A FRIENDLY INTRODUCTION TO THE RESULTS OF GROSS–ZAGIER

MATIJA TAPUŠKOVIĆ AND JAN VONK

Contents

These are the notes for the first two talks at the Gross–Zagier seminar at Oxford, October 2018. They were hastily written, and poorly proofread. I would be grateful for any corrections or suggestions! In this talk, we will give a very friendly introduction to the objects and statements involved in the theorem of Gross–Zagier, based on one single example. This is essentially what is done in [Zag85] where the elliptic curve $\texttt{37.a1}$ is investigated. To make sure we do not get lulled into a false sense of understanding by following Zagier's computations, we will instead consider the curve $\texttt{61.a1}$ and do all the computations from scratch.

The notes are structured around the computation of this example, and the aim is to introduce some of the main objects involved in the work of Gross–Zagier and Gross–Kohnen–Zagier guided by our excursions around $\texttt{61.a1}$. Whenever some object is introduced, we take the time to define everything precisely, and assume little to no familiarity with the subject. During the talk, definitions will be inserted as they are needed, but for the purpose of a smooth narrative, they have been collected in the appendices in this document.

1. The elliptic curve $E = \texttt{61.a1}$ and its L-series

Let us consider the elliptic curve with Weierstraß equation

$$E : y^2 + xy = x^3 - 2x + 1 \tag{1}$$

which has label $\texttt{61.a1}$ in Cremona's database. Clearly, it is defined over $\mathbf{Q}$, and its conductor is 61. We will now study some invariants of this elliptic curves over various base fields.

Date: October 2018.

1.1. **The curve E over $\mathbf{C}$.**

We now compute some of the invariants of the curve E over $\mathbf{C}$, most importantly its periods, which we do numerically. First, the variable transformation $y \mapsto 2y + x$ gives us the following model for E:

$$E : y^2 = 4x^3 + x^2 - 8x + 4 \tag{2}$$

Now let us compute approximate generators for the lattice of periods Λ. The cubic polynomial on the right hand side of the model (2) has precisely one real root, which is approximately

$$\gamma = -1.73497012425858 \tag{3}$$

and we get the following picture of $E(\mathbf{R})$:

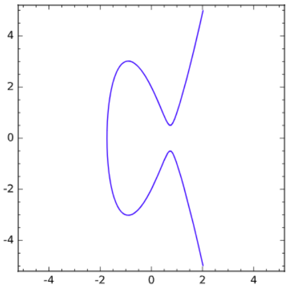

Figure 1. The set $E(\mathbf{R})$ for the model $y^2 = 4x^3 + x^2 - 8x + 4$

On the minimal Weierstraß model (1), the Néron differential is $dx/(2y + x)$, which is the differential dx/y in the model (2). We now compute numerically that

$$\begin{aligned} \Omega_E^+ &= 2\int_\gamma^\infty \frac{dx}{\sqrt{4x^3 + x^2 - 8x + 4}} \\ &\approx 6.13319314839454 \end{aligned} \tag{4}$$

is an approximation of the real period of E. Likewise, we may compute the complex period by numerically computing the two other conjugate roots

$$\alpha, \beta = 0.742485062129292 \pm 0.158413173442297i$$

and then

$$\begin{aligned} \Omega_E^- &= 2\int_\beta^\gamma \frac{dx}{\sqrt{4x^3 + x^2 - 8x + 4}} \\ &\approx 3.06659657419727 + 0.997205478384470i \end{aligned} \tag{5}$$

Finally, we record some of the invariants of the lattice of periods. By putting E in short Weierstraß form, which can be done by completing the cube on the right hand side of the model (2), we can read off the *exact* values of the Eisenstein series G_4 and G_6 on this lattice. That is, from the theory of Weierstraß uniformisation, it follows that

$$\begin{cases} 60G_4(\Lambda) = 10476 = 2^2 \cdot 3^3 \cdot 97 \\ 140G_6(\Lambda) = -217944 = -2^3 \cdot 3^3 \cdot 1009 \end{cases} \tag{6}$$

1.2. **The curve E over $\mathbf{F}_p$.** Let us consider a finite prime p and investigate the reduction of E modulo p. The curve E has good reduction at $p \neq 61$, and for $p = 61$ we reduce the equation (2) and do a simple change of variables to move the singular point to the origin, which yields an integral model

$$E_{\mathbf{Z}} : y^2 = 4x^3 + 433x^2 + 61 \cdot 2^8 x + 61 \cdot 2^2 \cdot 769. \tag{7}$$

This model clearly reduces to a nodal curve at 61. The singularity is regular, since the constant coefficient has 61-adic valuation 1. The equation of the reduction is

$$y^2 = 4x^3 + 6x^2 \tag{8}$$

The tangent lines at the singularity modulo 61 have slopes $\pm\sqrt{6}$, and are hence not defined over $\mathbf{F}_{61}$ so that the reduction is non-split multiplicative. This means that the Tamagawa number at 61, and hence at any prime, is trivial. Furthermore, the local root numbers are all 1, so the L-series of E should vanish at $s = 1$. We will prove in the next section (without using the modularity theorem) that it does vanish, to order 1.

By counting points modulo small primes, we obtain the first few terms of the L-function of E:

$$\begin{aligned} \mathrm{L}_E(s) &= (1 + 61^{-s})^{-1} \times \prod_{p \neq 61} \left(1 + a_p p^{-s} + p^{1-2s}\right)^{-1} \\ &= 1 - \frac{1}{2^s} - \frac{2}{3^s} - \frac{1}{4^s} - \frac{3}{5^s} + \frac{2}{6^s} + \frac{1}{7^s} + \frac{3}{8^s} + \frac{1}{9^s} + \frac{3}{10^s} - \frac{5}{11^s} + \dots \end{aligned} \tag{9}$$

If we compute the space of modular forms on $\Gamma_0(61)$, we find a newform whose q-expansion begins with

$$f(q) = q - q^2 - 2q^3 - q^4 - 3q^5 + 2q^6 + q^7 + 3q^8 + q^9 + 3q^{10} - 5q^{11} + \dots \tag{10}$$

These coefficients certainly seem to agree with those of $\mathrm{L}_E(s)$! If we use the modularity theorem of Wiles, we may turn this observation into a rigorous proof that *all* the coefficients agree, not just the finitely many we computed. But of course it's ridiculous to invoke the full strength of modularity when one is working with a concrete example! We will *prove* modularity of E in the next section via a direct calculation.

1.3. **The curve E over $\mathbf{Q}$.** In this subsection, we again use the global minimal model

$$E : y^2 + xy = x^3 - 2x + 1 \tag{11}$$

First, it is easy to check that $E(\mathbf{Q})$ is torsion-free. Indeed, the prime to p torsion injects into the group of points on E modulo any $p \neq 61$. Looking at the point counts that went into (9), we see that there are 4 points on E modulo 2, and 9 points modulo 5, which implies there can't be any torsion.

To determine the rank, one can use the method of descent via isogeny. I confess that I did not do this explicitly from scratch, since it is likely to be a messy calculation, but I encourage you to try! Using the routines in `Sage` or `Magma` we can show (provably) that

$$E(\mathbf{Q}) = \langle (1, -1) \rangle \simeq \mathbf{Z} \tag{12}$$

so that E is of rank 1 over $\mathbf{Q}$. Moreover, the generator $P = (1, -1)$ of the Mordell–Weil group has a canonical height that may readily be computed via Tate's algorithm. In fact, I was too lazy to implement that from scratch, and didn't want to use anything that was already implemented, so I just used the naive expression

$$h(P) = \lim_{n \to \infty} \log\left(h_{\text{naive}}(2^n P)\right) / 4^n \tag{13}$$

where the naive height on the right hand side is just the maximum of the absolute values of the numerator and denominator of the x-coordinate of the point. This is quite terrible from a computational viewpoint, but seemed to converge fast enough if we just want a few digits. I obtained

$$h(P) = 0.079187731362 \tag{14}$$

which seems to agree with what the professionals compute, though this did take a while to get right to that precision. Anyways, it's good enough for us!

2. The modularity of E

We show that E is modular, and deduce from it a number of statements about the L-series of E. The computations in this section will be used later, notably when we compute Heegner points on E.

2.1. **Verifying modularity for E.**

We start by verifying that E is modular. Recall that in (10) we found that there was a newform f whose first few coefficients agree with the coefficients of the L-series of E.

This can be done in two different ways, both of which have their merits. The first is via an algebraic computation and uses the fact that classical spaces of modular forms may be computed efficiently via the theory of modular symbols (which is not discussed here). The second is an analytic computation of the uniformisation map, which proves modularity by establishing the equality of the two lattices of periods.

2.1.1. *Method 1:* Consider the congruence subgroup $\Gamma_0(61)^+$ which is generated by $\Gamma_0(61)$ and the matrix

$$w_{61} = \begin{pmatrix} 0 & -1/\sqrt{61} \\ \sqrt{61} & 0 \end{pmatrix} \tag{15}$$

We easily check that the quotient $X_0(61)^+ = \Gamma_0(61)^+ \backslash \mathfrak{H}$ is of genus 1, and has a unique cusp ∞, which is rational. We will show that $E \simeq X_0(61)^+$. To do this, it suffices to find two $\Gamma_0(61)^+$-invariant functions ξ and η on $\mathfrak{H}$ such that

$$\eta(\tau)^2 + \xi(\tau)\eta(\tau) = \xi(\tau)^3 - 2\xi(\tau) + 1 \tag{16}$$

This does not uniquely determine the functions ξ and η, so we impose in addition the condition

$$\frac{d\xi}{2\eta + \xi} = f(q)\frac{dq}{q} \tag{17}$$

where f is the modular form (10), which is allegedly attached to E. From these conditions, we may compute the first few terms of the q-expansions of ξ and η, provided they exist. We obtain

$$\left\{ \begin{array}{rcl} \xi(q) & = & q^{-2} + q^{-1} + 2 + 3q + 6q^2 + 7q^3 + 11q^4 + 16q^5 + 23q^6 + 30q^7 + \dots \\ \eta(q) & = & -q^{-3} - 2q^{-2} - 4q^{-1} - 7 - 13q - 22q^2 - 36q^3 - 54q^4 - 85q^5 - 126q^6 + \dots \end{array} \right. \tag{18}$$

Of course, this doesn't show that ξ and η exist! But if they do, their q-expansions start off like this. Now here's the trick. The weakly holomorphic forms ξf^2 and ηf^3 should be holomorphic modular forms of weights 4 and 6 respectively, and therefore lie in finite-dimensional spaces which are furthermore explicitly computable. We know how their q-expansions start off, so if we compute enough terms, we can uniquely find these modular forms after a finite computation. In this case, we compute that

$$\dim M_4(\Gamma_0(61)) = 17, \qquad \dim M_6(\Gamma_0(61)) = 27 \tag{19}$$

so it suffices to construct a basis for both spaces (which can be done via the theory of modular symbols) and find ξf^2 and ηf^3 explicitly. The condition on ξ and η is equivalent to a relation between modular forms of weights 12, which may be checked after a finite amount of computation. Of course, this can be done much more cleverly, already by simply taking the action of w_{61} into consideration and reducing the dimensions of the spaces involved, but the basic idea remains the same.

