UiO : Department of Mathematics
University of Oslo

Congruent numbers, elliptic curves and Heegner points

Genís Calderer i Garcia

Master's Thesis, Spring 2023

This master's thesis is submitted under the master's programme *Mathematics*, with programme option *Mathematics*, at the Department of Mathematics, University of Oslo. The scope of the thesis is 60 credits.

The front page depicts a section of the root system of the exceptional Lie group E_8, projected into the plane. Lie groups were invented by the Norwegian mathematician Sophus Lie (1842–1899) to express symmetries in differential equations and today they play a central role in various parts of mathematics.

Abstract

Abstract A congruent number is a positive integer that appears as the area of a right triangle with rational sides. Determining whether a number n is congruent is equivalent to studying the rank of the elliptic curve $y^2 = x^3 - n^2x$. This thesis provides an overview of the theory of elliptic curves with a focus on the rank, along with examples of congruent number elliptic curves. It also explains the paper *Mock Heegner points and congruent numbers* by Monsky, which presents a method for finding non-torsion points on these curves in specific cases.

Abstract Un nombre congruent és un enter positiu que apareix com a àrea d'un triangle rectangle amb costats racionals. El problema de determinar si un enter n és congruent, és equivalent a estudiar el rang de la corba el · líptica $y^2 = x^3 - n^2x$. Aquesta tesi dóna una visió general de la teoria de corbes el · líptiques amb emfàsi en el rang, i amb exemples de les corbes el · líptiques corresponents a nombres congruents. També es presenta l'article de Monsky, *Mock Heegner points and congruent numbers*, que dóna un mètode per trobar punts d'ordre infinit en aquestes corbes en alguns casos particulars.

Sammendrag Et kongruent tall er et positivt heltall som dukker opp som arealet av en rettvinklet trekant med rasjonelle sider. Å bestemme om et tall n er kongruent tilsvarer å studere rangen til den elliptiske kurven $y^2 = x^3 - n^2x$. Denne masteroppgaven gir en oversikt over teorien om elliptiske kurver med fokus på rangen, sammen med eksempler på kongruent tall elliptiske kurver. Den forklarer også artikkelen *Mock Heegner points and congruent numbers* av Monsky, som presenterer en metode for å finne ikke-torsjonspunkter på disse kurvene i noen spesifikke tilfeller.

Preface

A positive integer n is called *congruent* if it appears as the area of a right-angle triangle with rational sides. There are known to be infinite congruent numbers, the smallest being 5. However, given n, it is not straightforward to know if it is congruent. This poses what is called *the congruent number problem*: Given n, is there an algorithm that can determine whether n is congruent in a finite number of steps? It turns out that this problem is equivalent to checking where the elliptic curve $y^2 = x^3 - n^2x$ has a rational point of infinite order, so it can be studied through the theory of elliptic curves.

This thesis provides an overview of some of the tools that are used to study the rank of elliptic curves, and construct rational points on them, and concludes with an exposition of the paper *Mock Heegner points and congruent numbers* ([Mon90]) by Paul Monsky, which builds up on this theory to prove among other things that primes $p \equiv 5 \pmod 8$ are congruent numbers, and so are numbers of the form $2p$ when $p \equiv 3 \pmod 8$.

Structure of the thesis

This thesis consists of four chapters.

The first chapter provides a first introduction to the congruent number problem and shows the equivalence with the computation of the rank of the curves $y^2 = x^3 - n^2x$.

The second chapter covers the main arithmetic tools that are used to study elliptic curves over a number field: reductions, some cohomological constructions, and the weak Mordell-Weil theorem. These tools are then used in some examples pertaining to the congruent number problem, in particular, we show that primes $p \equiv 3 \pmod 8$ are not congruent.

The third chapter gives an overview of the theory of elliptic curves with complex multiplication and the theory of modular curves and modular functions. These theories are then put together into defining Heegner points, which allow us to construct points in an elliptic curve that are rational on quadratic imaginary fields.

The fourth chapter gives an exposition of the *Mock Heegner points and congruent numbers* paper, which uses the ideas of the previous chapter to show some general results on the congruence of primes. Finally, the construction in this paper is showcased by a Mathematica implementation for the primes $p = 5$ and $p = 29$.

The main references of this thesis are the books *Arithmetic of elliptic curves* ([Sil09]), and, *Advanced topics in the arithmetic of elliptic curves*([Sil94]) by J. Silverman. *Elliptic curves* ([Mil06] by J.S Milne and the paper by Monsky ([Mon90]). Special mentions to the books by Lozano-Robledo ([Loz11]) and Cohen ([Coh07]).

Ackwnoledgements

I would first like to thank my advisor, Kristian Ranestad, for suggesting this topic, for his assistance, for interesting discussions, and for keeping me on track.

Vull agraïr a tothom que ha fet possible aquesta aventura lluny de casa, especialment als meus pares. Sóc molt afortunat de tenir la família i els amics que tinc. Us estimo i aprecio infinitament.

I would like to thank the friends I have made in Oslo. I am especially thankful to Rebeka and Gianni, for lots of great moments during these two years, for enduring my endless complaining, and for being my allies in this city.

Finalment, i més importantment, vull agraïr a la persona sense la que no podria dir que sóc. Gràcies Gerard pel teu suport etern. Moltes gràcies per ser la meva roca, el meu refugi i el meu spren.

Contents

CHAPTER 1

The congruent number problem

Definition 1.0.1. A positive integer n is called *congruent* if it appears as the area of a right-angle triangle with rational sides, that is, there are $a, b, c \in \mathbb{Q}$ satisfying the equations $a^2 + b^2 = c^2$ and $ab = 2n$.

Remark 1.0.2. As an immediate remark, given n, m positive integers, n is congruent if and only if $m^2 n$ is congruent. Therefore we restrict our study to square-free integers.

Example 1.0.3. The numbers $1, 2$ and 3 are known not to be congruent numbers, we prove this fact in corollary 2.4.5 and lemmas 2.5.1 and 2.5.2. The number 5 is the smallest congruent number, we prove that it is section 2.5.

There are several equivalent definitions for congruent numbers ([Con]), that allow for the study of the problem using fancier techniques, in particular, the following definition is in terms of elliptic curves, which have an extensive theory.

Theorem 1.0.4. Let n be a square-free positive integer. The following are equivalent:

1. The number n is a congruent number.
2. The elliptic curve E defined by $y^2 = x^3 - n^2 x$ has a rational point of infinite order. By the Mordell-Weil theorem, $E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$, r is called the rank of E. The property is equivalent to the rank of E being at least 1.

Proof. We want to rewrite the system of equations

$$a^2 + b^2 = c^2 \tag{1.1}$$

$$ab = 2n \tag{1.2}$$

into an elliptic curve. Write $c = a + t$ for some rational $t \neq 0$. The first equation becomes then $b^2 - t^2 = 2at$, and since $b \neq 0$, we can substitute a using the second equation to obtain $b^3 - t^2 b = 4nt$. Since $t \neq 0$, we can multiply the equation by $\frac{n^3}{t^3}$ to get the following,

$$\left(\frac{bn}{t}\right)^3 - \left(\frac{bn}{t}\right)n^2 = \left(\frac{2n^2}{t}\right)^2,$$

writing $x = \frac{bn}{t}$ and $y = \frac{2n^2}{t}$ we obtain the elliptic curve $E : y^2 = x^3 - n^2 x$. Since all the steps are reversible, we have the equivalence. Given a rational point (x, y) on E, we can solve for a, b, c:

$$\begin{aligned} a &= \frac{y}{x} \\ b &= \frac{2nx}{y} \\ c &= \frac{n^2 - x^2}{y}. \end{aligned}$$

The curve E has the obvious rational solutions $(0, 0)$, $(n, 0)$ and $(-n, 0)$, these do not correspond to triangles, note that in this case a, b, c are not well-defined. It turns out that these points, as well as the point at infinity, make up the whole torsion group of E defined over $\mathbb{Q}$. Therefore, the points in E that produce triangles are the points of infinite order. ■

We have therefore transformed the congruent number problem into the problem of computing the rank of curves of the form $y^2 = x^3 - n^2 x$. This approach not only gives a possible method to ascertain whether a given integer is a congruent number but it also gives a way to build the realizing triangle if we can compute the weak Mordell-Weil group (defined in theorem 2.3.1). For a given congruent n, there are infinite triangles that realize it as a congruent number, one of the advantages of the elliptic curve approach is that given two realizing triangles for n, we can build another one through the group law on E.

Remark 1.0.5. This particular transformation is the most usual characterization of congruent numbers through elliptic curves, but different changes of variables can yield other families of elliptic curves for which the equivalence also holds. In particular, in chapter 4 we use the elliptic curves $ny^2 = x^3 - x$, which are isomorphic over $\mathbb{Q}$ to the curves defined in this chapter.

The next chapter explores the structure of the group of rational points of an elliptic curve and gives some examples of the computation.

There is an algorithm that computes the rank of an elliptic curve, its finitude is however conditional on the Tate-Shafarevich conjecture, that states that the Tate-Shafarevich group is finite. If that were to be true for the family of elliptic curves of the form above (as it is expected to be), the we would be assured that the algorithm would compute the rank in a finite number of steps and it would settle the congruent number problem.

Current state

We state some elementary, and not so elementary results. These can be proved using the elliptic curve definition and the theory of modular functions. It is conjectured that all square-free numbers n such that $n \equiv 5, 6$ or $7 \pmod 8$ are congruent numbers. It was shown by J. Chahal in 1984 that the other residue classes $\bmod 8$ also contain congruent numbers. Later on, in 2002, M. Bennet generalized the result to residue classes modulo a general m.

Theorem 1.0.6 (Chahal)**.** Every non-square residue class modulo 8 contains infinitely many congruent numbers.

Proof. Theorem 2 in [Cha06]. ■

Theorem 1.0.7 (Bennet)**.** Given $m \geq 2$, every residue class modulo m contains infinitely many congruent numbers.

Proof. [Ben02]. ■

In the elliptic curve formulation, the result by Bennet was extended by J. Johnstone in 2010, to show that not only there are infinitely many congruent numbers in each residue class modulo $m \geq 2$, but there are also infinitely many so that the rank of the congruent number elliptic curve has a lower bound.

Theorem 1.0.8 (Johnstone)**.** Given $m \geq 2$, every residue class modulo m contains infinitely many congruent numbers such that the corresponding elliptic curve has rank at least 2.

Proof. [Joh10]. ■

The conjecture stated above is proved in almost all cases where n is the product of two primes or twice the product of two primes. The paper *Mock Heegner points and congruent numbers* by P. Monsky that we present in Chapter 4 gives this result. Denote p_i a prime such that $p_i \equiv i \pmod 8$.

Proposition 1.0.9. The primes p_3 are not congruent.

Proof. Proved in lemma 2.5.2 in chapter 2. ■

Theorem 1.0.10 (Monsky)**.** The following are congruent numbers:

1. p_5, p_7, $2p_7$ and $2p_3$.

2. p_3p_7, p_3p_5, $2p_3p_5$ and $2p_5p_7$.

3. p_1p_5 if $\left(\frac{p_1}{p_5}\right) = -1$, p_1p_7 and $2p_1p_7$ if $\left(\frac{p_1}{p_7}\right) = -1$ and $2p_1p_3$ if $\left(\frac{p_1}{p_3}\right) = -1$.

Proof. The full result is in [Mon90]. Chapter 4 presents the construction in the paper and proves the cases p_5 and $2p_3$. ∎

Finally, the congruent number problem was settled by Tunell in 1983 conditionally to the Birch and Swinerton-Dyer (BSD) conjecture. Therefore this is not an unconditional result, but the BSD conjecture is expected to be true. The theorem says that to check if a given n is congruent we need only compare the cardinality of two finite sets.

