sim_p b$ means that a and b have the same p-adic valuation.

This will probably remind the reader of the BSD-formula. Writing $\alpha_p, \beta_p \in \overline{\mathbb{Q}}$ to be the roots of the characteristic polynomial (5) of the reduced curve, we know that $a_p(\mathsf{E}) = \alpha_p + \beta_p$ and $\alpha_p\beta_p = p$.

Choosing α_p to be the p-adic unit under the fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$, we have $\alpha_p^{-1} = \beta_p p^{-1}$. Indeed, it is conjectured that in the setting of the previous lemma

$$f_{\mathsf{E}}(0) \sim_p \frac{(1-\beta_p p^{-1})^2 L(\mathsf{E},1)}{\Omega_{\mathsf{E}}}.$$

By definition, the regulator is trivial for rank 0 curves and does not appear in the formula.

Exercise 5.2. Show that $p \mid \#\widetilde{\mathsf{E}}(\mathbb{F}_p)$ if and only if $a_p(\mathsf{E}) \equiv 1 \pmod{p}$.

Exercise 5.3. Show that $\#\widetilde{\mathsf{E}}(\mathbb{F}_p)[p^\infty] \sim_p (1-\beta_p p^{-1})$.

A natural question to ask is whether the group $\mathrm{Sel}(\mathsf{E}/\mathbb{Q})$ can be recovered from $\mathrm{Sel}(\mathsf{E}/\mathbb{Q}_{\mathrm{cyc}})$. In this direction, we have the following result [18, Theorem 4.1]

Theorem 5.4 (Mazur's Control Theorem)**.** The natural maps

$$\mathrm{Sel}(\mathsf{E}/\mathbb{Q}_{(n)}) \longrightarrow \mathrm{Sel}(\mathsf{E}/\mathbb{Q}_{\mathrm{cyc}})^{\Gamma_n},$$

where $\Gamma_n = \mathrm{Gal}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}_{(n)})$ have finite kernels and cokernels. Moreover, their orders are bounded independent of n.

5.1.4. *Analytic Aspects.* Fix a primitive p^t-th root of unity ζ. Define

$$\psi_\zeta : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \Gamma \longrightarrow \overline{\mathbb{Q}_p}^\times,$$

to be the finite order character sending $\gamma \mapsto \zeta$. We also use it to denote the Dirichlet character $(\mathbb{Z}/p^{t+1}\mathbb{Z})^\times$ such that the image of $\gamma \in 1+p\mathbb{Z}_p$ is sent to ζ (unless $t=0$). Write $\phi_\zeta : \Lambda \to \mathbb{Z}_p[\zeta]$ to denote a homomorphism sending $\gamma \mapsto \zeta$ (or equivalently $x \mapsto \zeta - 1$).

The p-adic L-function of f_{E} denoted by $\mathcal{L}(\mathsf{E}/\mathbb{Q}_{\mathrm{cyc}})$ is an element of Λ that interpolates special values of the classical Hasse–Weil L-function $L(f_{\mathsf{E}}, s)$ at integer points, usually twisted by Dirichlet characters. This was first defined by Yvette Amice and Jacques Vélu [2] and Misha Vishik [57]. In the last lecture we saw the L-function associated with f_{E}. Twisting f_{E} by the Dirichlet character ψ_ζ^{-1}, we can define the twisted L-function $L(f_{\mathsf{E}}, \psi_\zeta^{-1}, s)$. Define

$$e_p(\zeta) \coloneqq \begin{cases} \alpha_p^{-(t+1)} \frac{p^{t+1}}{G(\psi_\zeta^{-1})} & \text{if } \zeta \neq 1, \\ \alpha_p^{-1}\left(1 - \frac{1}{\alpha_p}\right)^2 & \text{if } \zeta = 1. \end{cases}$$

Here, $G(\psi_\zeta^{-1})$ is the Gauss sum. Then the p-adic L-function satisfies

$$\phi_\zeta(\mathcal{L}(\mathsf{E}/\mathbb{Q}_{\mathrm{cyc}})) = e_p(\zeta)\frac{L(f_{\mathsf{E}}, \psi_\zeta^{-1}, 1)}{\Omega_{\mathsf{E}}}.$$