2.1.2. *Method 2:* The second method is analytic, and numerically computes the complex uniformisation of E. More precisely, define the function

$$\phi : \mathfrak{H} \longrightarrow \mathbf{C}/\Lambda', \qquad \tau \longmapsto 2\pi i \int_{\tau}^{i\infty} f(z)dz \tag{20}$$

where as before, f is the modular form found in (10), and Λ' is *some* lattice of periods, which we will show to be homothetic to the lattice of periods Λ of E. The function ϕ may be efficiently computed via the rapidly converging power series

$$\phi(\tau) = -q + \frac{1}{2}q^2 + \frac{2}{3}q^3 + \frac{1}{4}q^4 + \frac{3}{5}q^5 - \frac{1}{3}q^6 - \frac{1}{7}q^7 - \frac{3}{8}q^8 - \frac{1}{9}q^9 + \dots \tag{21}$$

It is clear that ϕ is almost Γ-invariant, in the sense that

$$\phi(\gamma\tau) - \phi(\tau) = \text{constant}. \tag{22}$$

This constant only depends on γ, and hence E induces an element of $\mathrm{H}^1(\Gamma, \mathbf{C})$. This is the subject of Eichler–Shimura theory, which (together with a result of Edixhoven) shows that

- The image of this morphism $\Gamma \to \mathbf{C}$ is the lattice of periods Λ',
- The constants $G_4(\Lambda')$ and $G_6(\Lambda')$ are integers.

By finding a set of generators for Γ, we can therefore approximate a pair of generators for the period lattice Λ' numerically, using the rapidly converging series 21. We obtain two generators

$$\left\{ \begin{array}{lcl} \Omega_1' & \approx & 1.02219885806576 \\ \Omega_2' & \approx & 0.511099429032878 + 0.166200913064078i \end{array} \right. \tag{23}$$

Then, we compute the constants $G_4(\Lambda')$ and $G_6(\Lambda')$, which we know to be integers, numerically up to some precision. By capping the double summation over Λ' to a box of size 2000, we obtain the approximations

$$\left\{ \begin{array}{lcl} 60G_4(\Lambda') & \approx & 10475.9998934 - 0.000046670i \\ 140G_6(\Lambda') & \approx & -217944.000000002 - .000000000089i \end{array} \right. \tag{24}$$

a careful precision analysis would show that the first few digits are significant, yielding a rigorous proof of the fact that $60G_4(\Lambda') = 10476$ and $140G_6(\Lambda') = -217944$, and hence that

$$\Lambda \sim \Lambda'.$$

This shows modularity of E.

2.2. **Consequences of modularity.** The statement *the elliptic curve E is modular* can be defined in one of many different ways, all of which are equivalent. For the purpose of our discussion, there are two viewpoints: One is an analytic statement about the coincidence of the L-functions attached to E and some modular form f, while the other is geometric in the sense that there is a finite cover $X_0(N) \to E$. It was the latter that was proved above, while it is the former that plays the most important role for the purpose of Gross–Zagier, and the explicit computations below.

Theorem 2.1. *Suppose E is an elliptic curve over $\mathbf{Q}$ of conductor N. Then the following are equivalent:*

- *There exists a newform $f \in S_2(\Gamma_0(N))$ such that $a_p(f) = a_p(E)$ for all p not dividing N,*
- *There exists a finite map $X_0(N) \longrightarrow E$ defined over $\mathbf{Q}$.*

Proof. A proof can be found, for instance, in Diamond–Shurman [DS05, Section 8.8]. □

If these equivalent conditions are fulfilled, we say that E is *modular*. It is known from the work of Wiles, and later Breuil–Conrad–Diamond–Taylor, that every elliptic curve over $\mathbf{Q}$ is modular. This result was not known at the time of the work of Gross–Zagier, but it could be checked efficiently for any particular example E, essentially using the method above.

For us, the main importance of this statement lies in the fact that the completed L-series

$$\widetilde{\mathrm{L}}_E(s) := 61^{s/2}(2\pi)^{-s}\Gamma(s)\mathrm{L}_E(s) \tag{25}$$

may be analytically continued to the entire complex plane $s \in \mathbf{C}$, through its integral representation

$$\widetilde{\mathrm{L}}_E(s) = \int_0^\infty f\left(\frac{i\tau}{\sqrt{61}}\right)\tau^{s-1}d\tau \tag{26}$$

$$= \int_1^\infty f\left(\frac{i\tau}{\sqrt{61}}\right)(\tau^{s-1} - \tau^{1-s})d\tau \tag{27}$$

First, we note that the fact that f is fixed by the Atkin–Lehner involution w_{61} implies that the completed L-function satisfies the functional equation

$$\widetilde{\mathrm{L}}_E(s) = -\widetilde{\mathrm{L}}_E(2-s) \tag{28}$$

which implies that $\widetilde{\mathrm{L}}_E(1) = 0$. If the value at $s = 1$ vanishes, it becomes natural to look at the derivative of the completed L-function at $s = 1$, which we expect to contain relevant information as predicted by the Birch–Swinnerton-Dyer conjecture. This quantity may be computed by differentiating the above integral representation, giving the expression

$$\left(\frac{d}{ds}\widetilde{\mathrm{L}}_E\right)(1) = 2\int_1^\infty f\left(\frac{i\tau}{\sqrt{61}}\right)\log(\tau)d\tau \tag{29}$$

$$= 2\sum_{n=1}^\infty a_n \int_1^\infty \log(\tau)\cdot\exp\left(-\frac{2n\pi\tau}{\sqrt{61}}\right)d\tau. \tag{30}$$

The above can be computed numerically, yielding

$$\left(\frac{d}{ds}\widetilde{\mathrm{L}}_E\right)(1) \approx 0.485673651427 \tag{31}$$

If we believe the Birch–Swinnerton-Dyer conjecture, this number should be equal to $\Omega^+ h(P_0)$, and indeed, using the numerical approximations above we get

$$\Omega^+ h(P_0) \approx 0.485673651427 \tag{32}$$

That's far from a proof of the Birch–Swinnerton-Dyer conjecture in this case, but it does make for compelling evidence, and a great sanity check that our computations so far are correct, or at the very least wrong in some consistent and minor way.

3. Heegner points on E

In this section, we establish some of the basic theory of Heegner points. We start with a discussion of the necessary background on quadratic orders, before we briefly recall CM theory and the definitions of Heegner points that are used in the work of Gross–Zagier. We note that in the literature the word *Heegner point* can mean different, closely related, things where various hypotheses are weakened, and one should always be careful when using the phrase.

3.1. **The arithmetic of quadratic orders.** Suppose $\mathcal{O}$ is an order in an imaginary quadratic field K. If $\mathcal{O}$ is not maximal, it is not a Dedekind domain, and therefore some care needs to be taken with class groups. We start by recording some necessary facts. Recall that the *Picard group* $\mathrm{Pic}(\mathcal{O})$ is defined to be the group of isomorphism classes of invertible sheaves on $\mathrm{Spec}(\mathcal{O})$, or otherwise said, the class group of Cartier divisors. In the context of an order $\mathcal{O}$, a Cartier divisor is better known under the name *fractional ideal.* We start by reviewing these definitions, and stating the relation with the class group of the maximal order.

Suppose that $\mathrm{disc}(\mathcal{O}) = \Delta c^2$, where Δ is a fundamental discriminant. We call $c > 0$ the *conductor* of the order $\mathcal{O}$. Let $\mathcal{O}_K$ be the ring of integers in K. If $\mathcal{O}_K$ has integral basis $\{1, \beta\}$, then we always have

$$\mathcal{O} = \langle 1, c\beta\rangle. \tag{33}$$

A *fractional ideal* is a subset of K which is a non-zero finitely generated $\mathcal{O}$-module. It is an easy exercise to show that every fractional ideal is of the form $\alpha\,\mathfrak{a}$ where $\alpha \in K^\times$ and $\mathfrak{a} \lhd \mathcal{O}$. There are a priori two ways that a fractional ideal can be “nice”. First, we say a fractional ideal $\mathfrak{b}$ is *proper* if

$$\mathcal{O} = \{\alpha \in K \;\mid\; \alpha\,\mathfrak{b} \subseteq \mathfrak{b}\}. \tag{34}$$

Second, we say a fractional ideal $\mathfrak{b}$ is *invertible* if there is another fractional ideal $\mathfrak{b}'$ such that $\mathfrak{b}\,\mathfrak{b}' = \mathcal{O}$. Such an ideal Note that principal fractional ideals, i.e. those of the form $\alpha\,\mathcal{O}$ for some $\alpha \in K^\times$, are automatically invertible. The following proposition says that the two notions coincide.

Proposition 3.1. *Let $\mathfrak{a}$ be a fractional ideal in K. Then $\mathfrak{a}$ is proper if and only if it is invertible.*

Proof. Suppose first that $\mathfrak{a}$ is invertible, with $\mathfrak{a}'$ an ideal such that $\mathfrak{a}\,\mathfrak{a}' = \mathcal{O}$. Let α be any element in K such that $\alpha\,\mathfrak{a} \subseteq \mathcal{O}$, then we have that

$$\alpha\,\mathcal{O} = (\alpha\,\mathfrak{a})\,\mathfrak{a}' \subseteq \mathfrak{a}\,\mathfrak{a}' = \mathcal{O} \tag{35}$$

so that $\alpha \in \mathcal{O}$. This shows that $\mathfrak{a}$ is proper.

Conversely, suppose that $\mathfrak{a}$ is proper. Let α_1, α_2 be two generators of $\mathfrak{a}$. Set $\tau = \alpha_2/\alpha_1$, and let $ax^2 + bx + x$ be its minimal polynomial over $\mathbf{Q}$, where a, b, c are integers with no common prime factors. It is shown in [Cox89, Lemma 7.5] that the set of all elements $\beta \in K$ such that $\beta\,\mathfrak{a} \subseteq \mathfrak{a}$ is equal to the order $\langle 1, a\tau\rangle$ in K. Since $\mathfrak{a}$ is proper, we get that

$$\mathcal{O} = \langle 1, a\tau\rangle. \tag{36}$$

Denoting $^-$ for complex conjugation, we calculate that

$$\begin{aligned} a\,\mathfrak{a}\,\overline{\mathfrak{a}} &= \mathrm{Nm}(\alpha)\langle a, a\tau, a\overline{\tau}, a\tau\overline{\tau}\rangle && (37)\\ &= \mathrm{Nm}(\alpha)\langle a, a\tau, b, c\rangle && (38)\\ &= \mathrm{Nm}(\alpha)\langle 1, a\tau\rangle = \mathrm{Nm}(\alpha)\,\mathcal{O} && (39)\end{aligned}$$

where the second equality follow from the identities $a(\tau+\overline{\tau}) = -b$ and $a\tau\overline{\tau} = c$, and the third equality follows from the coprimality of the triple (a, b, c). This shows that $\mathfrak{a}$ is invertible. □

The Picard group $\mathrm{Pic}(\mathcal{O})$ is by definition the set of proper fractional $\mathcal{O}$-ideals in K, modulo principal ideals. Since it is not immediately clear how to find and enumerate such ideal classes, we now relate them to ideals of the maximal order, which is more familiar territory. Recall that c denotes the conductor of $\mathcal{O}$. We start by defining a certain subset of the proper fractional $\mathcal{O}$-ideals.