Theorem 1.0.11 (Tunell's theorem)**.** Assuming BSD, for a square-free natural number n, let $d = 1$ if n is odd and $d = 2$ if n is even. Define the sets $N_1 = \{(a, b, c) \in \mathbb{Z}^3 \mid \frac{n}{d} = 2da^2 + b^2 + 8c^2\}$ and $N_2 = \{(a, b, c) \in \mathbb{Z}^3 \mid \frac{n}{d} = 2da^2 + b^2 + 32c^2\}$. Then n is congruent precisely when $|N_1| = 2|N_2|$.

Proof. [Tun83] ∎

CHAPTER 2

The weak Mordell-Weil theorem

This chapter, mainly based on [Sil09] and [Mil06], provides an overview of the arithmetic tools used to prove the weak Mordell-Weil, as well as some examples. We give the main definitions and results on elliptic curves defined over local fields, some tools used to study the groups $E(K)/mE(K)$ and $E[m]$, and we prove the weak Mordell-Weil theorem, which states that $E(K)/mE(K)$ is finite for any $m \geq 2$ and any number field K. Finally, these results are used to show that 1,2, and 3 are not congruent numbers and that 5 is.

2.1 Elliptic curves over a local field and reduction

Let K be a local field complete with respect to a valuation v. Let R be its ring of integers, which is a local ring with maximal ideal $\mathfrak{m}$. For simplicity we will suppose that K is a finite extension of $\mathbb{Q}_p$ and therefore $k = R/\mathfrak{m}R$ is a finite field of characteristic p. Let E be an elliptic curve over K, through the Riemann-Roch theorem, E has a Weierstrass equation,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.1}$$

with $a_i \in K$. Since we want to study the curve in the reductions modulo π and the characteristic of k could be 2 or 3, we don't have in general the reduced equation of the form $y^2 = x^3 + Ax + B$. We can however obtain an equation such that all the a_i are integral ($v(a_i) \geq 0$) and it satisfies a minimality condition. The substitutions $(x, y) \mapsto (u^{-2}x, u^{-3}y)$ give a new Weierstrass equation where the a_i becomes u^ia_i, so for a u sufficiently big (with respect to v) we can assume $a_i \in R$. Furthermore, in this case $\Delta \in R$, so $v(\Delta) \geq 0$. Since the valuation is discrete, there's a change u such that the $a_i \in R$ and $v(\Delta)$ is minimal.

Remark 2.1.1. The substitution $(x, y) \mapsto (u^{-2}x, u^{-3}y)$ changes the discriminant by $\Delta \mapsto u^{-12}\Delta$, therefore $v(\Delta)$ changes only by multiples of 12. If the $a_i \in R$ and $v(\Delta) < 12$ then the equation is minimal.

Definition 2.1.2. Let $E|K$ be an elliptic curve. A *minimal Weierstrass equation* is a Weierstrass equation subject to the condition that $a_i \in R$ and $v(\Delta)$ is minimal. The minimality condition assures that reduction modulo $\mathfrak{m}$ is as well-defined as possible.

Remark 2.1.3. Suppose E is an elliptic curve defined over the global field $\mathbb{Q}$, and p is a prime. We can consider $E|\mathbb{Q}_p$, defined over the completion with respect to the p-adic valuation v_p. Then $E|\mathbb{Q}_p$ will have a minimal Weierstrass equation. What cannot be assured, however, is that this equation is minimal over all $\mathbb{Q}_p$ when p runs through all primes of $\mathbb{Q}$.

Reduction modulo $\mathfrak{m}$

Since $\mathfrak{m}$ is a maximal ideal of R, we have that $R/\mathfrak{m}$ is a field, and by the assumption that K is a finite extension of some $\mathbb{Q}_p$ we have that $R/\mathfrak{m}$ is a finite field k of characteristic p. Given an elliptic curve $E|K$ with a minimal Weierstrass equation, we can reduce its coefficients modulo $\mathfrak{m}$ to obtain an equation over k. This equation defines a curve $\tilde{E}(k)$ and we obtain a reduction map,

$$\begin{aligned} E(K) &\longrightarrow \tilde{E}(k) \\ P &\longmapsto \tilde{P} \end{aligned}$$

by reducing the coordinates of P mod $\mathfrak{m}$. If $v(\Delta) = 0$, then we have that $\Delta \neq 0$ in k, and $\tilde{E}(k)$ is once again an elliptic curve, in such situation we say E has *good reduction* modulo $\mathfrak{m}$. This need not be the case, there can be singular points on the reduced curve. We denote $\tilde{E}_{\mathrm{ns}}(k)$ the set of non-singular points of $\tilde{E}(k)$. This leads us to the following definition.

Definition 2.1.4. Let $E|K$. We define the following subgroups of $E(K)$.

1. $E_0(K) = \{P \in E(K) \mid \tilde{P} \in \tilde{E}_{\mathrm{ns}}(k)\}$.
2. $E_1(K) = \{P \in E(K) \mid \tilde{P} = \tilde{O}\}$, the kernel of the reduction map.

Note that if E has good reduction then $\tilde{E}_{\mathrm{ns}}(k) = \tilde{E}(k)$ and $E_0(K) = E(K)$.

Proposition 2.1.5. Let $E|K$. The subgroups $E_0(K), E_1(K)$ sit in an exact sequence,

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \longrightarrow \tilde{E}_{\mathrm{ns}}(k) \longrightarrow 0, \tag{2.2}$$

where the last map is the reduction map. In particular, the reduction is surjective.

Proof. The proof is based on Hensel's lemma and can be found in [Sil09]VII.2.1. ■

As mentioned before, when reducing an elliptic curve defined by a minimal Weierstrass equation, if $v(\Delta) = 0$, then $\tilde{E}(k)$ will again be an elliptic curve. It can happen that $v(\Delta) > 0$, in such cases $\tilde{E}(k)$ will have singular points.

Definition 2.1.6. Let $E|K$ be an elliptic curve.

1. E has *good reduction* if $\tilde{E}(k)$ is non-singular (if $v(\Delta) = 0$).
2. E has *bad, multiplicative reduction* if $\tilde{E}(k)$ has a node.
3. E has *bad, additive reduction*, if $\tilde{E}(k)$ has a cusp.

Remark 2.1.7. The terminology multiplicative or additive reduction comes from the fact that if $E|K$ has multiplicative (resp. additive) reduction, then $\tilde{E}_{\mathrm{ns}}(\overline{k}) \simeq \overline{k}^{\times}$ (resp. $\tilde{E}_{\mathrm{ns}}(\overline{k}) \simeq \overline{k}^{+}$).

Remark 2.1.8. Let $L|K$ be a finite extension (of local fields). Then the valuation v_K extends to L in a unique way. In particular, if e is the ramification index of $L|K$, $v_L = ev_K$. This means that a Weierstrass equation that was minimal over K might no longer be minimal over L, and the reduction type could change over a field extension.

Definition 2.1.9. We say $E|K$ has *potential good reduction* if there is a finite extension $L|K$ such that $E|L$ has good reduction.

If $E|K$ has potential good reduction then we can always extend the field so that the Weierstrass equation can be minimized further and the curve has good reduction. This is only possible when the reduction is multiplicative ([Sil09]VII.5).

We conclude this section with a very straightforward example.

Example 2.1.10. Let d be a square-free integer and $E|\mathbb{Q}$ the associated congruent number curve given by $y^2 = x^3 - d^2x$. This equation has discriminant $\Delta = -2^6d^6$. The coefficients are integral and for any $p \not| \Delta$ we have that $v_p(\Delta) = 0$, therefore the curve defined over $E|\mathbb{Q}_p$ has good reduction. Suppose $p|\Delta$ and p odd, then $v_p(\Delta) = 6$, so the given equation is minimal over $\mathbb{Q}_p$, but the curve will have additive bad reduction because the reduced equation is $y^2 = x^3$, which has a cusp. If d is even and $p = 2$ the equation is no longer minimal because $v_2(\Delta) = 12$ but it will have additive bad reduction nonetheless. If d is odd, then the reduction at 2 will have a node. Thus we have seen that the elliptic curve for a congruent number d has good reduction at all primes but the ones that divide d.

Torsion

Proposition 2.1.11. Let K be a local field, $E|K$ be an elliptic curve and $m \geq 1$ an integer relatively prime to char k.

1. The subgroup $E_1(K)$ is m-torsion free.
2. If E has good reduction on k, then $E(K)[m]$ injects on $\tilde{E}(k)$ through the reduction map.

Proof. (1) is a consequence of the theory of formal group laws which is not covered in this thesis ([Sil09]IV). (2) Taking m-torsion of abelian groups is left-exact. We take m-torsion on the exact sequence in proposition 2.1.5. By (1) and the remark after definition 2.1.4 we obtain

$$0 \longrightarrow E(K)[m] \longrightarrow \tilde{E}(k).$$

■

If K is now a global field, and v a place[1]of K, we have that $E(K)$ injects into $E(K_v)$, so $E(K)_{\text{tors}}$ injects into $E(K_v)_{\text{tors}}$. This is used to compute the torsion group over global fields. The following example computes the torsion group for the congruent number elliptic curves.

Example 2.1.12. Let d be a square-free positive integer and let $E : y^2 = x^3 - d^2x$ be the associated congruent number elliptic curve. We show that $E(\mathbb{Q})_{\text{tors}} = E[2] = (\mathbb{Z}/2\mathbb{Z})^2$. The curve has good reduction at all primes that don't divide $2d$ and in these cases the reduced equation is minimal. For $p \not| 2d$ we have that $E(\mathbb{Q})_{\text{tors}}$ injects into $\tilde{E}(\mathbb{F}_p)$. We use the following lemma, given without proof ([Sil09]V.4.1).

Lemma 2.1.13. Let $E : y^2 = f(x)$ be an elliptic curve.

1. Let q be a power of an odd prime such that $f \in \mathbb{F}_q[x]$ has different roots in $\overline{\mathbb{F}_q}$. Then E is supersingular if and only if the coefficient of x^{p-1} in $(f(x))^{(p-1)/2}$ is zero.
2. Let $p \geq 5$ be prime. Then $\tilde{E}$ is supersingular if and only if $\tilde{E}(\mathbb{F}_p) = p + 1$.

A quick computation shows that if $p \equiv 3 \pmod 4$, then $(x^3 - d^2x)^{(p-1)/2}$ does not have x^{p-1} term. We get then that for infinitely many $p \equiv 3 \pmod 4$,

[1] A *place* of a number field K is an equivalence class of absolute values of K. The *finite places* correspond to the non-archimedean valuations and are represented by the $\mathfrak{p}$-adic valuations, for $\mathfrak{p} \subseteq \mathcal{O}_K$ a prime ideal. The *infinite places* correspond to the archimedean valuations and are in correspondence with the embeddings of K into $\mathbb{R}$ and conjugate pairs of embeddings of K into $\mathbb{C}$.

$\tilde{E}(\mathbb{F}_p) = p+1$. Therefore, 4 divides $|E(\mathbb{Q})_{\mathrm{tors}}|$ and any other factor would divide simultaneously $p+1$ for infinitely many primes, which is impossible. We have that the points O, $(-d, 0)$, $(0, 0)$ and $(d, 0)$ all have order 2 and therefore constitute a $(\mathbb{Z}/2\mathbb{Z})^2$. We conclude that $E(\mathbb{Q})_{\mathrm{tors}} = (\mathbb{Z}/2\mathbb{Z})^2 = \{O, (-d, 0), (0, 0), (d, 0)\}$.

Ramification (or more appropriately, unramification)

As the previous section hinted, we can study the curve over extensions of the base field, either the algebraic closure or just a finite extension, and see if the reduction type changes. Let $L|K$ be a finite extension and R_L the ring of integers of L. The maximal ideal $\mathfrak{m}$ of R, has only one divisor $\mathfrak{m}_L$ in R_L, and we have that $\mathfrak{m}_L = \mathfrak{m}^e$ in R_L for some $e \geq 1$ called the ramification index.