It is probably not surprising that there is a p-adic analogue of the BSD Conjecture. In particular, we may consider the series expansion of the p-adic L-function constructed above, which we denote by $\mathcal{L}^*(\mathsf{E}, x)$. The order of vanishing $\mathrm{ord}_x(\mathcal{L}^*(\mathsf{E}, x))$ at $x = 0$ is equal to the (algebraic) rank r_{E} of $\mathsf{E}(\mathbb{Q})$ if E has good ordinary reduction at p. Moreover, the leading term of the series expansion of the p-adic L-function has a concrete expression in terms of the invariants of $\mathsf{E}/\mathbb{Q}$,

$$\mathcal{L}^*(\mathsf{E}, 0) = \frac{\#Ш(\mathsf{E}/\mathbb{Q}) \cdot (1-\alpha_p^{-1})^2 \cdot \mathrm{Reg}_{\mathsf{E}}^{(p)} \cdot \prod_{q \mid N_{\mathsf{E}}} c_q}{\#(\mathsf{E}(\mathbb{Q})_{\mathrm{tors}})^2}.$$

The classical and p-adic BSD conjectures share many of the same arithmetic quantities; the main difference is that the regulator and L-series are replaced with their p-adic analogues.

5.2. **Greenberg-Iwasawa Main Conjecture.** We can now define the Main Conjecture

Conjecture. Suppose $\mathsf{E}/\mathbb{Q}$ has good ordinary reduction at p. The dual Selmer group $X(\mathsf{E}/\mathbb{Q}_{\text{cyc}})$ is a torsion Λ-module and its characteristic ideal $\text{char}_\Lambda(X)$ is generated by $\mathcal{L}(\mathsf{E}/\mathbb{Q}_{\text{cyc}})$ in $\Lambda \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

One divisibility is often proven using Euler systems (e.g., Kato's Euler system), which shows that the p-adic L-function divides the characteristic ideal of the Selmer group. The reverse inclusion often uses techniques like Ribet's Lemma or congruences between Eisenstein series and modular forms (for example, the work of Chris Skinner and Eric Urban).

5.2.1. *Progress in this direction.*

(1) The Main Conjecture for a CM elliptic curve with ordinary reduction at p was proved by Karl Rubin [46, 47].
(2) Ralph Greenberg and Vinayak Vatsal [20] exploited Kato's one divisibility and the classical Main Conjecture for Dirichlet characters to deduce the cyclotomic Main Conjecture for some elliptic curves $\mathsf{E}/\mathbb{Q}$ for which $\mathsf{E}[p]$ is a reducible $G_{\mathbb{Q}}$-representation.
(3) Works of Kazuya Kato [29] and Chris Skinner and Eric Urban [53] resolve the conjecture when $\mathsf{E}[p]$ is irreducible and there exists $\ell \,||\, N_{\mathsf{E}}$ such that $\mathsf{E}[p]$ is ramified at ℓ.

Acknowledgements

These lecture notes were prepared for a mini-course on 'Algebraic and Analytic Aspects of Elliptic Curves' at PUC Chile as a part of GARLAT 2026. DK thanks the organizers for this opportunity and for their support. She was partially funded by the NSERC Discovery Grant RGPIN-2026-07384. She thanks the students for all their comments and questions during the lectures, which has greatly helped improve the exposition.