Definition 3.2. *An ideal $\mathscr{I} \lhd \mathcal{O}$ is called prime to c if $\mathscr{I} + c\,\mathcal{O} = \mathcal{O}$.*

The importance of this definition lies in the following proposition, whose proof we omit here.

Theorem 3.3. *An ideal $\mathscr{I} \lhd \mathcal{O}$ is prime to c if and only if $\mathrm{Nm}(\mathscr{I})$ is an integer prime to c. As a consequence, any ideal prime to c is automatically proper, and the natural inclusion induces an isomorphism*

$$\{\textit{Ideals prime to } c \textit{ in } \mathcal{O}\}/\{\textit{Principal ideals}\} \simeq \mathrm{Pic}(\mathcal{O}). \tag{40}$$

Furthermore, there is a bijection

$$\{\textit{Ideals prime to } c \textit{ in } \mathcal{O}\} \overset{1:1}{\longleftrightarrow} \{\textit{Ideals prime to } c \textit{ in } \mathcal{O}_K\} \tag{41}$$

such that principal ideals coprime to c in $\mathcal{O}$ correspond to the set of ideals

$$P_{K,\mathbf{Z}}(c) = \{(\alpha) \mid \alpha \equiv n \pmod{c\mathcal{O}_K},\ n \in \mathbf{Z}\}. \tag{42}$$

Proof. The proofs of all the assertions in this theorem may be found in [Cox89, Section 7.C]. □

The main value of the above proposition is that it gives us a very concrete description of the Picard group of the order $\mathcal{O}$, entirely in terms of ideals in the maximal order $\mathcal{O}_K$. This makes it very amenable to explicit calculation, and provides a concrete abstract description of this group that is frequently useful. More precisely, we have

$$\begin{aligned} \mathrm{Pic}(\mathcal{O}) &\simeq \{\text{Ideals prime to } c \text{ in } \mathcal{O}\}/\{\text{Principal ideals}\} &(43)\\ &\simeq \{\text{Ideals prime to } c \text{ in } \mathcal{O}_K\}/P_{K,\mathbf{Z}}(c) &(44)\end{aligned}$$

This implies that there is a short exact sequence relating the Picard group of $\mathcal{O}$ to the class group of K. More precisely, we get the sequence

$$1 \longrightarrow (\mathcal{O}_K/c)^\times / \mathcal{O}_K^\times(\mathbf{Z}/c\mathbf{Z})^\times \longrightarrow \mathrm{Pic}(\mathcal{O}) \longrightarrow \mathrm{Pic}(\mathcal{O}_K) \longrightarrow 1 \tag{45}$$

where $\mathrm{Pic}(\mathcal{O}_K)$ is better known as the class group of K.

Example. Let us consider the example of $\mathcal{O} = \mathbf{Z}[3\sqrt{-3}]$, which is the order of conductor 6 in $K = \mathbf{Q}(\sqrt{-3})$. In this case, we know that

$$\mathcal{O}_K = \mathbf{Z}\left[\frac{1+\sqrt{-3}}{2}\right] \tag{46}$$

is a UFD, so that the short exact sequence (45) gives us an isomorphism

$$\begin{aligned} \mathrm{Pic}(\mathcal{O}) &\simeq \mathbf{F}_4^\times \times \big(\mathbf{F}_3[x]/(x^2)\big)^\times / (\mathbf{Z}/6\mathbf{Z}) &(47)\\ &\simeq \mathbf{Z}/3\mathbf{Z} &(48)\end{aligned}$$

3.2. **A quick introduction to CM theory.** We now quickly recall some statements from global class field theory, and discuss the important notion of *ring class fields*. These results are part of a subject called *CM theory*, which lies at the heart of the theory of Heegner points. Historically, it is one of the most important and beautiful achievements of number theory.

Given a number field K, its ring of adèles is defined as

$$\mathbf{A}_K = \prod_v{}' K_v \tag{49}$$

where the product runs over all places of K, and is *restricted* in the sense that it only contains the elements $(a_v)_v \in \mathbf{A}_K$ for which $a_v \in \mathcal{O}_v$ for all but finitely many v. We can give $\mathbf{A}_K$ a topology by decreeing $\prod_v \mathcal{O}_v$ with its product topology to be an open subset. There is a diagonal map

$$\Delta : K \hookrightarrow \mathbf{A}_K, \tag{50}$$

which endows K with the discrete topology. The quotient $\mathbf{A}_K/K$ is compact. The units in $\mathbf{A}_K$ form a group with respect to multiplication, which we will call the *idèle group*. We topologise it, not with the subspace topology from $\mathbf{A}_K$, but simply by declaring $\prod_v \mathcal{O}_v^\times$, with its product topology, to be open in $\mathbf{A}_K^\times$. The image of $K^\times$ under the diagonal map is again discrete, and the (non-compact) quotient

$$C_K = \mathbf{A}_K^\times / K^\times \tag{51}$$

is called the *idèle class group* of K. It plays the lead role in global class field theory.

Fix a separable closure of K, and take the maximal abelian subextension K^{ab}/K. Then class field theory provides a certain *global Artin map*

$$\varphi : C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K). \tag{52}$$

This map is surjective, and its kernel is the connected component of the identity. It becomes an isomorphism of topological groups when we pass to the *profinite completion*. More precisely, we have

$$\varphi : \widehat{C}_K \xrightarrow{\sim} \mathrm{Gal}(K^{\mathrm{ab}}/K), \qquad \text{where } \widehat{C}_K = \varprojlim_U C_K/U, \tag{53}$$

with the limit taken over all finite index open subgroups. This map is functorial and equivariant in a number of important ways, which we will not recall here. The power of this isomorphism lies in the fact that it describes a system of external objects (the finite abelian extensions of K) in terms of internal data (the finite index open subgroups of C_K). We can be even more specific: A finite abelian extension L/K corresponds to the finite index open subgroup $\mathrm{Nm}_{L/K} C_L$ of C_K. This is a powerful dictionary, but it lacks a satisfactory way to describe (i.e. find explicit generators) for the finite abelian extension corresponding to a given finite index open subgroup of C_K. This problem is known as Hilbert's 12th problem, and remains open to this day, except in very special examples of number fields K.

However, a full solution of Hilbert's 12th problem is given in the case where K is imaginary quadratic, by CM theory. We describe a few aspects of this theory now. Let $\mathcal{O}$ be an order in an imaginary quadratic field as above. Then we define the *ring class field $K_\mathcal{O}$* attached to $\mathcal{O}$ to be the finite abelian extension of K corresponding under (53) to the open subgroup

$$\mathbf{C}^\times \times \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^\times . \tag{54}$$

Suppose $\mathfrak{a}$ is a proper fractional ideal of $\mathcal{O}$, then $\mathfrak{a} \subset \mathbf{C}$ is a lattice and we may define its j-invariant $j(\mathfrak{a}) \in \mathbf{C}$. These are particular examples of *singular moduli*, i.e. values of the j-function at imaginary quadratic fields, which have remarkable properties. It is not so hard to see that the numbers $j(\mathfrak{a})$ are algebraic. The following theorem, which lies much deeper, is one of the main statements of CM theory.

Theorem 3.4. *If K is an imaginary quadratic field, and $\mathfrak{a}$ is a proper ideal of an order $\mathcal{O}$ in K, then $j(\mathfrak{a})$ is an algebraic integer which generates the ring class field $K_\mathcal{O}$ over K. There is an isomorphism*

$$s : \mathrm{Pic}(\mathcal{O}) \longrightarrow \mathrm{Gal}(K_\mathcal{O}/K) \tag{55}$$

defined by $\mathfrak{b} \mapsto \sigma$, where $j(\mathfrak{a})^\sigma = j(\mathfrak{b}^{-1}\,\mathfrak{a})$.

Example. As a beautiful application of these results, we obtain a very satisfactory answer to the age-old question: If $n > 0$ is an integer, when is a prime p of the form $x^2 + ny^2$? Indeed, let p be a prime not dividing n, then we see that this question is equivalent to the splitting of $p = \mathfrak{p}\,\overline{\mathfrak{p}}$ into two principal prime ideals $\mathfrak{p}, \overline{\mathfrak{p}}$. For those familiar with the definition of the Artin map ϕ above, it is not hard to see that this is equivalent to p splitting completely in the ring class field $K_\mathcal{O}/\,\mathbf{Q}$. This implies the following result:

Theorem 3.5. *Let $n > 0$ be an integer, and $K = \mathbf{Q}(\sqrt{-n})$. Define the order $\mathcal{O} = \mathbf{Z}[\sqrt{-n}]$ in K, and let $f_n(x) \in \mathbf{Z}[x]$ be the minimal polynomial of the algebraic integer $j(\mathcal{O})$. Then for any prime p that does not divide $2n\mathrm{disc}(f_n)$ we have that $p = x^2 + ny^2$ for some integers x, y if and only if both of the following conditions are satisfied:*

(1) $-n$ *is a square modulo* p,
(2) $f_n(x)$ *has a root modulo* p.

As an example, we will prove a famous conjecture of Euler about primes of the form $x^2 + 27y^2$. The order relevant for this problem is $\mathcal{O} = \mathbf{Z}[\sqrt{-27}]$. We showed in (48) that

$$\mathrm{Pic}(\mathcal{O}) \simeq \mathbf{Z}/3\mathbf{Z} \tag{56}$$

and hence $K_{\mathcal{O}}$ is a cubic Galois extension of K. Since K contains a third root of unity, Kummer theory guarantees that $K_{\mathcal{O}} = K(\sqrt[3]{a})$ for some element a of K. The extension $K_{\mathcal{O}}/\mathbf{Q}$ is generalised dihedral, which means that

$$\mathrm{Gal}(K_{\mathcal{O}}/\mathbf{Q}) \simeq \mathrm{Pic}(\mathcal{O}) \rtimes \langle \overline{\cdot} \rangle \tag{57}$$

where complex conjugation acts as inversion on the abelian group $\mathrm{Pic}(\mathcal{O})$. It follows that $K_{\mathcal{O}} \cap \mathbf{R}$ is an extension of $\mathbf{Q}$ of degree $|\mathrm{Pic}(\mathcal{O})|$, so that we may assume without loss of generality that a is real.