Definition 2.1.14. Let $\overline{K}$ be the algebraic closure of K, and let K^{un} the maximal unramified extension of K in $\overline{K}$. By Galois theory we have an exact sequence,

$$1 \longrightarrow \mathrm{Gal}(\overline{K}|K^{\mathrm{un}}) \longrightarrow \mathrm{Gal}(\overline{K}|K) \longrightarrow \mathrm{Gal}(K^{\mathrm{un}}|K) \longrightarrow 1,$$

We call the group $I = \mathrm{Gal}(\overline{K}|K^{\mathrm{un}})$ the inertia subgroup of $G = \mathrm{Gal}(\overline{K}|K)$. A set Σ with a G-action is called *unramified* if the action restricted to I is trivial. We can identify $\mathrm{Gal}(K^{\mathrm{un}}|K)$ with $\mathrm{Gal}(\overline{k}|k)$, therefore the action of I on $\overline{k}$ through the reduction map is trivial.

Let K now be a global field. For each place v of K, we have an inertia subgroup I_v corresponding to the completion K_v. If Σ is a set with an action by $\mathrm{Gal}(\overline{K}|K)$, we say it is *unramified at v* if the action of I_v is trivial.

Proposition 2.1.15. Let K be a local field and $E|K$ be an elliptic curve with good reduction. Let $m \geq 1$ be relatively prime to char k. Then $E[m]$ is unramified.

Proof. The group $E[m]$ need not be defined over K so we pass to a finite extension $K'|K$ such that $E[m] \subseteq E(K')$. The curve has good reduction to k, so minimal Weierstrass equations will stay minimal in K', and $v(\Delta) = 0$ implies $v'(\Delta) = 0$. Therefore $\tilde{E}(k')$ is non-singular and we may suppose then that $E[m] \subseteq K$. Let $\sigma \in I$, we have that σ acts trivially on $\tilde{E}(k)$. Let $P \in E[m]$. Then

$$\widetilde{\sigma(P) - P} = \sigma(\tilde{P}) - \tilde{P} = \tilde{O}$$

in $\tilde{E}(k)$. By proposition 2.1.11 the reduction map is injective, so $\sigma(P) = P$ and $E[m]$ is unramified. ■

2.2 Arithmetic tools on an elliptic curve

Let K be a number field, not necessarily algebraically closed. Let $m \geq 2$. In this section, we will introduce three pairings: the Weil pairing, the Kummer pairing, and the b-pairing.

The Weil pairing

The Weil pairing is a tool to study the arithmetic of the m-torsion of an elliptic curve through a bilinear form on $E[m]$ considered as a $\mathbb{Z}/m\mathbb{Z}$-module. The construction of the Weil pairing is technical and can be found in [Sil09]III.8. We only state its properties.

Proposition 2.2.1 (Properties of the Weil pairing)**.** Let $E|K$ be an elliptic curve and $m \geq 0$. Let $e_m : E[m] \times E[m] \longrightarrow \mu_m$ be the Weil pairing.

1. (Bilinearity). Let $S_1, S_2, T \in E[m]$. Then,

$$\begin{aligned} e_m(S_1 + S_2, T) &= e_m(S_1, T) \cdot e_m(S_2, T), \\ e_m(T, S_1 + S_2) &= e_m(T, S_1) \cdot e_m(T, S_2). \end{aligned}$$

2. (Alternation) For $T, S \in E[m]$,

$$\begin{aligned} &e_m(T, T) = 1, \\ &e_m(S, T) = e_m(T, S)^{-1}. \end{aligned}$$

3. (Non-degeneracy) If $e_m(T, S) = 1$ for all $T \in E[m]$ then $S = 0$.

4. (Galois invariance) Let $\sigma \in \mathrm{Gal}(\overline{K}|K)$ and $S, T \in E[m]$,

$$e_m(T, S)^\sigma = e_m(T^\sigma, S^\sigma).$$

5. (Compatibility with restrictions) Let $T \in E[mm']$, $S \in E[m]$, then,

$$e_{mm'}(T, S) = e_m([m']T, S).$$

Proof. [Sil09]III.8.1 ■

Remark 2.2.2. The explicit construction of the Weil pairing is hardly ever used, but its existence and its nice properties are what make it useful. In particular, the Galois invariance is what makes the bilinear form on $E[m]$ interesting to study the arithmetic of the curve. The following proposition showcases this usefulness.

Proposition 2.2.3. Let $E|K$ and $m \geq 2$.

1. The Weil pairing is surjective. There are $T, S \in E[m]$ such that $e_m(T, S)$ is a primitive m-th root of unity.

2. If $E[m] \subseteq E(K)$, then $\mu_m \subseteq K^\times$.

Proof. (1) The set of all $e_m(T, S)$, where T, S vary over all $E[m]$, is a subgroup μ_d of μ_m, for a $d|m$. Fixed S, T, we have thus that $e_m(T, S)^d = 1$. By linearity $1 = e_m([d]T, S)$. This is valid for all S, so by non-degeneracy $[d]T = 0$. Since this is valid for all $T \in E[m]$, we have that $d = m$.

(2) Let ζ_m be a primitive m-th root of unity and $S, T \in E[m]$ such that $\zeta_m = e_m(T, S)$. Then, by the Galois invariance of e_m we have that for all $\sigma \in \mathrm{Gal}(\overline{K}|K)$,

$$\zeta_m^\sigma = e_m(T, S)^\sigma = e_m(T^\sigma, S^\sigma) = e_m(T, S) = \zeta_m.$$

Therefore $\zeta_m \in K$ and $\mu_m \subseteq K^\times$. ■

Example 2.2.4. As an easy corollary we see that if $K = \mathbb{Q}$ and $E[m] \subseteq E(\mathbb{Q})$ then $m = 2$ since $\mathbb{Q}$ only contains μ_2. It is thus impossible to contain all m-torsion in $\mathbb{Q}$ for $m > 2$. The developed methods usually hinge on studying a particular $E[m]$, and we will want to assume that $E[m] \subseteq E(K)$. Fortunately we focus mainly on $m = 2$ and the curves we'll want to study already have all torsion in $\mathbb{Q}$, so we will not need to work in a field extension of $\mathbb{Q}$.

Example 2.2.5. Let $E|\mathbb{Q}$ and $m = 2$. Let's explicitly build the Weil pairing for the particular case where all 2-torsion points lie in $\mathbb{Q}$, that is, $y^2 = (x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$ for $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{Q}$. Denote $P = (\lambda_1, 0)$, $Q = (\lambda_2, 0)$ and $R = (\lambda_3, 0)$, then we have that $E[2] = \{O, P, Q, R\}$. We can use the properties of the pairing to compute its matrix without having to explicitly use the construction. By bilinearity, alternation and non-degeneracy we get the following:

	O	P	Q	R
O	1	1	1	1
P	1	1	1	1
Q	1	-1	1	-1
R	1	-1	1	1

Table 2.1: Explicit $e_2 : E[2] \times E[2] \longrightarrow \mu_2$.

This applies in particular to the congruent number elliptic curves since they are of the form $y^2 = x(x-d)(x+d)$.

The Kummer pairing

Sometimes elliptic curves and number fields have similar behaviour and tools to study elliptic curves can be inspired by ideas from algebraic number theory. Under some requirements on E, there's a pairing $E[m] \times G_K \longrightarrow \mu_m$ inspired by the Kummer theory on cyclic field extensions. We first recall the case for number fields.

Proposition 2.2.6 (Kummer pairing on number fields)**.** Let K be a field that contains μ_m. Let $\overline{K}$ be its algebraic closure and G_K the absolute Galois group. There's a paring $K^\times \times G_K \longrightarrow \mu_m$.

Proof. The following sequence is exact,

$$1 \longrightarrow \mu_m \longrightarrow \overline{K}^\times \xrightarrow{\cdot m} \overline{K}^\times \longrightarrow 1. \tag{2.3}$$

Taking Galois cohomology and using Hilbert's theorem 90, we obtain the following exact sequence,

$$1 \longrightarrow \mu_m \longrightarrow K^\times \xrightarrow{\cdot m} K^\times \xrightarrow{\delta_K} H^1(G_K, \mu_m) \longrightarrow 1. \tag{2.4}$$

To construct the connecting morphism, given $x \in K^\times$ we need to define a map $\delta_K(x) : G_K \longrightarrow \mu_m$. By exactness of (2.3) there is $y \in \overline{K}^\times$ such that $y^m = x$. For any $\sigma \in G_K$, $\frac{\sigma(y)}{y}$ is in μ_m. We define thus $\delta_K(x) : G_K \longrightarrow \mu_m$ by $\sigma \mapsto \frac{\sigma(y)}{y}$ for some $y \in \overline{K}^\times$ such that $y^m = x$. This in turn defines the pairing we were after:

$$\begin{aligned} \kappa : K^\times \times G_K &\longrightarrow \mu_m \\ (x, \sigma) &\longmapsto \delta_K(x)(\sigma). \end{aligned}$$

■

Remark 2.2.7. The exact sequence (2.4) gives an isomorphism $K^\times / K^{\times m} \simeq H^1(G_K, \mu_m)$ induced by δ. Since G_K acts trivially on μ_m, we have that $H^1(G_K, \mu_m) = \mathrm{Hom}(G_K, \mu_m)$. This means that a morphism $\varphi : G_K \longrightarrow \mu_m$ is determined by an element of $x \in K^\times / K^{\times m}$ and $\varphi(\sigma) = \delta_K(x)(\sigma)$.

As hinted above, something very similar can be done for elliptic curves. In this case, the role of μ_m will be taken by $E[m]$ and the condition that K contains μ_m will be that the whole m-torsion of E is defined over K.

Proposition 2.2.8 (Kummer pairing on elliptic curves)**.** Let $E|K$ be an elliptic curve over a number field such that $E[m] \subseteq E(K)$. There is a pairing $\kappa : E(K) \times G_K \longrightarrow E[m]$.

Proof. We parallel the procedure for number fields. The following sequence is exact,

$$0 \longrightarrow E[m] \longrightarrow E(\overline{K}) \xrightarrow{[m]} E(\overline{K}) \longrightarrow 0. \tag{2.5}$$

Taking Galois cohomology, we obtain the following exact sequence,

$$0 \longrightarrow E[m] \longrightarrow E(K) \xrightarrow{[m]} E(K) \xrightarrow{\delta_E} H^1(G_K, E[m]) \longrightarrow \cdots \tag{2.6}$$

We use the exactness of (2.5) to build δ_E. For $P \in E(K)$, take $Q \in E(\overline{K})$ such that $[m]Q = P$. For any $\sigma \in G$, $Q^\sigma - Q \in E[m]$, so we can define $\delta_E(P) : G_K \longrightarrow E[m]$ by $\sigma \mapsto Q^\sigma - Q$. This gives a well-defined pairing

$$\begin{aligned} \kappa : E(K) \times G_K &\longrightarrow E[m] \\ (P, \sigma) &\longmapsto \delta_E(P)(\sigma) = Q^\sigma - Q. \end{aligned}$$

■

This pairing is the key ingredient in the proof of the weak Mordell-Weil theorem, it will allow us to transform the question on the finitude of $E(K)/mE(K)$ into a question about number fields. We give now some properties of the Kummer pairing.

Proposition 2.2.9.

1. The Kummer pairing is bilinear.
2. The kernel on the left is $mE(K)$.
3. The kernel on the right is $\mathrm{Gal}(\overline{K}|L)$, where $L = K([m]^{-1}E(K))$, the field generated over K by the coordinates of all points $\mathbb{Q} \in E(\overline{K})$ such that $[m]Q \in E(K)$. (We can think about this as taking m-th roots of the points in $E(K)$).