References

[1] L. Alpöge, M. Bhargava, W. Ho, and A. Shnidman. Rank stability in quadratic extensions and Hilbert's tenth problem for the ring of integers of a number field. *Invent. math.*, 243(3):1129–1139, 2026.
[2] Y. Amice and J. Vélu. Distributions p-adiques associées aux séries de Hecke. In *Journées Arithmétiques de Bordeaux (Conf., Univ. Bordeaux, Bordeaux, 1974)*, volume 24, page 119, 1975.
[3] N. Arthaud. On Birch and Swinnerton-Dyer's conjecture for elliptic curves with complex multiplication. I. *Compositio Math.*, 37(2):209–232, 1978.
[4] T. Barnet-Lamb, D. Geraghty, M. Harris, and R. Taylor. A family of Calabi–Yau varieties and potential automorphy II. *Publ. Res. Inst. Math. Sci.*, 47(1):29–98, 2011.
[5] M. Bhargava and A. Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *Annals of Mathematics*, pages 191–242, 2015.
[6] M. Bhargava and A. Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Annals of Mathematics*, pages 587–621, 2015.
[7] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939, 2001.
[8] L. Clozel, M. Harris, and R. Taylor. Automorphy for some l-adic lifts of automorphic mod l Galois representations. *Publ. Math. IHÉS*, 108(1):1–181, 2008.
[9] J. Coates and R. Sujatha. *Galois cohomology of elliptic curves*. Narosa, New Delhi, India, 2000.
[10] J. Coates and A. Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Invent. math.*, 39(3):223–251, 1977.
[11] M. Davis and H. Putnam. *Diophantine sets over polynomial rings*. New York University, Institute of Mathematical Sciences, 1961.
[12] M. Davis, H. Putnam, and J. Robinson. The decision problem for exponential Diophantine equations. *Ann. Math.*, pages 425–436, 1961.
[13] F. Diamond and J. M. Shurman. *A first course in modular forms*, volume 228. Springer, 2005.
[14] T. Dokchitser and V. Dokchitser. On the Birch–Swinnerton-Dyer quotients modulo squares. *Ann. Math.*, pages 567–596, 2010.
[15] N. D. Elkies. The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$. *Invent. math.*, 89(3):561–567, 1987.