Since $K_{\mathcal{O}}/K$ is unramified outside of $2, 3$ we may furthermore assume without loss of generality that $a = 2, 3, 6$, or 12. Now we calculate that

$$31\,\mathcal{O}_K = \mathfrak{p}\,\overline{\mathfrak{p}}, \qquad \mathfrak{p} = (2 + 9\sqrt{-3}) \tag{58}$$

where we notice that the $\mathcal{O}_K$-ideal $\mathfrak{p} = (2 + 9\sqrt{-3})$ belongs to $P_{K,\mathbf{Z}}(6)$. This implies that the associated Frobenius element acts trivially on the residue field. Concretely, this means that

$$\sqrt[3]{a} = \mathrm{Frob}_{\mathfrak{p}}(\sqrt[3]{a}) \equiv \sqrt[3]{a}^{31} \equiv a^{10}\sqrt[3]{a} \pmod{\mathfrak{p}}. \tag{59}$$

This immediately rules out three of the four possibilities for a, and we conclude that $K_{\mathcal{O}} = K(\sqrt[3]{2})$. This implies, by the above theorem, that

$$p = x^2 + 27y^2 \iff \begin{cases} p \equiv 1 \pmod 3 \\ x^3 - 2 \text{ has a root in } \mathbf{F}_p\,. \end{cases} \tag{60}$$

This was conjectured by Euler, but he was unable to find a proof during his lifetime (what a loser, amirite?).

3.3. Heegner points on $X_0(N)$.

Finally, we come to the definition of a Heegner point. Let $N \geq 1$ be any integer, and recall that the affine open $Y_0(N) \subset X_0(N)$ of the modular curve of level $\Gamma_0(N)$ classifies cyclic isogenies of degree N, in the sense that its complex points $y \in Y_0(N)(\mathbf{C})$ correspond to an isogeny $E \to E'$ whose kernel is isomorphic to $\mathbf{Z}/N\mathbf{Z}$. We say that y is a *Heegner point* if furthermore

$$\mathrm{End}(E) \simeq \mathrm{End}(E') \simeq \mathcal{O} \tag{61}$$

for some order $\mathcal{O}$ in an imaginary quadratic field K. If we set $D = \mathrm{Disc}(\mathcal{O})$, then $D = c^2 d$ for some integer c which we call the *conductor* of the Heegner point. Likewise, say that the Heegner point y is of *discriminant* D.

Suppose that we choose a quadratic imaginary order $\mathcal{O}$, and ask ourselves whether there exist any Heegner points at all, and if so, whether we can determine all of them explicitly. We first formulate a necessary and sufficient condition for their existence.

Lemma 3.6. *Suppose* $N \geq 1$ *and* $\mathcal{O}$ *is an order in an imaginary quadratic field* K*. Then the set of Heegner points of discriminant* D *is non-empty if and only if there exists an ideal* $\mathfrak{n} \lhd \mathcal{O}$ *such that* $\mathcal{O}/\mathfrak{n} \simeq \mathbf{Z}/N\mathbf{Z}$.

Proof. First, let us assume that we have a Heegner point corresponding to an isogeny $E \to E'$ whose kernel is cyclic of order N. Then we have that

$$E \simeq \mathbf{C}/\mathfrak{a}, \qquad E' \simeq \mathbf{C}/\mathfrak{b} \tag{62}$$

for some fractional ideals $\mathfrak{a}, \mathfrak{b}$ in $\mathcal{O}$. We may assume without loss of generality, by rescaling these fractional ideals, that $\mathfrak{a} \subset \mathfrak{b}$ and the isogeny is simply given by

$$\left\{ \begin{array}{ccc} \mathbf{C} / \mathfrak{a} & \longrightarrow & \mathbf{C} / \mathfrak{b} \\ z + \mathfrak{a} & \longmapsto & z + \mathfrak{b} \end{array} \right. \tag{63}$$

Then the fractional ideal $\mathfrak{n} = \mathfrak{a}\,\mathfrak{b}^{-1}$ is actually a subset of $\mathcal{O}$, and we furthermore have that

$$\mathcal{O} / \mathfrak{n} = \mathfrak{b}\,\mathfrak{b}^{-1} / \mathfrak{a}\,\mathfrak{b}^{-1} \simeq \mathfrak{b} / \mathfrak{a} \simeq \mathbf{Z}/N\mathbf{Z}\,. \tag{64}$$

Conversely, suppose that there is such an ideal $\mathfrak{n}$. Then choose any proper fractional ideal $\mathfrak{a}$ of $\mathcal{O}$, and set $E = \mathbf{C} / \mathfrak{a}$ and $E' = \mathbf{C} / \mathfrak{a}\,\mathfrak{n}^{-1}$, which are related by the isogeny

$$\left\{ \begin{array}{ccc} \mathbf{C} / \mathfrak{a} & \longrightarrow & \mathbf{C} / \mathfrak{a}\,\mathfrak{n}^{-1} \\ z + \mathfrak{a} & \longmapsto & z + \mathfrak{a}\,\mathfrak{n}^{-1} \end{array} \right. \tag{65}$$

The kernel of this isogeny is

$$\mathfrak{a}\,\mathfrak{n}^{-1} / \mathfrak{a} \simeq \mathfrak{a} / \mathfrak{a}\,\mathfrak{n} \simeq \mathcal{O} / \mathfrak{n} \simeq \mathbf{Z}/N\mathbf{Z}\,. \tag{66}$$

□

So in general, Heegner points are only guaranteed to exist if we make the following additional assumption, often referred to as the *Heegner hypothesis*:

$$\text{(HH)} \qquad {}^{\exists}\,\mathfrak{n} \lhd \mathcal{O} \quad \text{s.t.} \quad \mathcal{O} / \mathfrak{n} \simeq \mathbf{Z}/N\mathbf{Z}\,.$$

Now suppose the Heegner hypothesis (H) is satisfied. As in the proof of Lemma 3.6, we see that any Heegner point (E, E') must satisfy that $E \simeq \mathbf{C} / \mathfrak{a}$ for some fractional ideal, and $E' \simeq \mathbf{C} / \mathfrak{a}\,\mathfrak{n}^{-1}$ for some ideal $\mathfrak{n}$ as in (HH). Conversely, any such choice of $\mathfrak{a}$ and $\mathfrak{n}$ gives rise to a Heegner point, which furthermore only depends on the class of $\mathfrak{a}$ in $\mathrm{Pic}(\mathcal{O})$. This shows that there is a bijection

$$\{\text{Heegner points on } X_0(N)\} \overset{1:1}{\longleftrightarrow} \{(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]) \;:\; \mathcal{O} / \mathfrak{n} \simeq \mathbf{Z}/N\mathbf{Z}, [\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})\} \tag{67}$$

This bijection makes the set of Heegner points extremely concrete. We now turn to a description of the action of the Galois group and Hecke algebra, which have concrete descriptions in terms of triples via this bijection. **Henceforth, we make the assumption that the conductor c is coprime to N.**

3.3.1. *The Galois action.* By CM theory, we see that the set of Heegner points is algebraic, and we first describe the action of $\mathrm{Aut}(\mathbf{C})$ in terms of the corresponding triples under the bijection (67). First, complex conjugation acts via the rule

$$\overline{(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])} = (\mathcal{O}, \overline{\mathfrak{n}}, [\overline{\mathfrak{a}}]) \tag{68}$$

simply because it is a continuous automorphism of $\mathbf{C}$. By CM theory, the action of any other element of $\mathrm{Aut}(\mathbf{C})$ factors through $\mathrm{Gal}(K_{\mathcal{O}}/K)$. Using the isomorphism s with the Picard group defined in (55) we may now describe the action via

$$(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])^{s(\mathfrak{b})} = (\mathcal{O}, \mathfrak{n}, [\mathfrak{b}^{-1}\,\mathfrak{a}]) \tag{69}$$

3.3.2. *The Hecke action.* We first describe the action of the Atkin–Lehner involutions, of which there is one for every prime divisor p of N. Write $N = p^k m$ with m coprime to p. Suppose $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ is a Heegner point, then there is a unique divisor $\mathfrak{p}$ of p which divides $\mathfrak{n}$, and we may likewise write $\mathfrak{n} = \mathfrak{p}^k\,\mathfrak{m}$, where (p) is coprime to $\mathfrak{m}$. Then the Atkin–Lehner involution w_p acts via

$$w_p(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]) = (\mathcal{O}, \overline{\mathfrak{p}}^k\mathfrak{m}, [\mathfrak{a}\,\mathfrak{p}^{-k}]). \tag{70}$$

The Hecke correspondences T_ℓ, for ℓ a prime not dividing N, also act on the set of Heegner points with conductor prime to N. The action is given by the formula

$$T_\ell(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]) = \sum_{\mathfrak{a}/\mathfrak{b} = \mathbf{Z}/\ell\mathbf{Z}} (\mathcal{O}_\mathfrak{b}, \mathfrak{n}_\mathfrak{b}, [\mathfrak{b}]), \tag{71}$$

where the sum runs over the $(\ell+1)$ sublattices $\mathfrak{b}$ of index ℓ in $\mathfrak{a}$, and $\mathcal{O}_\mathfrak{b} = \mathrm{End}(\mathfrak{b})$ and $\mathfrak{n}_\mathfrak{b} = \mathfrak{n}\mathcal{O}_\mathfrak{b} \cap \mathcal{O}_\mathfrak{b}$.

3.4. **Heegner points on E.**

For our guiding example, this construction gives rise to plethora of potentially interesting rational points on E, which are furthermore explicitly computable via the uniformisation (20).