With these properties the Kummer pairing is a perfect bilinear pairing

$$E(K)/mE(K) \times \mathrm{Gal}(L|K) \longrightarrow E[m].$$

Proof. [Sil09]VIII.1.2 ■

The b pairing

As if three pairings were not enough, we introduce yet another one that will combine all of them, and as we will see later on, will allow us to give a computational approach to finding describing $E(K)/mE(K)$. We will build a pairing

$$b : E(K)/mE(K) \times E[m] \longrightarrow K^\times/K^{\times m}.$$

We start with an element $P \in E(K)/mE(K)$, then $\delta_E(P)(-)$ is a map $G_K \longrightarrow E[m]$. If we pick a point $T \in E[m]$, we have that $e_m(\delta_E(P)(-), T)$ is a map $G_K \longrightarrow \mu_m$, and by remark 2.2.7, it is determined by an element $b \in K^\times/K^{\times m}$ (we write $b(P,T)$ to emphasize dependence on P and T) so that $\delta_K(b(P,T), -) = e_m(\delta_E(P)(-), T)$. The following proposition summarizes this and gives some properties of this pairing b.

Proposition 2.2.10 (The b pairing)**.** . There's a bilinear paring

$$b : E(K)/mE(K) \times E[m] \longrightarrow K^\times/K^{\times m}$$

such that $\delta_K(b(P,T), -) = e_m(\delta_E(P)(-), T)$.

1. It is non-degenerate on the left.

2. Let S be the union of the set of infinite places, the set of finite places where E has bad reduction and the set of places dividing m. Then the image of the b pairing lies in the subgroup of $K^\times/K^{\times m}$ given by

$$K(S,m) = \{b \in K^\times/K^{\times m} \mid \operatorname{ord}_v(b) \equiv 0 \pmod m \ \ \forall v \notin S\}.$$

3. For each $T \in E[m]$, take $f_T, g_T \in E[m]$ as in the definition of the Weil pairing, that is, $\operatorname{div}(f_T) = m(T) - m(O)$ and $f_T \circ [m] = g_T^m$. Then, for any $P \neq T$,

$$b(P,T) \equiv f_T(P) \pmod{K^{\times m}}.$$

Proof. [Sil09]X.1.1. (1) follows easily from the properties of the Weil and Kummer pairings. (2) is a consequence of the coming theorem 2.2.11. (3) follows from the construction of the Weil pairing. ■

The maximal abelian extension of exponent m unramified outside a set S

This section gives a theorem from algebraic number theory that a priori has nothing to do with elliptic curves. It will however be the key to proving the weak Mordell-Weil theorem. Let K be a number field. We denote M_K the set of places of K. Suppose S is a finite subset of M_K containing the infinite places. If L, L' are abelian extensions of K of exponent m and unramified outside of S, then $LL'|K$ is also abelian, of exponent m and unramified outside S. Taking the composition of all of these we obtain the maximal abelian extension that satisfies these properties.

Theorem 2.2.11. The maximal abelian extension $L|K$ of exponent m unramified outside S is finite.

Proof. We give a sketch of the proof, which relies on the fact that the class number of the S-integers is finite, and the Dirichlet unit theorem for S-integers.

- Adding a finite number of places to S only makes L larger so we can do it without loss of generality. We can then assume that K contains μ_m, and that the ring of S-integers is a PID. We assume also that $v(m) = 0$ for all $v \notin S$.
- By Kummer theory, the maximal abelian extension of K of exponent m is $K(\sqrt[m]{a} \mid a \in K^\times)$. We have that $K(\sqrt[m]{a})|K$ is ramified at v if and only if $v(a) \equiv 0 \pmod{m}$, so the $K(S, m)$ as defined in 2.2.10 represents the elements of $K^\times$ that give rise to unramified extensions. We have thus that $L = K(\sqrt[m]{a} \mid a \in K(S, m))$. We show that $K(S, m)$ is finite.
- The natural map $R_S^\times \longrightarrow K(S, m)$ is surjective. Taking $a \in K(S, m)$, the ideal aR_S is $b^m R_S$ for some $b \in K$, since R_S is a PID. This means $a = ub^m$ for some $u \in R_S^\times$, which lies in the same class as a in $K(S, m)$.
- The kernel of the map contains $R_S^{\times m}$, so there is a surjection $R_S^\times / R_S^{\times m} \longrightarrow K(S, m)$ and since $R_S^\times$ is finitely generated, we get that $K(S, m)$ is finite as we wanted to see.

■

Heights

In this section, we let $K = \mathbb{Q}$. We will prove in the next section the weak Mordell-Weil theorem, which states that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. We give now a tool that is used to prove the Mordell-Weil theorem by lifting the generators of $E(\mathbb{Q})/2E(\mathbb{Q})$ into generators of $E(\mathbb{Q})$. We do not prove this result but we give the basic definitions as well as a brief comment on how this tool is used. Heights provide a way to measure the size of a point in $\mathbb{P}^n(\mathbb{Q})$ and find finite subsets where one can try to find generators of $E(\mathbb{Q})$.

Definition 2.2.12. Let $P = (x_0 : \cdots : x_n) \in \mathbb{P}^n(\mathbb{Q})$ be a point. Multiplying out denominators and eliminating common factors suppose that $x_i \in \mathbb{Z}$ and $\gcd(x_0, \ldots, x_n) = 1$. We define the *height* of P to be $H(P) = \max_i\{|x_i|\}$. We define the *logarithmic height* of P to be $h(P) = \log H(P)$.

Definition 2.2.13. Let E be an elliptic curve defined over $\mathbb{Q}$ with a Weierstrass equation. Let $P = (x : y : z) \in E(\mathbb{Q})$, we define $H(P) = H((x : z))$ if P finite and $H(\infty) = 1$. The logarithmic height can be defined accordingly, we have thus a function

$$\begin{aligned} h : E(\mathbb{Q}) &\longrightarrow [0, +\infty) \\ P &\longmapsto \log H(P). \end{aligned}$$

Remark 2.2.14. Given $M \geq 0$, the set of points in $\mathbb{P}^n(\mathbb{Q})$ such that $H(P) \leq M$ is finite, as there is only a finite amount of possibilities. Given an elliptic curve E over $\mathbb{Q}$, the set of points such that $H(P) \leq M$ is also finite, there is only a finite number of possible $(x : z)$ and for each of those, at most two points.

Remark 2.2.15. Suppose $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite and let $Q_1, \ldots, Q_s$ be generators. Let point $P \in E(\mathbb{Q})$, we have that $P = 2P_1 + Q_{i_1}$ and we can construct a sequence of $P_j = 2P_{j-1} + Q_{i_j}$. It can be seen that for a sufficiently large n, the logarithmic height of all the P_j, $j \leq n$ is less than a constant C dependent only on the Q_i and not on P. Then P can be seen as a linear combination of the $P_1, \ldots, P_n$ and $Q_1, \ldots, Q_s$, since this does not depend on P we have that $P_1, \ldots, P_n, Q_1, \ldots, Q_s$ generate $E(\mathbb{Q})$, in particular it is finitely generated. All these points have logarithmic height bounded by C, so if we are able to compute C and the points Q_i then a finite search yields generators for $E(\mathbb{Q})$. The constant is computable given the Q_i, but as we see in the following section, finding generators for $E(\mathbb{Q})/2E(\mathbb{Q})$ is far from straightforward.

2.3 The Weak Mordell-Weil theorem

The Mordell-Weil theorem states that the group of points of an elliptic curve $E|K$, where K is a number field, is a finitely generated abelian group. Thus, by the structure theorem for finitely generated abelian groups we have that

$$E(K) \simeq E(K)_{\text{tors}} \oplus \mathbb{Z}^r,$$

for some $r \geq 0$ called the rank. We have seen in section 2.1, that $E(K)_{\text{tors}}$ can be easily computed with the theory of reductions. Finding whether there are points of infinite order, that is $r > 0$, is not straightforward in general. We do not prove this theorem but will be content in proving the following.

Theorem 2.3.1 (Weak Mordell-Weil)**.** Let $E|K$ be an elliptic curve and $m \geq 2$. Then $E(K)/mE(K)$ is finite.

With the procedure described in remark 2.2.15, the Mordell-Weil theorem is proved from the weak one.

First reductions and proof

To prove the weak Mordell-Weil theorem we use the pairings developed in section 2.2. Note that the construction of the pairings required that $E[m] \subseteq E(K)$, and therefore that $\mu_m \in K$, by proposition 2.2.3. The following lemma allows us to reduce to that case.

Lemma 2.3.2. Let $E|K$ and $L|K$ be a finite Galois extension. If $E(L)/mE(L)$ is finite then $E(K)/mE(K)$ is also finite.

Proof. Let L be a finite Galois extension of K such that $E[m] \subseteq E(L)$, and suppose $E(L)/mE(L)$ is finite. We have an exact sequence

$$0 \longrightarrow E[m] \longrightarrow E(L) \longrightarrow mE(L) \longrightarrow 0.$$

Taking Galois cohomology with $\mathrm{Gal}(L|K)$ we get the following long exact sequence,

$$\begin{gathered} 0 \longrightarrow E[m](K) \longrightarrow E(K) \longrightarrow mE(L) \cap E(K) \longrightarrow \\ \longrightarrow H^1(\mathrm{Gal}(L|K), E[m]) \longrightarrow H^1(\mathrm{Gal}(L|K), E(L)), \end{gathered}$$

from which we can extract the following injection,

$$0 \longrightarrow \frac{mE(L) \cap E(K)}{mE(K)} \longrightarrow H^1(\mathrm{Gal}(L|K), E[m]).$$

Since both $E[m]$ and $\mathrm{Gal}(L|K)$ are finite, $H^1(\mathrm{Gal}(L|K), E[m])$ is finite and therefore so is $(mE(L) \cap E(K))/mE(K)$. This is the kernel of the map $E(K)/mE(K) \longrightarrow E(L)/mE(L)$, so $E(K)/mE(K)$ is finite. ■

From now on we assume that $E[m] \subseteq E(K)$. We will reformulate the finitude question into a problem in algebraic number theory that can be easily solved. By proposition 2.2.9, we have a perfect pairing

$$E(K)/mE(K) \times \mathrm{Gal}(L|K) \longrightarrow E[m].$$

That means that we have an isomorphism $E(K)/mE(K) \simeq \mathrm{Hom}(\mathrm{Gal}(L|K), E[m])$ induced by δ_E. Since $E[m]$ is finite, we have that $E(K)/mE(K)$ will be finite if and only if $L|K$ is a finite extension. Thus we focus on studying the field $L = K([m]^{-1}E(K))$, which was defined in proposition 2.2.9.

Proposition 2.3.3. Let $L = K([m]^{-1}E(K))$.

1. $L|K$ is an abelian extension of exponent m.

2. Let S be the union of the set of infinite places, the set of finite places where E has bad reduction, and the set of places dividing m. Then $L|K$ is unramified outside S.

Proof. (1) The Kummer pairing on elliptic curves induces an injective map

$$\mathrm{Gal}(L|K) \longrightarrow \mathrm{Hom}(E(K), E[m]),$$

so $\mathrm{Gal}(L|K)$ has exponent m.

(2) Let $Q \in E(L)$ so that $[m]Q \in E(K)$, and let $K' = K(Q)$. Let $v \in M_K$ and $v \notin S$, let v' be a place in K' above v. We check that K' is unramified at v'. Since $v \notin S$, E has good reduction in k_v and $E(K')$ has good reduction at $k'_{v'}$. Moreover, the Weierstrass equation will be the same and the reduction map is well-defined. Let $\sigma \in I_{v'|v}$, we have to see it acts trivially on Q. Since inertia acts trivially on $k'_{v'}$, we have that $\widetilde{\sigma(Q) - Q} = \tilde{O}$; it is in the kernel of the reduction. On the other hand,

$$[m](\sigma(Q) - Q) = \sigma([m]Q) - [m]Q = O.$$

Since $E(K')[m]$ injects into $\tilde{E}(k'_{v'})$, we get that $\sigma(Q) = Q$. This reasoning works for any $K' = K(Q)$, and any v' above v. Therefore L is unramified outside S. ■

Corollary 2.3.4 (Weak Mordell-Weil)**.** $L|K$ is finite. And therefore $E(K)/mE(K)$ is finite.