[16] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent, math.*, 73(3):349–366, 1983.
[17] R. Greenberg. Iwasawa theory for p-adic representations. *Adv. Stud. Pure Math.*, 17:97–137, 1989.
[18] R. Greenberg. Introduction to Iwasawa theory for elliptic curves. *Arithmetic algebraic geometry. IAS/Park City Math. Ser*, 9:407–464, 1999.
[19] R. Greenberg. Iwasawa theory for elliptic curves. In *Arithmetic theory of elliptic curves (Cetraro, 1997)*, volume 1716 of *Lecture Notes in Math.*, pages 51–144. Springer, Berlin, 1999.
[20] R. Greenberg and V. Vatsal. On the Iwasawa invariants of elliptic curves. *Invent. Math.*, 142(1):17–63, 2000.
[21] B. H. Gross and D. B. Zagier. Heegner points and derivatives of L-series. *Invent. math.*, 84(2):225–320, 1986.
[22] M. Harris, N. Shepherd-Barron, and R. Taylor. A family of Calabi-Yau varieties and potential automorphy. *Ann. Math.*, pages 779–813, 2010.
[23] K. Iwasawa. A note on class numbers of algebraic number fields. In *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, volume 20, pages 257–258. Springer, 1956.
[24] K. Iwasawa. On some invariants of cyclotomic fields. *Am. J. Math.*, 80(3):773–783, 1958.
[25] K. Iwasawa. On Γ-extensions of algebraic number fields. *Bull. Amer. Math. Soc.*, 65(4):183–226, 1959.
[26] K. Iwasawa. On the theory of cyclotomic fields. *Ann. Math.*, 70(3):530–561, 1959.
[27] S. Kamienny. Torsion points on elliptic curves over all quadratic fields. *Duke Math. J.*, 53(1):157–162, 1986.
[28] S. Kamienny, B. Mazur, and A. Granville. Rational torsion of prime order in elliptic curves over number fields. *Astérisque*, 228(3):81–100, 1995.
[29] K. Kato. p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, 295:117–290, 2004.
[30] V. Kolyvagin. Finiteness of $E(\mathbf{Q})$ and $Ш(E, \mathbf{Q})$ for a subclass of Weil curves. *Izvestiya: Mathematics*, 32(3):523–541, 1989.
[31] P. Koymans and C. Pagano. Hilbert's tenth problem via additive combinatorics, 2024. arXiv preprint arXiv:2412.01768.
[32] S. Lang and H. Trotter. Primitive points on elliptic curves. *Bull. Amer. Math. Soc.*, 83(6):289–292, 1977.
[33] E. Lutz. Sur l'équation $y^2 = x^3 - ax - b$ dans les corps p-adiques. *Journal für die reine und angewandte Mathematik*, 177:238–247, 1937.
[34] Y. Matijasevic. Enumerable sets are Diophantine. In *Soviet Math. Dokl.*, volume 11, pages 354–358, 1970.
[35] B. Mazur. Rational points of abelian varieties with values in towers of number fields. *Invent. math.*, 18(3):183–266, 1972.
[36] B. Mazur. Modular curves and the Eisenstein ideal. *Publ. Math. IHÉS*, 47(1):33–186, 1977.
[37] B. Mazur and A. Wiles. Class fields of abelian extensions of $\mathbb{Q}$. *Invent. math.*, 76:179–330, 1984.
[38] L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. math.*, 124(1):437–450, 1996.
[39] L. J. Mordell. On the rational resolutions of the indeterminate equations of the third and fourth degree. *Proc. Cambridge Phil. Soc.*, 21:179–192, 1922.
[40] M. R. Murty and V. K. Murty. The sato-tate conjecture and generalizations. *Current Trends in Science: Platinum Jubilee Special*, pages 639–646, 2009.
[41] T. Nagell. *Solution de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre.* Number 1. I kommisjon hos Jacob Dybwad, 1936.
[42] J. Nekovář. On the parity of ranks of Selmer groups IV. with an appendix by Jean-Pierre Wintenberger. *Compositio Math.*, 145(6):1351–1359, 2009.
[43] J. Park, B. Poonen, J. Voight, and M. M. Wood. A heuristic for boundedness of ranks of elliptic curves. *J. Eur. Math. Soc.*, 21(9), 2019.
[44] B. Poonen. Using elliptic curves of rank one towards the undecidability of Hilbert's tenth problem over rings of algebraic integers. In *International Algorithmic Number Theory Symposium*, pages 33–42. Springer, 2002.
[45] J. Robinson. Unsolvable Diophantine problems. *Proc. Amer. Math. Soc.*, 22(2):534–538, 1969.
[46] K. Rubin. On the main conjecture of Iwasawa theory for imaginary quadratic fields. *Invent. Math.*, 93(3):701–713, 1988.
[47] K. Rubin. The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Invent. Math.*, 103(1):25–68, 1991.
[48] E. S. Selmer. The diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Math.*, 85(1):203–362, 1951.
[49] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Publ. Math. IHÉS*, 54:123–201, 1981.
[50] A. Shlapentokh. Elliptic curves retaining their rank in finite extensions and Hilbert's tenth problem for rings of algebraic numbers. *Trans. Amer. Math. Soc.*, 360(7):3541–3555, 2008.
[51] J. H. Silverman. Advanced topics in the arithmetic of elliptic curves. *Graduate Texts in Mathematics*, 151, 1994.
[52] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2009.
[53] C. Skinner and E. Urban. The Iwasawa main conjectures for GL_2. *Invent. Math.*, 195(1):1–277, 2014.

[54] J. T. Tate. Algebraic cycles and poles of zeta functions. In *Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963)*, pages 93–110. Harper & Row, 1965.
[55] R. Taylor. Automorphy for some l-adic lifts of automorphic mod l Galois representations. II. *Publ. Math. IHÉS*, 108(1):183–239, 2008.
[56] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. Math.*, 141(3):553–572, 1995.
[57] M. M. Visik. Nonarchimedean measures associated with Dirichlet series. *Mat. Sb.(NS)*, 99(141):248–260, 1976.
[58] L. C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.
[59] L. C. Washington. *Elliptic curves: number theory and cryptography*. Chapman and Hall/CRC, 2008.
[60] A. Weil. L'arithmétique sur les courbes algébriques. *Acta mathematica*, 52(1):281–315, 1929.
[61] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. Math.*, 141(3):443–551, 1995.

Department of Mathematics and Statistics, University of Regina, Saskatchewan, Canada
Email address: debanjana.kundu@uregina.ca