For explicit computations, we will make use of the uniformisation

$$\phi : \mathfrak{H} \longrightarrow \Gamma\backslash\mathfrak{H} \xrightarrow{\sim} E \tag{72}$$

described in the previous section, which factors through $X_0(N)$. For computational reasons, it will therefore be important to understand the points in the upper half plane that correspond to the Heegner points on $X_0(N)$. To do this, we first establish a correspondence between proper ideals and binary quadratic forms:

Lemma 3.7. *Suppose*

$$F(x,y) = ax^2 + bxy + cy^2 \tag{73}$$

is a primitive, positive definite, binary quadratic form of discriminant $\Delta < 0$. *Then*

$$\mathfrak{a} = \left(a, \frac{-b+\sqrt{\Delta}}{2}\right) \tag{74}$$

is a proper ideal of the quadratic order $\mathcal{O}$ *of discriminant* Δ. *Moreover, this assignment induces a bijection*

$$\{F(x,y) \textit{ prim. pos. def. discriminant } D\}/\,\mathrm{SL}_2(\mathbf{Z}) \xrightarrow{1:1} \mathrm{Pic}(\mathcal{O}) \tag{75}$$

Proof. A proof can be found in [Cox89, Section 7.B]. It is worth noting that the inverse map is

$$\mathfrak{a} = (\alpha, \beta) \longmapsto \mathrm{Nm}(\alpha x + \beta y)/\,\mathrm{Nm}(\mathfrak{a}). \tag{76}$$

□

Remark. This bijection in particular endows the set of $\mathrm{SL}_2(\mathbf{Z})$-equivalence classes of primitive positive definite quadratic forms of any discriminant with the structure of a finite group. The description of this group law in terms of quadratic forms was originally discovered by Gauß, and goes by the name *Gauß composition.* In 2004, Bhargava presented a new treatment of Gauß composition that allows for generalisations to new settings. We define a *Bhargava cube* to be a $2 \times 2 \times 2$ cube with integers associated to its vertices. To a Bhargava cube, we associate three quadratic forms as follows:

$$\left\{\begin{array}{rcl} Q_1(x,y) & = & -\det\left(x \cdot \begin{pmatrix} a & e \\ b & f \end{pmatrix} + y \cdot \begin{pmatrix} c & g \\ d & h \end{pmatrix}\right) \\ Q_2(x,y) & = & -\det\left(x \cdot \begin{pmatrix} a & c \\ e & g \end{pmatrix} + y \cdot \begin{pmatrix} b & d \\ f & h \end{pmatrix}\right) \\ Q_3(x,y) & = & -\det\left(x \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} + y \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix}\right) \end{array}\right.$$

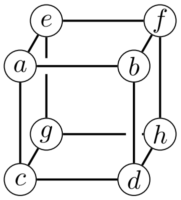

FIGURE 2. Cubus Bhargaviensis

These three forms have the same discriminant. If two of these three quadratic forms are primitive, then so is the third one. In this case, we say the cube is *projective*. It turns out that $Q_3(x,-y)$ is a direct composition of $Q_1(x,y)$ and $Q_2(x,y)$ in the sense of Gauß! The language of Bhargava has the advantage of "unraveling" some of the difficult algebra of Gauß. ■

From Lemma 3.7, it follows that the set of points $\tau \in \mathfrak{H}$ corresponding to elliptic curves with complex multiplication by an order $\mathcal{O}$ of discriminant Δ is the finite set of $\mathrm{SL}_2(\mathbf{Z})$-orbits of solutions of quadratic equations $a\tau^2 + b\tau + c$ where a, b, c are coprime integers such that $b^2 - 4ac = \Delta$. This may now easily be turned into a proof of the following statement:

Lemma 3.8. *Let $N \geq 1$ and $\mathcal{O}$ an order of discriminant $\Delta < 0$ such that*

- *the conductor c of $\mathcal{O}$ is prime to N,*
- *the Heegner hypothesis (HH) is satisfied.*

Then there is a bijection

$$\{\textit{Heegner points } (\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])\} \xleftrightarrow{1:1} \left\{ \begin{array}{c} ax^2 + bxy + cy^2 \textit{ prim. pos. definite} \\ \textit{s.t. } b^2 - 4ac = \Delta, \textit{ and } N \mid a \end{array} \right\} / \, \Gamma_0(N) \tag{77}$$

Proof. TODO. □

This lemma clearly results in an explicit method to determine the finite set of Heegner points. These points map to points in $E(\overline{\mathbf{Q}})$ which are defined over the ring class field $K_{\mathcal{O}}$ of K, and when appropriately averaged they give rise to rational points on E.

More precisely, is we let $\mathcal{H}_{\mathcal{O}}$ be the set of Heegner points associated to $\mathcal{O}$ in $\mathfrak{H}$, which is of size $2h$, where h is the class number of $\mathcal{O}$. As before, we denote $\phi : \mathfrak{H} \to E$ be the uniformisation map from (20). Now for any $\tau \in \mathcal{H}_{\mathcal{O}}$ we define

$$P_\tau = \phi(\tau) \in E(\overline{\mathbf{Q}}). \tag{78}$$

Note that the set of such points P_τ is naturally acted on by the Atkin–Lehner involution w_{61}, and the size u of the projective stabiliser of P_τ is usually of size 1, unless $\Delta = -3, -4$, when $u = 3, 2$ respectively. Then we define $P_\Delta \in E(\mathbf{Q})$ by

$$2uP_\Delta = \sum_{\tau \in \mathcal{H}_{\mathcal{O}}} P_\tau \tag{79}$$

where the rationality of the point P_Δ follows from the Galois-stability of the set $\phi(\mathcal{H}_{\mathcal{O}})$ described above. We see that if Δ is not a square modulo 61, the set $\mathcal{H}_{\mathcal{O}}$ is empty and $P_\Delta = 0$. When Δ is a square, the points P_Δ have the potential to be of infinite order, and using the numerical techniques described above, most notably the rapidly convergent series (21) for the uniformisation ϕ, we compute for instance that for

$\Delta = -52$, the class number is 2 and we get the following Heegner points on E:

(80)

$\tau \in \mathcal{H}_{\mathcal{O}}$	$\phi(\tau) \in \mathbf{C}$	$P_\tau \in E(\overline{\mathbf{Q}})$
$\frac{-29+\sqrt{-13}}{854}$	-0.668988176	$\left(\frac{1+\sqrt{13}}{2}, 2\right)$
$\frac{-32+\sqrt{-13}}{1037}$	-0.668988176	$\left(\frac{1+\sqrt{13}}{2}, 2\right)$
$\frac{-29+\sqrt{-13}}{427}$	$0.281978261 + 0.99720547i$	$\left(\frac{1-\sqrt{13}}{2}, 2\right)$
$\frac{-93+\sqrt{-13}}{4331}$	$0.281978261 + 0.99720547i$	$\left(\frac{1-\sqrt{13}}{2}, 2\right)$

In this case, we get that the normalised sum P_{-52} is

$$P_{-52} = \left(\frac{16}{9}, \frac{29}{27}\right) = -3P. \tag{81}$$

In general, we can set $P_\Delta = b_\Delta P$ for some $b_\Delta \in \mathbf{Z}$, and we may wonder how b_Δ varies as we vary Δ. The following table ranges over all discriminants up to -200, and lists the values of b_Δ:

Δ	$\left(\frac{\Delta}{61}\right)$	b_Δ	Δ	$\left(\frac{\Delta}{61}\right)$	b_Δ	Δ	$\left(\frac{\Delta}{61}\right)$	b_Δ	Δ	$\left(\frac{\Delta}{61}\right)$	b_Δ	Δ	$\left(\frac{\Delta}{61}\right)$	b_Δ
-3	1	1	-43	-1	0	-83	1	2	-123	1	3	-163	1	-5
-4	1	-1	-44	-1	0	-84	-1	0	-124	-1	0	-164	1	-1
-7	-1	0	-47	1	2	-87	-1	0	-127	1	-3	-167	1	1
-8	-1	0	-48	1	0	-88	1	1	-128	-1	0	-168	1	-4
-11	-1	0	-51	-1	0	-91	-1	0	-131	1	1	-171	1	-1
-12	1	2	-52	1	-3	-92	-1	0	-132	-1	0	-172	-1	0
-15	1	-1	-55	-1	0	-95	1	-1	-135	1	2	-175	-1	0
-16	1	0	-56	1	-1	-96	-1	0	-136	1	0	-176	-1	0
-19	1	1	-59	-1	0	-99	-1	0	-139	-1	0	-179	1	-2
-20	1	1	-60	1	2	-100	1	3	-140	-1	0	-180	1	-3
-23	-1	0	-63	-1	0	-103	1	3	-143	-1	0	-183	0	1
-24	-1	0	-64	1	0	-104	-1	0	-144	1	-2	-184	1	-1
-27	1	0	-67	-1	0	-107	1	-2	-147	1	2	-187	1	5
-28	-1	0	-68	-1	0	-108	1	2	-148	-1	0	-188	1	-4
-31	-1	0	-71	-1	0	-111	-1	0	-151	-1	0	-191	-1	0
-32	-1	0	-72	-1	0	-112	-1	0	-152	-1	0	-192	1	4
-35	-1	0	-75	1	0	-115	-1	0	-155	-1	0	-195	1	3
-36	1	0	-76	1	0	-116	-1	0	-156	1	2	-196	1	-3
-39	1	-1	-79	-1	0	-119	1	-1	-159	-1	0	-199	1	0
-40	-1	0	-80	1	-1	-120	-1	0	-160	-1	0	-200	-1	0

TABLE 1. The values b_Δ for which $P_\Delta = b_\Delta P$.

We will investigate the patterns suggested by this table in the next section.

4. The theorems of Waldspurger and Gross–Zagier

The theory of Heegner points discussed in the previous section clearly gives rise to a large and interesting supply of rational points on elliptic curves. Though there have been many exciting developments since, it remains true that at its core, this is the only systematic supply of rational points on elliptic curves that is known today. For applications to the Birch–Swinnerton-Dyer conjecture, it is absolutely crucial to have a satisfactory answer to the following questions:

> **Q:** Do the points P_Δ generate $E(\mathbf{Q})$? What is their position in $E(\mathbf{Q})$?

In rank 1 situations, we will see that an answer to the first question is provided by the theorem of Gross–Zagier [GZ86], in analytic terms. Whereas the second question is rather vague at this point, we will see that a very satisfactory answer is suggested by the theorem of Waldspurger, which is made precise in the work of Gross–Kohnen–Zagier [GKZ87].

4.1. **Waldspurger.** We start with a brief discussion of Waldspurger's theorem, which relates the Fourier coefficients of a certain modular form of half-integral weight with the special values of the value at $s = 1$ of certain twists of the L-function $\mathrm{L}_E(s)$. This seminal formula is of tremendous importance in number theory, and though it has been generalised and refined considerably, we content ourselves with a discussion of the special case relevant to our discussion of E. We first discuss the set of quadratic twists of E, then the Shimura correspondence, which attaches a form of weight $3/2$ to E, and then finally the connection between the two provided by Waldspurger's theorem, in the form of a subsequent refinement due to Kohnen.

4.1.1. *Quadratic twists of E.* The short Weierstraß model for E is given by

$$E : y^2 = x^3 - 2619x + 54486 \tag{82}$$

Now suppose $\Delta < 0$ is a fundamental discriminant. We define the *quadratic twist*

$$E_\Delta : \Delta y^2 = x^3 - 2619x + 54486 \tag{83}$$

which is defined over $\mathbf{Q}$. We will now investigate the L-function of these quadratic twists, as well as their Brich–Swinnerton-Dyer invariants. I must confess I did not rigorously work through the invariants, and in fact I do not know how to fully justify most of the claims below. If anyone is interested in working this out in detail with me, please do get in touch, I'd still love to do this some time.