Proof. Let S be as before. The set S contains the infinite places and the extension L is contained in the maximal abelian extension of exponent m unramified outside S. Therefore, by theorem 2.2.11, L is a finite extension. ■

The Selmer and Tate-Shafarevich groups

There is another route to prove the weak Mordell-Weil theorem that gives a cohomological interpretation to the complete 2-descent procedure we will introduce in the next section. Consider the exact sequence (2.3), the full cohomology long exact sequence is

$$\begin{aligned} 0 \longrightarrow E[m] \longrightarrow E(K) \xrightarrow{[m]} E(K) \xrightarrow{\delta_E} H^1(G_K, E[m]) \longrightarrow& \\ \longrightarrow H^1(G_K, E(\overline{K})),& \end{aligned} \tag{2.7}$$

and from it, we can extract a short exact sequence,

$$0 \longrightarrow \frac{E(K)}{mE(K)} \xrightarrow{\delta_E} H^1(G_K, E[m]) \xrightarrow{\alpha} H^1(G_K, E(\overline{K}))[m] \longrightarrow 0. \tag{2.8}$$

By exactness, we have that $E(K)/mE(K)$ injects into $H^1(G_K, E[m])$ and corresponds to $\ker \alpha$.

The group $H^1(G_K, E(\overline{K}))$ can be interpreted to be the group of equivalence classes of homogeneous spaces for E, the theory of homogeneous spaces will however not be developed here and can be found in [Sil09]X.2-3. Two things worth remarking though, are the facts that a homogeneous space can be defined by an equation over K, and that the class of a homogeneous space is trivial in $H^1(G_K, E(\overline{K}))$ if and only if the corresponding equation has a point in K. Therefore we may study $\ker \alpha$ through the solvability of some equations over K. This is in general difficult so we appeal to a local-global principle. We will study the equations over completions of K at places v since over local fields we can use Hensel's lemma to solve equations. If there's a solution over every completion we can try to lift it to K. This is generally called the *Hasse principle*, and it doesn't always hold for equations of degree higher than 2; there can be equations with solutions over all completions that do not lift to a solution on K. The following constructions measure this failure.

Let $v \in M_K$ be a place, let $G_v = \mathrm{Gal}(\overline{K}_v | K_v)$. We have the following inclusions

$$\begin{tikzcd} K \arrow[r, hook] \arrow[d, hook] & K_v \arrow[d, hook] \\ \overline{K} \arrow[r, hook] & \overline{K_v} \end{tikzcd} \qquad \begin{tikzcd} G_v \arrow[r, hook] & G_K, \end{tikzcd}$$

and, by repeating the procedure in (2.7) and (2.8), we get the following commutative diagram where the rows are exact and the columns are the natural restriction maps:

$$\begin{tikzcd} 0 \arrow[r] & \frac{E(K)}{mE(K)} \arrow[r, "\delta_E"] \arrow[d] & H^1(G_K, E[m]) \arrow[r, "\alpha"] \arrow[d, "r"] \arrow[rd, bend left=10, "\beta\circ\alpha = \alpha_v\circ r"] & H^1(G_K, E(\overline{K}))[m] \arrow[r] \arrow[d, "\beta"] & 0 \\ 0 \arrow[r] & \prod_v \frac{E(K_v)}{mE(K_v)} \arrow[r, "\delta_v"] & \prod_v H^1(G_v, E(K_v)[m]) \arrow[r, "\alpha_v"] & \prod_v H^1(G_K, E(\overline{K}_v))[m] \arrow[r] & 0. \end{tikzcd}$$

We aim to replace $E(K)/mE(K)$ with a subgroup of $H^1(G_K, E[m])$ that is easier to study.

Definition 2.3.5. The Selmer group $S^{(m)}(E|K)$ is the following kernel,

$$\ker\Big(H^1(G_K, E[m]) \longrightarrow \prod_v H^1(G_v, E(\overline{K}_v))\Big),$$

by the previous commutative diagram, it contains Im δ_E, and it corresponds to the cocycles $\gamma \in H^1(G_K, E[m])$ such that for each $v \in M_K$, $r(\gamma) \in$ Im δ_v. By the previous interpretation of the $H^1(G_v, E(\overline{K_v}))$, the elements $\gamma \in H^1(G_K, E[m])$ get mapped to an homogeneous space, defined by some equations, and the Selmer group $S^{(m)}(E|K)$ corresponds to the γ such that the equations have a solution over all completions of K.

Definition 2.3.6. The Tate-Shafarevich group $Ш(E|K)$ is the kernel following kernel,

$$\ker\Big(H^1(G_K, E(\overline{K})) \longrightarrow \prod_v H^1(G_v, E(\overline{K}_v))\Big).$$

Note that $Ш(E|K)[m] = \ker\beta$. It corresponds to homogeneous spaces over K that have K_v-rational points for all $v \in M_K$. If $Ш(E|K) = 0$ all homogeneous spaces in $H^1(G_K, E(\overline{K}))$ that are locally trivial are trivial over K, so it measures failure of the Hasse principle.

Proposition 2.3.7. The groups $S^{(m)}(E|K)$ and $Ш(E|K)$ lie on an exact sequence,

$$0 \longrightarrow \frac{E(K)}{mE(K)} \longrightarrow S^{(m)}(E|K) \longrightarrow Ш(E|K)[m] \longrightarrow 0, \tag{2.9}$$

and $S^{(m)}$ is finite.

Proof. The exact sequence comes from the application of the kernel-cokernel sequence to

$$H^1(G_K, E[m]) \longrightarrow H^1(G_K, E)[m] \longrightarrow \prod_v H^1(G_v, E)[m].$$

The finitude of $S^{(m)}$ us shown through a procedure similar to the proof of the weak Mordell-Weil and can be found in [Sil09]X.4.2. ■

Remark 2.3.8. The finitude of the m-th Selmer group $S^{(m)}(E|K)$ implies the weak Mordell-Weil theorem. This can be interpreted as the order of Selmer group being an upper bound for $E(K)/mE(K)$ with the order of $Ш(E|K)[m]$ as error term. Computing the image of $E(K)/mE(K)$ in $S^{(m)}(E|K)$ is not a trivial process, the same goes for computing $Ш(E|K)$.

2.4 Explicit constructions

In this section we introduce an explicit construction that uses the b-pairing to compute explicitly the group $E(\mathbb{Q})/2E(\mathbb{Q})$.

Complete 2-descent

The b pairing introduced in proposition 2.2.10 and its properties can be used to compute the group $E(K)/mE(K)$ explicitly. Since we are interested in the case of congruent number curves, we drop generality. We will be content by considering the case $m = 2$ and $K = \mathbb{Q}$, since the curves only have 2-torsion over $\mathbb{Q}$. We note, however, that this can be generalized to number fields and any $m \geq 2$.

Let $E|\mathbb{Q}$ be a curve such that $E[2] \subseteq E(\mathbb{Q})$ (as is our case of particular interest). Let $\mathbb{Q}(S,2)$ be as defined in proposition 2.2.10. By 2.2.10.2 we have that the image of the b pairing is contained in $\mathbb{Q}(S,2)$, which is finite by theorem 2.2.11. To compute $E(\mathbb{Q})/2E(\mathbb{Q})$ we aim to compute the preimage of b.

Suppose $E : y^2 = (x-e_1)(x-e_2)(x-e_3)$, and suppose further $e_1 < e_2 < e_3$. Let $T_i = (e_i, 0)$ be the 2-torsion points of E over $\mathbb{Q}$. We can take T_1, T_2 as basis of $E[2]$ as $\mathbb{Z}/2\mathbb{Z}$-module. With this basis we can define a group morphism

$$\begin{aligned} \varphi : E(\mathbb{Q})/2E(\mathbb{Q}) &\longrightarrow \mathbb{Q}(S,2) \times \mathbb{Q}(S,2) \\ P &\longmapsto (b(P,T_1), b(P,T_2)), \end{aligned}$$

by the non-degeneracy of b, this morphism is injective, and by finding an explicit expression for it, given a pair $(b_1, b_2) \in (\mathbb{Q}(S,2))^2$ we can try to invert and see if it is the image of a point in $E(\mathbb{Q})/2E(\mathbb{Q})$.

Remark 2.4.1. This already gives us a rather coarse bound on the rank of E. We have that $\mathbb{Q}(S,2)$ can be represented by the classes of $\pm p$ for $p \in S$ and ± 1. Therefore $|\mathbb{Q}(S,2)| = 2^{l+2}$, where l is the number of primes dividing Δ. Since $|E(\mathbb{Q})/2E(\mathbb{Q})| = 2^{r+2}$ and it injects into $(\mathbb{Q}(S,2))^2$ we have that $r \leq 2l$.

Now, it can be shown (using the duplication formula) that $f_{T_i}(x,y) = x - e_i$ satisfies the properties in proposition 2.2.10.3, so if $P = (x,y) \neq T_1, T_2$, then $b(P,T_i) \equiv x - e_i \pmod{\mathbb{Q}^{\times 2}}$. Moreover, using the linearity of b we can explicitly determine φ:

$$\varphi(P) = \begin{cases} (x-e_1, x-e_2)\mathbb{Q}^{\times 2} & \text{if } P \neq T_1, T_2, \\ \left(\frac{e_1-e_3}{e_1-e_2}, e_1-e_2\right)\mathbb{Q}^{\times 2} & \text{if } P = T_1 \\ \left(e_2-e_1, \frac{e_2-e_3}{e_2-e_1}\right)\mathbb{Q}^{\times 2} & \text{if } P = T_2 \\ (1,1) & \text{if } P = O. \end{cases} \tag{2.10}$$

Given a pair $(b_1, b_2) \in (\mathbb{Q}(S,2))^2$, to see if it is the image of a point $P = (x,y) \neq O, T_1, T_2$ amounts to simultaneously solving in $\mathbb{Q}$ the equation for E, $b_1 z_1^2 = x - e_1$ and $b_2 z_2^2 = x - e_2$. Introducing a third variable z_3 and manipulating a bit, we can rewrite this as finding non-trivial rational solutions to:

$$\begin{cases} b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1 \\ b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 - e_1. \end{cases} \tag{2.11}$$

The corresponding rational point is then $(b_1 z_1^2 + e_1, b_1 b_2 z_1 z_2 z_3)$.

Remark 2.4.2. The systems of equations in 2.11 correspond to homogeneous spaces for E. In order to show that one of these does not have rational points, we can show that it does not have a point over some particular completion of

$\mathbb{Q}$. However it might happen that there is a solution over all completions of $\mathbb{Q}$, these pairs correspond to elements in the Tate-Shafarevich group of E. If $Ш(E|K) \neq 0$ then some of the pairs that have solutions over all completions do not have solutions over $\mathbb{Q}$.

The following proposition studies some of the first consequences of this construction.

Proposition 2.4.3. For each prime p and point $P \in E(\mathbb{Q})/2E(\mathbb{Q})$, define $\varphi_p(P) = v_p(\varphi(P)) \pmod 2 \in \mathbb{F}_2^2$ (the valuation and modulo are applied component-wise). Define also $\varphi_\infty(P) = \operatorname{sgn}(\varphi(P)) \in \{\pm\}^2$. Then,

1. For any P, $\varphi_p(P) = 0$ if $p \not|\Delta$,
2. If the reduction at p is nodal, then $\varphi_p(P)$ is either $(0,0)$ or $(1,1)$.
3. With the ordering $e_1 < e_2 < e_3$, $\varphi_\infty(P)$ is either $(+,+)$ or $(+,-)$.
4. The rank is bounded by $r \leq s_1 + 2s_2 - 1$, where s_1 is the number of primes where the reduction is nodal and s_2 the number of primes where the reduction is cuspidal.

Proof. (1) follows from the fact that the image of b is contained in the $\mathbb{Q}(S,2)$ which is represented by integers having only elements in S as factors.

(2) Suppose without loss of generality that $e_1 \equiv e_2 \pmod p$, let $P = (x,y) \in E(\mathbb{Q})$ be a point and let $a_i = v_p(x-e_i)$. Since $(x-e_1)(x-e_2)(x-e_3)$ is a square mod p, $a_1 + a_2 + a_3 \equiv 0 \pmod 2$. If $a_1 = 0$ then $a_2 = 0$ and $\varphi_p(P) = (0,0)$. If $a_1 > 0$ then p^{a_1} is a factor of the numerator of $x - e_1$. Since $p \not| e_1 - e_3$, then $p \not| x - e_3 = x - e_1 + e_1 - e_3$, so $a_3 = 0$. Therefore $a_1 + a_2 \equiv 0 \pmod 2$ and $\varphi_p(P)$ is in the diagonal of $\mathbb{F}_2^2$. If $a_1 < 0$, p^{a_1} is a factor of the denominator of x, so $a = b = c$ and since $a + b + c \equiv 0 \pmod 2$, $a \equiv b \equiv c \equiv 0 \pmod 2$, so $\varphi_p(P) = (0,0)$.

(3) Due to the ordering, we have that $e_3 - e_1, e_2 - e_1 > 0$. This means that pairs (b_1, b_2) of the form $(-,-)$ and $(-,+)$ cannot be in the image of φ since the corresponding equations (2.11) don't have solutions over $\mathbb{R}$.

(4) The considerations in (2) and (3) allow to reduce the space of possible images of φ and refine the bound in remark 2.4.1. ■

Remark 2.4.4. For the curve $y^2 = x^3 - d^2x$, let l be the number of prime factors of d. Then $r \leq 2l$ if d is odd, and $r \leq 2l + 1$ if d is even.

Corollary 2.4.5. The curve $y^2 = x^3 - x$ has rank 0 and 1 is not a congruent number.

Proof. No prime divides 1, so $l = 0$ and $r = 0$. ■

2.5 Examples

We will use the theory of 2-descent developed in the previous sections to show that 1 is not a congruent number and that 5 is a congruent number. We use the characterization in terms of elliptic curves given in theorem 1.0.4.

Therefore we aim to compute the rank of the congruent number curves to show whether a given d is or is not a congruent number.

Bound on the rank for $d = p$ prime

Before starting with explicit computations, the following lemmas give a bound on the rank of the elliptic curve associated to the congruence of prime numbers.

Lemma 2.5.1. The curve $y^2 = x^3 - 4x$ has rank 0 and therefore 2 is not a congruent number.

Proof. The only prime that divides the discriminant is 2, and we have that the reduction is cuspidal. By remark 2.4.4, $r \leq 3$. The set S will be $S = \{2, \infty\}$. We can take $\{\pm1, \pm2\}$ as representatives of $\mathbb{Q}(S, 2)$. The torsion points $(-2, 0)$, $(0, 0)$ and $(2, 0)$ are sent to $(2, -2)$, $(2, 1)$ and $(1, 2)$ in $\mathbb{Q}(S, 2)^2$ through φ.

- Suppose P is a point of infinite order, then $P + Q$ has also infinite order when Q is a torsion point. The components of $\varphi(P)$ can have four combinations of parity. If $\varphi(P) = (\pm1, \pm1)$, then $\varphi_2(P) = 0$. In the other three cases, we can replace P by $P + Q$ to obtain a point of infinite order such that $\varphi_2(P) = 0$. In this case we have $\varphi(P) = (\pm1, \pm1)$.
- Now, by proposition 2.4.3, we have that $\varphi_\infty(P)$ is either $(+, +)$ or $(+, -)$. In the case $(+, -)$ we reach the system of equations $a^2 + b^2 = 2$, $a^2 + c^2 = 4$. It is easy to see that a, b, c expressed as a quotient to the lowest terms must have the same denominator d, so by introducing a factor d we get the system $a^2 + b^2 = 2d^2$, $a^2 + c^2 = 4d^2$ for $a, b, c, d \in \mathbb{Z}$. Reducing modulo 2 we get that a, b, c have the same parity, and they cannot be even, otherwise d would be even and it would contradict that the expression was given in lowest terms. Reducing the second equation modulo 4 we get then $2 \equiv 0 \pmod 4$, a contradiction, so the system has no rational solutions.

  Therefore $\varphi_\infty(P) = (+, +)$ and $\varphi(P) = (1, 1)$. The morphism φ is injective, so $P = O$. We get a contradiction and P cannot have infinite order.

Therefore the curve has rank 0 and 2 is not a congruent number. ■

Lemma 2.5.2. Consider the curve $y^2 = x^3 - p^2x$, let r be its rank. Then,

$$\begin{aligned} &r \leq 2 \text{ if } p \equiv 1 \pmod 8 \\ &r = 0 \text{ if } p \equiv 3 \pmod 8 \\ &r \leq 1 \text{ otherwise.} \end{aligned}$$

In particular, the primes $p \equiv 3 \pmod 8$ are not congruent numbers.

Proof. In this case the primes that divide the discriminant are 2 and p, so $S = \{2, p, \infty\}$, with cuspidal reduction at p and nodal reduction at 2. By remark 2.4.4 we get that $r \leq 2$. We represent $\mathbb{Q}(S, 2) = \{\pm 1, \pm 2, \pm p, \pm 2p\}$ and the torsion points $(-p, 0)$, $(0, 0)$ and $(p, 0)$ are sent to $(2, -p)$, $(p, 1)$ and $(2p, p)$ in $\mathbb{Q}(S, 2)^2$ respectively. We use now proposition 2.4.3 to refine the bound on the rank, and reduce the search space.

- Suppose P is a point of infinite order, as in the previous lemma, we can replace P with $P + Q$, where Q is a torsion point, so that we obtain a point of infinite order with $\varphi_p(P) = 0$. Therefore we study only pairs in $\mathbb{Q}(S, 2)^2$ not involving p.
- We have that $\varphi_\infty(P)$ has to be $(+, +)$ or $(+, -)$, so we discard all the pairs with $(-, +)$ and $(-, -)$.
- Nodal reduction gives $\varphi_2(P)$ is diagonal, we may further discard pairs with different parity. The remaining pairs are $(1, 1)$, $(1, -1)$, $(2, 2)$ and $(2, -2)$.

The first pair corresponds to O. This reduction of the search space is equivalent to having the bound $r \leq 2$. We study each pair now.

- If $\varphi(P) = (1, -1)$ then there are $a, b \in \mathbb{Q}$ such that $x + p = a^2$ and $x = -b^2$. Then $a^2 + b^2 = p$, multiplying p by a factor c^2, $c \in \mathbb{Z}$, we may assume $a, b \in \mathbb{Z}$. Then we get that pc^2 is a sum of squares, if $p \equiv 3 \pmod 4$, this cannot happen. This reduces the bound by 1 in the cases $p \equiv 3, 7 \pmod 8$.
- If $\varphi(P) = (2, 2)$. Then $x + p = 2a^2$ and $x = 2b^2$ for $a, b \in Q$. Substituting into the equation of E we obtain $y^2 = 8a^2b^2(a^2 - p)$, multiplying c^2, for a $c \in \mathbb{Z}$, on both sides we can assume $a, b \in \mathbb{Z}$. Then reducing $\bmod p$ we see that for the equation to have a solution, 2 must be a square $\bmod p$. By the supplement to quadratic reciprocity, 2 is a quadratic residue $\bmod p$

when $p \equiv \pm 1 \pmod 8$. This reduces the rank by 1 in the case $p \equiv 5 \pmod 8$ and reduces the rank to 0 in the case $p \equiv 3 \pmod 8$.

These considerations prove the proposition and the fact that $r = 0$ when $p \equiv 3 \pmod 8$ shows that in that case p is not a congruent number. ■

Example of complete 2-descent: Congruent number

We study the curve $E : y^2 = x^3 - 25x$. The equation factors as $y^2 = x(x-5)(x+5)$, so it has all its 2-torsion defined over $\mathbb{Q}$ and $E(\mathbb{Q})_{\text{tors}} = E[2] = \{O, (-5,0), (0,0), (5,0)\} \simeq (\mathbb{Z}/2\mathbb{Z})^2$. By lemma 2.5.2 we know that $r \leq 1$, we will use the method of 2-descent to find a point of infinite order and thus show the rank is exactly 1.

The discriminant of E is $\Delta = -2^6 \cdot 5^6$, so in this case $S = \{2, 5, \infty\}$, and $\mathbb{Q}(S,2)$ has representatives $\{\pm 1, \pm 2, \pm 5 \pm 10\}$. For each pair of the 64 pairs $(b_1, b_2) \in \mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$ we have to check now for solutions $z_1, z_2, z_3 \in \mathbb{Q}$ of the following systems,

$$\begin{cases} b_1 z_1^2 - b_2 z_2^2 = 5, \\ b_1 z_1^2 - b_1 b_2 z_3^2 = 10. \end{cases}$$

1. We map the 2-torsion points using the group morphism φ given in (2.10). We get the following,

   $$O \longmapsto (1,1), \quad (-5,0) \longmapsto (2,-5) \quad (0,0) \longmapsto (5,1), \quad (5,0) \longmapsto (10,5).$$

2. Since 5 is prime in the class of 5 (mod 8) by 2.5.2, we can reduce the search to the pair $(1,-1)$. We have the system of equations

   $$\begin{cases} z_1^2 + z_2^2 = 5, \\ z_1^2 + z_3^2 = 10. \end{cases}$$

   By inspection we see that the system has an integral solution $(1,2,3)$. We can use this to find the point $P = (-4,-6)$, which is easily checked to be a point in E.

By the lemma 2.5.2 and the previous computation we conclude that the rank of E is 1 and $E(\mathbb{Q})$ is generated by the 2-torsion points and P. If p is a prime number $p \equiv 5 \pmod 8$ the rank is always 1 and p is a congruent number. We will prove this in proposition 4.5.1 in chapter 4.

CHAPTER 3

Complex multiplication, modular functions, and Heegner points

The goal of this chapter is to introduce the concept of Heegner points. This is used to find rational points on an elliptic curve and is the main idea of the *Mock Heegner points and congruent numbers* paper that we analyze in chapter 4. Firstly, we will discuss some concepts and results in the theory of complex multiplication. After that, we will introduce the modular curves and modular functions. Finally, we will combine these sections to introduce Heegner points as an application of this theory.

3.1 Complex multiplication

This section gives an overview of the theory of elliptic curves with complex multiplication, that is, curves that have more endomorphisms than just $\mathbb{Z}$. The theory of complex multiplication explicitly develops the class field theory of imaginary quadratic fields. The class field theory of $\mathbb{Q}$ concerns the description of all abelian extensions of $\mathbb{Q}$, and by the Kronecker-Weber theorem, these are all subfields of cyclotomic extensions. This means that any field extension $K|\mathbb{Q}$ is generated by sums of roots of unity. In this case, the algebraic number theory is well understood. General class field theory studies abelian extension of number fields, but the main theorems do not give explicit constructions as in the rational case. However, in the case of imaginary quadratic number fields $K = \mathbb{Q}(\sqrt{D})$, with $D < 0$, such an explicit construction is possible using the torsion points and j-invariant of an elliptic curve with complex multiplication by $\mathcal{O}_K$.