First, we note that E_Δ is always modular, a fact which follows from the modularity of E. Indeed, it is a classical fact that for any Δ coprime to 61 the twisted series

$$f_\Delta = \sum_{n\geq 1} \left(\frac{\Delta}{n}\right) a_n q^n \tag{84}$$

is the q-expansion of a modular form of level $N\Delta^2$ and weight 2. We now check that these Fourier coefficients agree with the coefficients of the L-series of the quadratic twist E_Δ.

- Suppose $p \nmid 6 \cdot 61 \cdot \Delta$: Choose a model $y^2 = f(x)$ for E that has good reduction at p. The number of points modulo p may be counted by choosing a random value of x, and determining whether $f(x) \cdot \Delta$ is a square modulo p. We see that when Δ is a square, this yields the same point count as E, whereas when Δ is a non-square this gives the complement of the points counted for E. This yields that $a_p(E_\Delta)$ is equal to the p-th Fourier coefficient of f_Δ.
- One would imagine a similar argument would work for $p = 2, 3$ if the curve has good reduction there, by working with a more complicated model. I did not check.
- When $p = 61$ we see that the reduction is still multiplicative, but changes from non-split to split exactly when Δ is a square modulo 61. In that case, it is predicted by the Birch–Swinnerton-Dyer conjecture that the rank of $E_\Delta(\mathbf{Q})$ is even, and we expect that it is generically 0.
- When $p \mid \Delta$ I also did not check, but it looks fun so let's try it over a cup of coffee some time.

The real period $\Omega^+_{E_\Delta}$ may also be computed, and it follows from a result of Vivek Pal that we have

$$\Omega^+_{E_\Delta} = \frac{\Omega^-_E}{\sqrt{\Delta}} \tag{85}$$

In this case, we can probably give a simple proof, but I did not check this. The crux of the problem is to find the Néron minimal model for E_Δ, which seemed slightly painful. Maybe it's not so bad, since the primes dividing Δ cannot divide the discriminant of the twist of the minimal model for E more than twice.

Now comes the torsion. Note that E_Δ does not have any 2-torsion, since any such point must have $y = 0$ in the above model, and hence the same coordinates must also define a 2-torsion point on E, which does not exist. Now suppose that there is some torsion of prime order $l > 2$, then we must have a congruence between the higher coefficients of the form f_Δ and the Eisenstein series

$$E_2^{(61)}(q) = \frac{5}{2} + \sum_{n \geq 1} \sigma_1^{(61)}(n) q^n \tag{86}$$

which, since f_Δ is cuspidal, can only happen if $l = 5$. I'm not sure how to rule this possibility out, but one additional thing one can show is that any such discriminant must be divisible by all of the first 10 or so primes, so it seems very unlikely that this could exist.

Finally, we mention the Tamagawa numbers. This seems a little tricky. Zagier completely ignores these, though in his example they always seem to be trivial. In our example, the product of the Tamagawa numbers always seems to be 2, andthe contribution always happens at some prime divisor of Δ. I don't know how to prove this in general, or if it is even always true. Rubin has a nice paper on fudge factors of quadratic twists where this problem is discussed, and he gives a rather explicit criterion which I could not turn into a proof of this experimental factor 2 in this example. Again, if anyone wants to try, do get in touch.

The L-function of E_Δ may now be made explicit, and is given for $\mathrm{Re}(s) > 3/2$ by the expression

$$\mathrm{L}_{E,\Delta}(s) = \sum_{n \geq 1} \left(\frac{\Delta}{n}\right) \frac{a_n}{n^{-s}}. \tag{87}$$

We likewise have a rapidly convergent series for the special value at 1, which may be used to compute numerical approximations in practice, just like we did for E. The sign of the functional equation of this L-function is given by $-\left(\frac{\Delta}{61}\right)$, and hence we expect the rank of $E_\Delta(\mathbf{Q})$ to be even (and in fact, most often 0) whenever the sign is equal to $+1$. According to the Birch–Swinnerton-Dyer conjecture, we should have

$$\mathrm{L}_{E,\Delta}(1) = \Omega^+_{E_\Delta} \cdot \prod_p c_p \cdot A_\Delta, \qquad A_\Delta \in \mathbf{Z} \tag{88}$$

and in fact, A_Δ should be the order of the Tate–Shafarevich group, which, if finite, is a square. Using the theorem of Waldspurger, we can in fact *prove* that it is a square, though of course that still falls short of proving finiteness of $Ш_E$. We compute explicitly the numbers A_Δ for the first few fundamental discriminants for which the sign of the functional equation is equal to $+1$, and obtain the following table.

First of all, notice that indeed A_Δ always nicely seems to be a square. Ok, fine. That's what we expected from Birch–Swinnerton-Dyer, and what will follow from Waldspurger's theorem below. But now look at the table of the quantities b_Δ related to Heegner points above, and notice something truly beautiful and amazing is happening. More on that later.

Δ	A_Δ	Δ	A_Δ	Δ	A_Δ	Δ	A_Δ
-3	1	-81	4	-136	0	-195	1
-4	1	-88	1	-163	25	-199	0
-15	1	-95	1	-164	1		
-19	1	-103	9	-167	1		
-20	1	-107	4	-168	4		
-39	1	-119	1	- 179	4		
-47	4	-123	9	-183	1		
-52	9	-127	9	-184	1		
-56	1	-131	1	-187	25		

TABLE 2. The values A_Δ for which $\mathrm{L}_{E,\Delta}(1) = \Omega^+_{E_\Delta} \cdot \prod_p c_p \cdot A_\Delta$.

4.1.2. *The Shimura correspondence.* We showed in §2 that the elliptic curve E has an associated newform f of weight 2 and level 61, whose q-expansion coefficients we may compute up to our heart's desire. There is another modular form 'attached' to E, which is of weight $3/2$ and goes through the Shimura correspondence. This modular form plays a central role in the work of Waldspurger [Wal81] and Gross–Kohnen–Zagier [GKZ87].

To state the theorem of Shimura precisely in the form we need it, define $S_k^{\pm}(\Gamma_0(N))$ to be the space of weight k forms f for which

$$w_N f = \pm f \tag{89}$$

Likewise, we define $S_{k/2}^{\pm}(\Gamma_0(4N))$ to be the space of half-integral weight $k/2$ forms of level $\Gamma_0(4N)$ whose Fourier expansion is of the form

$$\sum_{n\geq 1} c_n \tag{90}$$

Theorem 4.1 (Shimura, Kohnen). *Let* $\varepsilon \in \{\pm 1\}$. *We have that* $\dim(S^{\varepsilon}_{k+1/2}(\Gamma_0(4N)) = \dim(S^{\varepsilon}_{2k}(\Gamma_0(N))$, *and for each Hecke eigenform*

$$f = \sum_{n\geq 1} a_n q^n \qquad \dim(S^{\varepsilon}_{2k}(\Gamma_0(N)) \tag{91}$$

there is a 1-dimensional space of forms $g \in \dim(S^{\varepsilon}_{k+1/2}(\Gamma_0(4N))$ *whose Fourier coefficients are related to those of* f *by the rule*

$$a_n c_m = \sum_{d \mid n} \left(\frac{-m}{d}\right) c_{mn^2/d^2}. \tag{92}$$

This result is usually referred to as the *Shimura correspondence*, and its proof is entirely analytic and quite deep. We will not say anything about how this theorem was proved here, but note that in our case of the modular form f attached to the elliptic curve E, the associated form through the Shimura correspondence is of weight $3/2$. So how do we compute it?

In general, it is quite difficult to compute this Shimura lift explicitly, though there are methods available, see for instance [Ham12]. I noticed however that `Magma` is able to compute bases for spaces of half-integral weight modular forms very fast, which I suspect is happening by using a unary theta series to reduce the problem to a computation in integral weight, and deciding which forms come from half-integral weight, since it is really fast. From there, I was able to compute the desired Shimura lift through the Hecke equivariance of this correspondence. More precisely, the space $S_{3/2}(\Gamma_0(244))$ comes equipped with Hecke operators T_{p^2} for every prime $p \neq 2, 61$, and the space of forms G such that

$$T_{p^2} G = a_p G \tag{93}$$

for almost all p is known to be 2-dimensional, and contains a unique form g in the Kohnen plus space. The Hecke operators have a simple description in terms of q-expansions, which is more complicated than it is in integral weight, but not overly so. To be exact, the n-th coefficient of the modular form $T_{p^2}G$, where $G = \sum c_m q^m$ is given by

$$c_{mp^2} + \left(\frac{-1}{p}\right)^k \left(\frac{n}{p}\right) p^{k-1} c_m + p^{2k} c_{m/p^2} \tag{94}$$

Using this expression, I wrote some code to compute Hecke operators on the spaces of half-integral weight, and then looks for the unique form in the Kohnen space associated to f. For the example considered above, we get the following form of weight $3/2$.

$$\begin{aligned} g &= q^3 - q^4 - q^{15} + q^{16} + q^{19} + q^{20} - 2q^{27} + q^{36} - q^{39} + 2q^{47} - 2q^{48} - 3q^{52} \\ &\quad -q^{56} + 2q^{60} + q^{64} - 2q^{75} - q^{80} + 2q^{83} + q^{88} - q^{95} + O(q^{100}) \end{aligned}$$

4.1.3. *The theorem of Kohnen–Waldspurger.* We now come to the statement of the theorem of Waldspurger [Wal81], as extended and refined by Kohnen [Koh85].

Theorem 4.2. *Suppose $f \in S_2^{\varepsilon}(\Gamma_0(N))$ is a Hecke eigenform with rational eigenvalues, corresponding to the elliptic curve E over $\mathbf{Q}$, and $g \in S_{3/2}^{\varepsilon}(\Gamma_0(4N))$ is a modular form corresponding to it under the Shimura correspondence. If the Fourier expansion of g is*

$$g = \sum_{n \geq 1} c_n q^n \tag{95}$$

then for any fundamental discriminant $\Delta < 0$ with $\left(\frac{\Delta}{N}\right) = \varepsilon$ or 0, we have that

$$L_{E,\Delta}(1) = 3\pi \frac{\|f\|^2}{\|g\|^2} \cdot \frac{c_{|\Delta|}^2}{\sqrt{|\Delta|}}. \tag{96}$$

where $\|f\|$ and $\|g\|$ are the norms of f and g in the Petersson metric.