Definition 3.1.1. Let $E|\mathbb{C}$ be an elliptic curve. In the case of complex elliptic curves, the endomorphism ring $\mathrm{End}(E)$ is always abelian, and it is either $\mathbb{Z}$ or an order R in an imaginary quadratic field K. In the second case, we say that E has *complex multiplication by R*.

Remark 3.1.2. We remind that an order R in a number field K is a subring of K such that $K = R \otimes \mathbb{Q}$. The ring of integers $\mathcal{O}_K$ is an order in K. Let $K = \mathbb{Q}(\tau)$ be an imaginary quadratic extension where τ is such that $\mathcal{O}_K = \mathbb{Z}[\tau]$. The possible orders of K are then $R = \mathbb{Z} \oplus \mathbb{Z}c\omega$, for a $c \geq 1$ called the *conductor of* R. Note that $\mathcal{O}_K$ is the maximal order in K.

Remark 3.1.3. For a curve $E|\mathbb{C}$ with complex multiplication, there are two possible ways to identify $\operatorname{End}(E)$ with R inside $\mathbb{C}$. There is a canonical way to pick one of these embeddings; if ω is an invariant differential, and $f : R \longrightarrow \operatorname{End}(E)$ is an embedding, we pick the embedding such that $f(\alpha)^*\omega = \alpha\omega$ for all $\alpha \in R$.

Example 3.1.4. The congruent number elliptic curves, $E : y^2 = x^3 - n^2x$, defined over $\mathbb{C}$, have j-invariant $j(E) = 1728$. The automorphism group of elliptic curves with j-invariant 1728 has order 4 ([Sil09]III.10). If $\operatorname{End}(E) = \mathbb{Z}$, then the only possible automorphisms are $\{\pm 1\}$, therefore $\operatorname{End}(E)$ has to be strictly bigger than $\mathbb{Z}$ and E has complex multiplication.

Let $E|\mathbb{C}$, by the Weierstrass' uniformization theorem, we know that any complex elliptic curve is isomorphic to $\mathbb{C}/\Lambda$, for a lattice $\Lambda \subseteq \mathbb{C}$. Moreover, two complex elliptic curves E_1, E_2 are isomorphic if and only if the corresponding Λ_1, Λ_2 are homothetic. This gives the following correspondence,

$$\{\text{Elliptic curves over } \mathbb{C} \text{ up to isomorphism}\}$$
$$\updownarrow$$
$$\{\text{Lattices } \Lambda \subseteq \mathbb{C} \text{ up to homothety}\}.$$

If $E|\mathbb{C}$ is the elliptic curve corresponding to the lattice Λ, an endomorphism of E is given by an $\alpha \in \mathbb{C}$ such that $\alpha\Lambda \subseteq \Lambda$. With this presentation, it is clear that $\mathbb{Z} \subseteq \operatorname{End}(E)$, but if E has complex multiplication by R, then there's a non-integral α such that $\alpha\Lambda \subseteq \Lambda$. For the sake of simplicity, we will restrict ourselves to the case where $R = \mathcal{O}_K$ for the rest of the chapter.

Given an elliptic curve with complex multiplication, we can obtain an imaginary quadratic field, $\operatorname{End}(E) \otimes \mathbb{Q}$. How can we get an elliptic curve with complex multiplication by $\mathcal{O}_K$ given an imaginary quadratic field K? Let $\mathfrak{a} \subseteq K$ be a fractional ideal, that is, a finitely generated $\mathcal{O}_K$-submodule of K. Fractional ideals can be seen as lattices in $\mathbb{C}$, therefore we can define the corresponding elliptic curve $E_{\mathfrak{a}}$, and it is easy to check that $\operatorname{End}(E_{\mathfrak{a}}) = \mathcal{O}_K$. Moreover, since homothetic lattices give isomorphic elliptic curves, we have that fractional ideals that lie in the same ideal class give rise to an isomorphic curve. We have thus a map

$$\begin{aligned}\mathrm{Cl}(\mathcal{O}_K) &\longrightarrow \mathcal{ELL}(\mathcal{O}_K)\\ \overline{\mathfrak{a}} &\longmapsto E_{\mathfrak{a}},\end{aligned}$$

where $\mathcal{ELL}(\mathcal{O}_K)$ is the set of isomorphism classes of complex elliptic curves with complex multiplication by $\mathcal{O}_K$. This allows us to define an action of $\mathrm{Cl}(K)$ into $\mathcal{ELL}(\mathcal{O}_K)$.

Proposition 3.1.5. Let Λ be a lattice such that $E_\Lambda \in \mathcal{ELL}(\mathcal{O}_K)$, let $\mathfrak{a}$ be a non-zero fractional ideal of K, we can define $\mathfrak{a}\Lambda$ to be the product of $\mathfrak{a}$ and Λ as $\mathbb{Z}$-submodules of $\mathbb{C}$. We have then

1. $\mathfrak{a}\Lambda$ is a lattice in $\mathbb{C}$.
2. The curve $E_{\mathfrak{a}\Lambda}$ has complex multiplication by $\mathcal{O}_K$.
3. Let $\mathfrak{b}$ be another non-zero fractional ideal, then $E_{\mathfrak{a}\Lambda} \simeq E_{\mathfrak{b}\Lambda}$ if and only if $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$ in $\mathrm{Cl}(K)$.
4. $\mathrm{Cl}(K)$ acts on $E_\Lambda \in \mathcal{ELL}(\mathcal{O}_K)$ by $\overline{\mathfrak{a}} * E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}$ simply transitively, so $|\mathcal{ELL}(\mathcal{O}_K)| = |\mathrm{Cl}(K)|$.

Proof. [Sil94]II.1.2. ■

Remark 3.1.6. An interesting thing to note is that for the case of elliptic curves with complex multiplication, we can also consider $\mathfrak{a}$-torsion and the $\mathfrak{a}$ isogeny, for a fractional ideal $\mathfrak{a} \subseteq K$. We have $E[\mathfrak{a}] = \{P \in E \mid [a]P = 0\ \forall a \in \mathfrak{a}\}$ and the isogeny $[\mathfrak{a}] : E_\Lambda \longrightarrow \mathfrak{a} * E_\Lambda$. It is easy to see that $\ker[\mathfrak{a}] = E[\mathfrak{a}]$ and $E[\mathfrak{a}]$ is a rank 1 $\mathcal{O}_K/\mathfrak{a}$-module. This is a generalization of the case of integral torsion.

Up to this point, we have seen that elliptic curves with complex multiplication have a close relationship with the arithmetic of the associated imaginary quadratic field K. We see now that the j-invariant such an elliptic curve is an algebraic number, and therefore it will generate a finite field extension of K.

Proposition 3.1.7. Let $E|\mathbb{C}$ be an elliptic curve.

1. If $\sigma : \mathbb{C} \longrightarrow \mathbb{C}$ be a field automorphism. Then $\mathrm{End}(\sigma(E)) = \mathrm{End}(E)$.
2. If E has complex multiplication by $\mathcal{O}_K$, for a imaginary quadratic field K, then $j(E)$ is algebraic.

Proof. [Sil94]II.2.1. ■

The fact that j is algebraic is somewhat surprising, taking into account that E is defined over $\mathbb{C}$, and j could be any complex number. This implies that curves with complex multiplication can be defined over a number field. Moreover, the specific field extension $K(j(E)|K$ turns out to be the Hilbert class field of K. That is, the maximal abelian extension of K which is unramified at all primes of K. Through class field theory and the Artin reciprocity law, the Galois group $\mathrm{Gal}(K(j(E))|K)$ is isomorphic to the class group $\mathrm{Cl}(K)$. The next proposition, which could be called the main theorem of complex multiplication, states that the action of $\mathrm{Gal}(K(j(E))|K)$ on the $j(E_{\mathfrak{a}_i})$ is compatible with the action of $\mathrm{Cl}(K)$ on the $E_{\mathfrak{a}_i}$ described in proposition 3.1.5 through the isomorphism given by Artin reciprocity.

Theorem 3.1.8. Let $E|\mathbb{C}$ be an elliptic curve with complex multiplication by $\mathcal{O}_K$, for K some imaginary quadratic field. The field $H = K(j(E))$ is the Hilbert class field of K. Moreover, if $E_{\mathfrak{a}_1}, \dots, E_{\mathfrak{a}_{h_K}}$ are representatives of $\mathcal{ELL}(\mathcal{O}_K)$ for each ideal class in $\mathrm{Cl}(K)$, then the action of the Artin automorphism on the $j(E_{\mathfrak{a}_i})$ is the following:

$$\sigma_{\mathfrak{a}_i}(j(E_{\mathfrak{a}_j})) = j(\mathfrak{a}_i * E_{\mathfrak{a}_j}) = j(E_{\mathfrak{a}_i^{-1}\mathfrak{a}_j}).$$

Proof. [Sil94]II.4.3 ■

3.2 Modular functions

We explain now the main concepts in the theory of modular functions and modular curves. To begin with, we introduce the modular curve $X(1)$, which is the moduli space of complex elliptic curves. Next, we talk about the curves $X(N)$ and $X_0(N)$, which also represent equivalence classes of complex elliptic curves, but with some additional structure. These curves are defined by taking the quotient of the upper half plane $\mathbb{H}$ by specific subgroups Γ of $\mathrm{PSL}(2, \mathbb{Z})$, and then compactifying the result. Finally, we introduce modular functions and modular forms, which are meromorphic functions on $\mathbb{H}$ that satisfy certain compatibility conditions with the action of Γ. Additionally, we state the modularity theorem, which enables us to use modular functions to parameterize any elliptic curve over $\mathbb{Q}$.

The curve $X(1)$

As mentioned above, elliptic curves over $\mathbb{C}$ up to isomorphism are in bijective correspondence with lattices in $\mathbb{C}$ up to homothety. In this section, we study elliptic curves from the perspective of the later space. We denote $\mathcal{L}$ the space of lattices and $\mathcal{L}/\mathbb{C}^*$ the space of lattices up to homothety.

A lattice Λ is given by two periods ω_1, ω_2 not both in $\mathbb{R}$, we further assume that they are ordered such that $\frac{\omega_1}{\omega_2} \in \mathbb{H}$. We would like to find a good representative of the class of lattices, and we can obtain a homothetic lattice by dividing by ω_2 The lattice is then represented by $1, \tau$ with $\tau \in \mathbb{H}$. We have a surjective map

$$\mathbb{H} \longrightarrow \mathcal{L}/\mathbb{C}^*.$$

This map is however not injective. For this, we have to see which $\tau, \tau' \in \mathbb{H}$ give rise to the same lattice.

Definition 3.2.1. We define the *modular group* $\Gamma(1) = \mathrm{SL}(2, \mathbb{Z})/\{\pm 1\} = \mathrm{PSL}(2, \mathbb{Z})$. Given $\tau \in \mathbb{H}$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$, we define the action of $\Gamma(1)$ on $\mathbb{H}$ by $\gamma\tau = \frac{a\tau+b}{c\tau+d}$.

Lemma 3.2.2. Let $\tau, \tau' \in \mathbb{H}$ and Λ, Λ' be the corresponding lattices. Then Λ and Λ' are homothetic if and only if there is a $\gamma \in \Gamma(1)$ such that $\gamma\tau = \tau'$.

Proof. [Sil94]I.1.2. ■

In virtue of this lemma, we can finally give a bijective correspondence. There is a one-to-one correspondence between $\mathcal{L}/\mathbb{C}^*$ and the quotient of $\mathbb{H}$ by $\Gamma(1)$. We denote this quotient by $\Gamma(1)\backslash\mathbb{H}$ or $Y(1)$. The following propositions will describe this space, give it a topological structure, and a complex structure.