In our example, we get from looking at $\Delta = -3$ that there is an equality

$$\begin{aligned} 3\pi \cdot \frac{\|f\|}{\|g\|} \cdot \frac{1}{\sqrt{3}} &= \Omega_{E_\Delta}^{+} \cdot \prod_p c_p \cdot A_{|\Delta|} && (97) \\ &= \frac{\Omega_E^{-}}{\sqrt{3}} \cdot 2 \cdot 1 && (98) \end{aligned}$$

so that the transcendental factors on both sides, which are independent of Δ, must be equal. It follows that for every fundamental discriminant $\Delta < 0$ we have an equality

$$A_{|\Delta|} = c_{|\Delta|}^2. \tag{99}$$

4.2. **Gross–Zagier.** Recall that we defined the quantity b_Δ to be the multiple of the generator $P = (1, -1)$ obtained from the Heegner point P_Δ attached to a discriminant Δ. This quantity plays a central role in the theorem of Gross–Zagier. We state it in the specific case under consideration, and postpone the general statement to the next section, where we also give a short overview of the proof.

Theorem 4.3 (Gross–Zagier)**.** *Suppose $\Delta < 0$ is a fundamental discriminant, which is a square modulo 61. Then*

$$h(P_\Delta) = \frac{\sqrt{|\Delta|}}{8\pi^2\|f\|^2} \cdot L'_E(1)L_{E_\Delta}(1). \tag{100}$$

Since the canonical height is a quadratic function, this gives us a very interesting concrete consequence for the quantity b_Δ. Indeed, by combining equation (100) with Waldspurger's theorem (96) for the quantity $L_{E_\Delta}(1)$, we obtain that

$$b_\Delta^2 \cdot h(P) = \left(\frac{3}{8\pi\|g\|\|f\|} L'_E(1)\right) \cdot c_\Delta^2 \tag{101}$$

Note that the factor in front of c_Δ on the right hand side of this equation is independent of Δ. Therefore, we can avoid its explicit computation by simply noting that for $\Delta = -3$ we get that $b_{-3}^2 = c_{-3}^2$, and therefore it follows that for any fundamental discriminant $\Delta < 0$ we have

$$b_\Delta^2 = c_\Delta^2 \qquad (= A_\Delta). \tag{102}$$

4.3. **The positions of Heegner points.** The results above are quite striking. The quantity A_Δ, which should be closely related to the order of the Tate–Shafarevich group $Ш_E$, was proved to be a square in two different ways, by exhibiting two canonical square roots for it: One being the Fourier coefficient of a modular form of weight $3/2$, the other being prescribed by the theory of Heegner points. The work of Gross–Kohnen–Zagier shows that in fact, both of these quantities are equal, that is

$$b_\Delta = c_\Delta. \tag{103}$$

This is a fascinating result, and significantly finer than the theory of Gross–Zagier, which only captures the "size" of Heegner points, through the quantity b_Δ^2. The true "position" of the Heegner point is given by the quantity b_Δ, which by the above theorem is given by the Fourier coefficient of a modular form!

The proof is absolutely beautiful, and easily deserves an entire study group devoted to it. We will quickly outline some of the ideas here, and refer the interested reader to the papers [Zag85] and [GKZ87]. Choose an auxiliary prime $p \equiv 1 \pmod 4$ such that 61 is a square mod p. Define the *Hilbert modular surface*

$$S_p = (\mathfrak{H} \times \mathfrak{H} \,/\, \mathrm{SL}_2(\mathcal{O}))^{*,\sim} \tag{104}$$

where $\mathcal{O}$ is the maximal order in $\mathbf{Q}(\sqrt{p})$, and the superscripts denote an appropriate compactification and desingularisation. The divisor at infinity [+]

5. The proof of Gross–Zagier

The general statement of the Gross–Zagier theorem takes place on the Jacobian J of the modular curve $X_0(N)$. Suppose that $\Delta < 0$ is a fundamental discriminant, of an imaginary quadratic field K. Recall that we have an isomorphism

$$s : \mathrm{Cl}_K \xrightarrow{\sim} \mathrm{Gal}(H/K) \tag{105}$$

where H is the Hilbert class field of K. For any ideal class $\mathcal{A} \in \mathrm{Cl}_K$ define the partial theta series

$$\theta_{\mathcal{A}}(z) = \frac{1}{2u} + \sum_{\substack{\mathfrak{a} \lhd \mathcal{O}_K \\ \mathfrak{a} \in \mathcal{A}}} q^{\mathrm{Nm}(\mathfrak{a})} \tag{106}$$

$$= \frac{1}{2u} + \sum_{n \geq 1} r_{\mathcal{A}}(n) q^n \tag{107}$$

which is a modular form of weight 1, level $\Gamma_1(\Delta)$, and nebentypus given by the quadratic character attached to K. For any $f = \sum a_n q^n \in S_2(\Gamma_0(N))^{\mathrm{new}}$, we define

$$L_{\mathcal{A}}(f,s) = \sum_{\substack{n \geq 1 \\ (n, \Delta N)=1}} \left(\frac{\Delta}{n}\right) n^{1-2s} \cdot \sum_{n \geq 1} a_n r_{\mathcal{A}}(n) n^{-s}. \tag{108}$$

We then have the following result:

Theorem 5.1 (Gross–Zagier). *The series*

$$g_{\mathcal{A}}(z) = \sum_{m \geq 0} \langle c, T_m c^{s(\mathcal{A})} \rangle q^m \tag{109}$$

is a modular form of weight 2 *and level* $\Gamma_0(N)$*, and furthermore*

$$(f, g_{\mathcal{A}}) = \frac{u^2 \sqrt{|\Delta|}}{8\pi^2} \cdot L'_{\mathcal{A}}(f,1) \tag{110}$$

where

- $c = (x) = (\infty) \in J(H)$ *where* x *is a Heegner point of discriminant* Δ,
- $(\cdot\,,\,\cdot)$ *is the Petersson inner product,*
- $\langle \cdot\,,\,\cdot \rangle$ *is the height pairing on* $J(H) \times J(H)$.

By averaging over ideal classes $\mathcal{A}$, we get the most celebrated result of Gross–Zagier. Let

$$\chi : \mathrm{Cl}_K \longrightarrow \mathbf{C}^\times \tag{111}$$

be a class group character, and define the twisted L-series

$$L(f, \chi, s) = \sum_{\mathcal{A} \in \mathrm{Cl}_K} \chi(\mathcal{A}) L_{\mathcal{A}}(f,s) \tag{112}$$

Likewise, we define twisted versions of the Heegner divisor c by

$$c_\chi = \sum_{\mathcal{A} \in \mathrm{Cl}_K} \chi^{-1}(\mathcal{A}) L_{\mathcal{A}}(f,s) \tag{113}$$

which lies in the subspace of $J(H) \otimes \mathbf{C}$ where $s(\mathcal{A})$ acts as multiplication by $\chi(\mathcal{A})$. Furthermore, the projection of c_χ onto the f-isotypic component for the action of the Hecke algebra is denoted by $c_{f,\chi}$.

Theorem 5.2 (Gross–Zagier). *We have*

$$L'(f, \chi, 1) = \frac{\|\omega_f\|^2}{u\sqrt{|\Delta|}} \cdot h_K(c_{\chi,f}) \tag{114}$$

where $\omega_f = 2\pi i f(z) dz$ *is the differential associated to* f.

5.1. **The plan.** The plan for the rest of the seminar is to prove the above theorems of Gross–Zagier. The strategy will be as follows. The canonical Néron–Tate height h is the quadratic function induced by the bilinear global height pairing

$$\langle\cdot,\cdot\rangle \;:\; J(H)\times J(H) \longrightarrow \mathbf{R}\,. \tag{115}$$

Néron shows that this height decomposes as a sum of local symbols

$$\langle\cdot,\cdot\rangle_v \;:\; \mathrm{Div}^0(X)\times \mathrm{Div}^0(X) \longrightarrow \mathbf{R} \tag{116}$$

for each place v of H. This local function is uniquely characterised by the following two conditions:

- It is bi-additive, symmetric, and continuous,
- Suppose that we have two divisors

$$a=\sum_P m_P P, \qquad b=\mathrm{div}(f) \tag{117}$$

then if a and b have disjoint support, the local symbol is given by

$$\langle a,b\rangle_v = \log|f(a)|_v := \sum_P m_P \log|f(P)|_v. \tag{118}$$

The plan for the rest of this seminar is to set $c=(x)-(\infty)$ and $d=(x)-(0)$, for x a Heegner point as above, and compute in very explicit terms the global pairing

$$\langle c, T_m c^\sigma\rangle = \langle c, T_m d^\sigma\rangle \tag{119}$$

where the equality is satisfied because the divisor $(\infty)-(0)$ is torsion by the theorem of Manin–Drinfeld. This switch from c to d is to increase the number of cases where the two divisors in question are disjoint, which will greatly aid the computation. The global pairing is then computed by computing for every place v of H the local symbol

$$\langle c, T_m d^\sigma\rangle_v \tag{120}$$

When v is archimedean, this involves a careful construction of an appropriate Green's function, and we will see how to do this in Tiago's talk. Then Netan and Francesca will tell us how to compute the local symbol when v is non-archimedean. There, the problem is reduced to certain counting problems for norm equations in quaternion algebras, which are tackled using the theory of quasi-canonical liftings.

Once the global pairing is computed in very explicit terms, we will see in the talk of Tom and Alex that one can construct a form $g_{\mathcal{A}}$ with the required properties using Rankin's method. After it has been constructed, its Fourier coefficients are computed, and the computation reveals that we end up with the same expression as the one we obtained for $\langle c, T_m d^\sigma\rangle$. This will prove the theorem, and almost conclude our seminar.

In addition to the above talks, we will start off with a talk by Nils, who will explain the proof of the Gross–Zagier theorem in level 1. In this case, the statement above is of course vacuous, but what is meant is that the local contribution to the height of a Heegner divisor is computed, first for all the non-archimedean places, and then at the archimedean place. Since the height is trivial, both expressions must be the same. Finally, to end the seminar, we have a talk by Francesco, which is aimed at reinterpreting the statements and proofs of the Gross–Zagier and Waldspurger theorems in the adelic language. This is more akin to the modern viewpoint of these theorems, and provides an extremely flexible language which is adopted in the proofs of subsequent generalisations in the literature.

Appendix A. Elliptic curves

In this appendix, we will collect some basic facts about elliptic curves. We will content ourselves with an extremely concise description, and for full details and proofs we refer the reader to standard texts such as [Sil09].

An elliptic curve over a field K is defined to be a smooth projective algebraic curve of genus 1, endowed with a distinguished point $0 \in E(K)$. Riemann–Roch implies that every such curve has an algebraic equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in K. \tag{121}$$

Elliptic curves are most easily understood when $K = \mathbf{C}$ through the theory of Weierstraß uniformisation, which we discuss first. Over other base fields, notably the field of rational numbers $\mathbf{Q}$, the arithmetic of elliptic curves is extremely complex, and continues to hold many mysteries today.

A.1. **Weierstraß uniformisation.** Suppose that $\Lambda \subset \mathbf{C}$ is a lattice, then the quotient $\mathbf{C}/\Lambda$ is an algebraic variety. This can be shown by explicitly constructing an algebraic model for it. Define first the Weierstraß $\wp$-function by

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}. \tag{122}$$

The following facts are proved easily by a direct computation, see [Sil09, Section VI].

- The series (122) converges absolutely, and uniformly on compact open subsects of $\mathbf{C}$,
- Its Laurent series expansion around $z = 0$ is given by

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{k \geq 1} (2k+1) G_{2k}(\Lambda) z^{2k}, \qquad \text{where} \quad G_{2k}(\Lambda) = \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^{2k}}. \tag{123}$$

A short argument shows that the first statement implies that the function $\wp(z)$ is invariant under translation by Λ. We say that $\wp_\Lambda$ is an *elliptic function* for Λ. Furthermore, by computing the first few coefficients of the Laurent series expansion of both sides, we obtain the relation

$$\wp'_\Lambda(z) = 4\wp_\Lambda(z)^3 - 60G_4(\Lambda)\wp_\Lambda(z) - 140G_6(\Lambda). \tag{124}$$

The functions $\wp\Lambda, \wp'_\Lambda$ generate the function field of $\mathbf{C}/\Lambda$, so that (124) provides an algebraic equation for the elliptic curve $\mathbf{C}/\Lambda$.

The converse. The Weierstraß uniformisation theorem states that also conversely, for every elliptic curve $E/\mathbf{C}$, there exists a unique lattice Λ such that E is isomorphic to $\mathbf{C}/\Lambda$. Concretely, if

$$\{\alpha, \beta\} \quad \text{is a basis for} \quad \mathrm{H}_1(E(\mathbf{C}), \mathbf{C}) \tag{125}$$

then the quantities

$$\Omega_1 = \int_\alpha \frac{dx}{y}, \qquad \Omega_2 = \int_\beta \frac{dx}{y} \tag{126}$$

are independent over $\mathbf{R}$, and if $\Lambda = \langle \Omega_1, \Omega_2 \rangle$ is the lattice generated by these two periods, then we have a complex analytic isomorphism

$$E(\mathbf{C}) \longrightarrow \mathbf{C}/\Lambda : \quad z \longmapsto \int_0^z \frac{dx}{y} \pmod{\Lambda}. \tag{127}$$

The real period. When E is defined over a subfield of $\mathbf{R}$, it makes sense to consider $E(\mathbf{R})$, which is a real Lie group, and hence isomorphic to either

$$E(\mathbf{R}) \simeq \left\{ \begin{array}{cl} S^1 & \text{if} \\ S^1 \times \mathbf{Z}/2\,\mathbf{Z} & \text{if} \end{array} \right. \tag{128}$$

Given a minimal Weierstraß model of the form (121) above, we define the *Néron differential* to be

$$\omega_{\text{Nér}} = \frac{dx}{2y + a_1 x}. \tag{129}$$

The real period is then defined to be

$$\Omega_E^+ = \int_{E(\mathbf{R})} \omega_{\text{Nér}}. \tag{130}$$

A.2. Elliptic curves over a local field.

A.3. The Birch–Swinnerton-Dyer conjecture.

A.3.1. *The Tate–Shafarevich group.* Mordell-Weil Proof via Selmer, define Tate–Shafarevich.

A.3.2. *The Néron canonical height.*

A.3.3. *The root number and functional equation.*

A.3.4. *The BSD conjecture.* Having defined all these various quantities above, we can now state the Birch–Swinnerton-Dyer conjecture, which predicts a deep relation between the analytically defined L-function of an elliptic curve E over $\mathbf{Q}$, and various pieces of arithmetic data, most notably the rank of $E(\mathbf{Q})$. More precisely, it states that

Conjecture A.1. *Let E be an elliptic curve over $\mathbf{Q}$, with Mordell–Weil group of rank r. Then its L-function analytically continues to the entire complex plane, and the order of vanishing at $s = 1$ is precisely equal to r. The leading term in its Taylor expansion at that point is given by*

$$\frac{\mathrm{L}_E^{(r)}(1)}{r!} = \frac{|\text{Ш}_E| \cdot \Omega_E^+ \cdot R_E \cdot \prod_p c_p}{|E(\mathbf{Q})_{\text{tor}}|^2}. \tag{131}$$

This conjecture is wide open, though many partial results exist in the cases where the rank is 0 or 1. The theorem of Gross–Zagier, as well as its various subsequent generalisations, remains one of the more significant results towards this conjecture, as it manages to show the existence of points of infinite order in case the analytic rank is equal to 1. These points are provided by the theory of Heegner points.

Appendix B. Modular forms and the Hecke algebra

B.1. Modular forms of integral weight. Suppose $k \in \mathbf{Z}$ and Γ is a congruence subgroup of $\mathrm{SL}_2(\mathbf{Z})$. A *weakly holomorphic modular form* of weight k and level Γ is a holomorphic function $f : \mathfrak{H} \to \mathbf{C}$ such that

$$f\left(\frac{a\tau + b}{c\tau + d}\right)(c\tau + d)^{-k} = f(\tau), \qquad \text{for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma. \tag{132}$$

The *cusps* of Γ are the finitely many Γ-orbits on $\mathbf{P}^1(\mathbf{Q})$. If in addition, f is holomorphic at the cusps of Γ, then we call f a *holomorphic modular form* or simply *modular form*. The space of modular forms of weight k and level Γ is denoted by $M_k(\Gamma)$, and the subspace spanned by forms that vanish at all the cusps (which are called *cusp forms*) is denoted by $S_k(\Gamma)$. Assume for simplicity that the translation matrix T belongs to Γ (in general, some power of it always does) then any modular form f has a Fourier expansion

$$f(q) = a_0 + a_1q + a_2q^2 + a_3q^3 + a_4q^4 + \dots \qquad a_i \in \mathbf{C}, q = e^{2\pi i\tau} \tag{133}$$

which is referred to as its *q-expansion.*

The following basic facts about modular forms will be used without further mention, their proofs can be found in [Ser77, DS05].

- The spaces $M_k(\Gamma)$ are finite-dimensional, and trivial for $k < 0$,
- The space $S_2(\Gamma)$ is isomorphic to the space of differentials on the modular curve $X(\Gamma)$ (for definitions, see next section) via the map $f(\tau) \mapsto f(\tau)d\tau \pmod{\Gamma}$,
- The spaces $S_k(\Gamma)$ are endowed with an inner product, called *Petersson inner product*, defined by

$$\langle f, g\rangle = \int_{\Gamma\backslash\,\mathfrak{H}} f(x+iy)\overline{g(x+iy)}y^{k-2}dxdy. \tag{134}$$

B.2. **Modular curves.**

B.3. **Hecke algebras.** The reason that modular forms enter in number theory at all, is probably the fact that modular curves are defined over $\mathbf{Q}$ (or some number field that depends on the level structure), and that there exist Hecke operators which are defined over the same field.

Hecke

Diamond, Atkin-Lehner

B.4. **Modular forms of half-integral weight.** Let us first define the prototypical example of a form of weight $1/2$, on which our general definition will be modelled. Define

$$\theta(z) = \sum_{n\in\mathbf{Z}} q^{n^2} = 1 + 2q + 2q^4 + \dots \tag{135}$$

which is a holomorphic form on $\mathfrak{H}$ such that θ^2 is a weight 1 modular form for $\Gamma_1(4)$ with non-trivial nebentypus χ_4. This means that θ itself should be considered a modular form of weight $1/2$, a notion which we now formalise.

Let k be an integer, and define $G_{k+1/2}$ to be the group consisting of pairs $(\gamma, \phi(z))$ where $\gamma \in \mathrm{GL}_2^+(\mathbf{R})$ and $\phi(z)$ is a complex valued holomorphic function on $\mathfrak{H}$ satisfying

$$|\phi(z)| = (\det\gamma)^{-k/2-1/4}|cz+d|^{k+1/2} \tag{136}$$

where the group law is defined by the rule

$$(\gamma_1, \phi_1(z)) \cdot (\gamma_2, \phi_2(z)) = (\gamma_1\gamma_2, \phi_1(\gamma z)\phi_2(z))\,. \tag{137}$$

We define an action of $G_{k+1/2}$ on the set of functions $f : \mathfrak{H} \to \mathbf{C}$ by setting

$$f|(\gamma, \phi(z)) = \phi(z)^{-1}f(\gamma z). \tag{138}$$

We let $\widetilde{\Gamma}(4N)_\chi$ be the subgroup of $G_{k+1/2}$ consisting of pairs $(\gamma, \phi(z))$ where $\gamma \in \Gamma_0(4N)$ and

$$\phi(z) = \chi(d)\left(\frac{c}{d}\right)\left(\frac{-4}{d}\right)^{-k-1/2}(cz+d)^{k+1/2}. \tag{139}$$

A modular form of weight $k + 1/2$ on $\Gamma_0(4N)$ with nebentypus χ is a holomorphic function $f : \mathfrak{H} \to \mathbf{C}$ which is holomorphic at the cusps and satisfies

$$f|(\gamma, \phi(z)), \qquad \forall(\gamma, \phi(z)) \in \widetilde{\Gamma}_0(4N) \tag{140}$$

Remark. It should be noted that geometric definitions remain difficult, and are the subject of much recent research.

References

[Cox89] D. Cox. *Primes of the form* $x^2 + ny^2$. Wiley-Interscience, 1989. ↑7, 8, 12.

[DS05] F. Diamond and J. Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005. ↑5, 24.

[GKZ87] B. Gross, W. Kohnen, and D. Zagier. Heegner points and derivatives of L-series ii. *Math. Ann.*, 278:497–562, 1987. ↑15, 17, 19.

[GZ86] B. Gross and D. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986. ↑15.

[Ham12] A. Hamieh. Ternary quadratic forms and half-integral weight modular forms. *LMS J. Comp. Math.*, 15:418–435, 2012. ↑17.

[Koh85] W. Kohnen. Fourier coefficients of modular forms of half-integral weight. *Math. Ann.*, 271:237–268, 1985. ↑18.

[Ser77] J.-P. Serre. *Cours d'arithmétique*. Presses Universitaires de France, Paris, 1977. ↑24.

[Sil09] J. Silverman. *The arithmetic of elliptic curves, 2nd edition*, volume 106 of *GTM*. Springer-Verlag, 2009. ↑22.

[Wal81] J.-L. Waldspurger. Sure les coefficients de Fourier des formes modulaires de poids demi-entier. *J. Math. pures et appl.*, 60:375–484, 1981. ↑17, 18.

[Zag85] D. Zagier. Modular points, modular curves, modular surfaces, and modular forms. In *Arbeitstagung Bonn 1984*, volume 1111, pages 225–248, Berlin-Heidelberg-New York, 1985. Springer-Verlag. ↑1, 19.

Department of Mathematics and Statistics, Burnside Hall, 805 Sherbrooke Street West, Montreal, QC, Canada, H3A 0B9

E-mail address: jan.vonk@mcgill.ca