Proposition 3.2.3. Let $\mathcal{F} = \{\tau \in \mathbb{H} \mid |\tau| \geq 1\ ,\ |\operatorname{Re}(\tau)| \leq \frac{1}{2}\}$. Let $\tau \in \mathbb{H}$.

1. There is $\gamma \in \Gamma(1)$ such that $\gamma\tau \in \mathcal{F}$,
2. If $\tau, \gamma\tau \in \mathcal{F}$ for some $\gamma \in \Gamma(1)$, then

$$\begin{cases} \operatorname{Re}(\tau) = -\frac{1}{2} \text{ and } \gamma\tau = \tau + 1, \\ \operatorname{Re}(\tau) = \frac{1}{2} \text{ and } \gamma\tau = \tau - 1, \text{ or} \\ |\tau| = 1 \text{ and } \gamma\tau = \frac{-1}{\tau}. \end{cases}$$

Proof. [Sil94]I.1.5. ■

This proposition describes a fundamental domain for the action of $\Gamma(1)$ on $\mathbb{H}$. The quotient space by this action looks like a punctured sphere, which is not compact. To obtain a compact space we consider an extension of $\mathbb{H}$.

Definition 3.2.4. We define the *extended upper half plane* $\mathbb{H}^*$ to be $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$. We call these added points, *cusps.* The action of $\Gamma(1)$ extends to the rational projective line as follows, for a point $(x:y) \in \mathbb{P}^1(\mathbb{Q})$, and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$, we define

$$\gamma(x:y) = (ax + by : cx + dy).$$

We define $X(1) = \Gamma(1)\backslash\mathbb{H}^*$.

Remark 3.2.5. Any point in $\mathbb{P}^1(\mathbb{Q})$ can be represented as $(x:y)$, with $x, y \in \mathbb{Z}$ and $\gcd(x,y) = 1$. There are then $a, b \in \mathbb{Z}$ such that $ax + by = 1$, and the transformation $\begin{pmatrix} a & b \\ -y & x \end{pmatrix} \in \Gamma(1)$ sends $(x:y)$ to $(1:0)$. This means that all points in $\mathbb{P}^1$ are in the same orbit of the action of $\Gamma(1)$ and that $\Gamma\backslash\mathbb{H}^*$ only adds one point to $\Gamma(1)\backslash\mathbb{H}$, that is, $X(1)$ has only one cusp.

The extended upper half plane can be given a topology with a basis of open neighborhoods:

- For $\tau \in \mathbb{H}$, the basis is the usual basis.
- For $\tau_0 = \infty$, we take as basis the sets $\{\tau \in \mathbb{H} \mid \operatorname{Im}(\tau) > k\} \cup \{\infty\}$ for $k > 0$.
- For any other cusp τ_0, represented by a rational number, we take as a basis the interior of the circles in $\mathbb{H}$ that are tangent to τ_0 on the real axis.

This is a Hausdorff topology on $\mathbb{H}^*$, and $X(1)$ becomes a compact Hausdorff topological space through the quotient map. As mentioned before, $Y(1)$ is a punctured 2-sphere, and with the added cusp, $X(1)$ becomes the whole sphere. Moreover, $X(1)$ can be given a complex structure by which it becomes a Riemann surface of genus 0, that is, the Riemann sphere.

Given a finite $\tau \in X(1)$, we can compute the j-invariant of the associated elliptic curve $\mathbb{C}/\Lambda_\tau$. This extends to a bijective map of sets

$$\begin{aligned} j : X(1) &\longrightarrow \mathbb{P}^1(\mathbb{C}) \\ \tau &\longmapsto j(\mathbb{C}/\Lambda_\tau), \end{aligned}$$

which can be shown to actually be a complex isomorphism. With this, we have completely described the moduli space for complex elliptic curves, a space that parametrizes all possible elliptic curves over $\mathbb{C}$ up to isomorphism. For every isomorphism class of complex elliptic curves we get a unique point in $X(1)$, and for every non-cuspidal point in $X(1)$ we get a unique isomorphism class of complex elliptic curves.

Remark 3.2.6. The details of this construction are technical and complicated, and therefore omitted from this chapter. They can be found in [Sil94]I.2.2-6.

Congruence subgroups and the curves $X(N)$ and $X_0(N)$

In the previous section we have described the quotient of $\mathbb{H}$ by the modular group $\Gamma(1)$, which was $\mathrm{PSl}(\mathbb{Z}, 2)$. Given a subgroup Γ of $\Gamma(1)$, we can restrict the action on $\mathbb{H}$ to Γ, and consider the quotient. These quotients become also complex curves, although more complicated that, $\mathbb{P}^1(\mathbb{C})$. Moreover, for some specific subgroups of $\Gamma(1)$, the resulting curves parameterize objects of number theoretical interest. We introduce the Γ_0 and Γ.

Definition 3.2.7. Let $N \geq 1$ be an integer, we define the subgroup $\Gamma_0(N)$ by

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \pmod{N} \right\},$$

and the subgroup $\Gamma(N)$ by

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

We define the curves $Y_0(N) = \mathbb{H}\backslash\Gamma_0(N)$ and $Y(N) = \mathbb{H}\backslash\Gamma(N)$ and their compactifications $X_0(N) = \mathbb{H}^*\backslash\Gamma_0(N)$ and $X(N) = \mathbb{H}^*\backslash\Gamma(N)$. These curves are called *modular curves of level* N. Note that for $N = 1$ we have that $\Gamma_0(1) = \Gamma(1)$ and therefore $X_0(1) = X(1)$.

Remark 3.2.8. We saw in remark 3.2.5 that all points in $\mathbb{P}^1(\mathbb{Q})$ are equivalent under the action of $\Gamma(1)$. This does not happen when restricting the action to the $\Gamma_0(N)$ or $\Gamma(N)$ when $N > 1$, so, therefore, the curves $X_0(N)$ and $X(N)$ have more than one cusp. For example, $X(2)$ has three cusps that can be represented by $(0:1)$, $(1:1)$ and $(1:0)$ ([DS05]2.4).

Remark 3.2.9. In the same way that $X(1)$ parameterizes elliptic curves up to complex isomorphism, the $X_0(N)$ and $X(N)$ also parameterize families of elliptic curves, but in this case with added structure ([DS05]1.5). Namely,

- $Y_0(N)$ is in correspondence with pairs (E, C) where E is an elliptic curve and C is a cyclic subgroup of order N. In this case, the isomorphism relation for two pairs (E, C) and (E', N') is a complex isomorphism $\varphi : E \longrightarrow E'$ such that $\varphi(C) = C'$. It also can be interpreted as the set of isogenies $\varphi : E \longrightarrow E'$ with $E, E'|\mathbb{C}$ and $\ker\varphi$ cyclic of order N, up to isomorphism.

- $Y(N)$ is in correspondence with triples (E, P, Q), where E is an elliptic curve and P, Q are generators for $E[N]$ such that the Weil pairing is $e_N(P, Q) = e^{2\pi i/N}$. The isomorphism relation is the natural one.

Remark 3.2.10. It can be shown that the curves $X(N)$ and $X_0(N)$ actually have models as algebraic curves over $\mathbb{Q}$. In the particular case of $X_0(N)$, it can be seen ([Bir04]) that there is $f \in \mathbb{Q}[x, y]$ such that $f(j, j_N) = 0$, where j is the modular j-invariant defined in example 3.2.15, and j_N is $j(N\tau)$. This gives a singular model for $X_0(N)$ as a plane curve, but it implies that $X_0(N)$ can be parameterized by $(j(\tau), j_N(\tau))$ outside a finite number of singular points.

Modular functions and modular forms

In the previous section, we have introduced the curves $X(N)$ and $X_0(N)$ and we have stated that they have a compact Riemann surface structure. Modular functions and modular forms for a $\Gamma \subseteq \Gamma(1)$ are meromorphic functions defined on $\mathbb{H}$ with a controlled action of Γ. In some cases these are meromorphic functions on the modular curves but not always.

Definition 3.2.11. Let Γ be $\Gamma(N)$ or $\Gamma_0(N)$. A *weakly modular function of level N and weight k* is a function $f : \mathbb{H} \longrightarrow \mathbb{C}$ such that

1. f is meromorphic on $\mathbb{H}$, and
2. $f(\gamma z) = (cz + d)^k f(z)$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.

Both groups $\Gamma(N)$ and $\Gamma_0(N)$ contain the matrix $\gamma_N = \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}$ so if f is a weakly modular function of level N, then the second condition implies that $f(z) = f(\gamma_N z) = f(z+N)$, so f is N-periodic. This means that it can be Fourier transformed, that is, expressed as a function $\tilde{f}$ of $q = e^{\frac{2\pi i}{N}}$, this q is called *nome*. This transform is meromorphic on the punctured disk $\{q \in \mathbb{C} \mid 0 < |q| < 1\}$, and has Laurent expansion

$$\tilde{f}(q) = \sum_{n=-\infty}^{\infty} a_n q^n.$$

This transformation allows us to define a notion of meromorphy, or holomorphy at the cusps.

Definition 3.2.12. Let $f : \mathbb{H} \longrightarrow \mathbb{C}$ be a weakly modular function of weight k and level N for the group Γ, with Fourier transform $\tilde{f}(q)$.

1. We say that f is *meromorphic at the cusps of* $\Gamma \backslash \mathbb{H}^*$ if there is an $m_0 \geq 0$ such that $\tilde{f}(q) = \sum_{-m_0}^{\infty} a_n q^n$. In that case, we say f is a *modular function* of weight k for Γ.

2. We say that a modular function of weight k for Γ, f, is *holomorphic at the cusps of* $\Gamma\backslash\mathbb{H}^*$ if $\tilde{f}(q) = \sum_0^\infty a_n q^n$. In that case, we say that f is a *modular form* of weight k for Γ.

3. We say that a modular form of weight k for Γ *vanishes at the cusps of* $\mathbb{H}^*/\Gamma$ if $a_0 = 0$. In that case, we say it is a *cusp form.*

Remark 3.2.13. Note that modular functions of weight $k = 0$ for Γ correspond to meromorphic functions on the curve $\Gamma\backslash\mathbb{H}^*$. Moreover, these functions cannot be holomorphic because there are no non-constant globally defined holomorphic functions on a compact Riemann surface.

Remark 3.2.14. The set of modular functions for Γ of weight k form a vector space over $\mathbb{C}$, we denote it by $M_k(\Gamma)$. Moreover $\bigoplus_k M_k(\Gamma)$ has a graded $\mathbb{C}$-algebra structure. The set of cusp forms of weight k, denoted by $S_k(\Gamma)$ is also a vector space over $\mathbb{C}$ and a subspace of $M_k(\Gamma)$. These subspaces have geometric interpretation as differential forms on the corresponding $X(\Gamma)$, for example, $S_2(\Gamma_0(N))$ can be interpreted as the space of differential 1-forms on $X_0(N)$.

Example 3.2.15. Let

$$g_2(\tau) = 60 \sum_{(m,n)\neq(0,0)} \frac{1}{(m+n\tau)^4},$$
$$g_3(\tau) = 140 \sum_{(m,n)\neq(0,0)} \frac{1}{(m+n\tau)^6}.$$

These sums converge, for $\tau \in \mathbb{H}$, to meromorphic functions $\mathbb{H} \longrightarrow \mathbb{C}$. It can be shown that g_2 and g_3 are modular functions for $\Gamma(1)$ of weights 4 and 6 respectively. These functions are called the *Weierstrass invariants* since the Weierstrass equation of the elliptic curve $\mathbb{C}/\Lambda_\tau$, given by the Weierstrass uniformization $z \longmapsto (\wp_\tau(z), \wp'_\tau(z))$, is $y^2 = 4x^3 - g_2(\tau) - g_3(\tau)$. This motivates the definition of the *modular discriminant* $\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2$, which is a modular function for Γ of weight 12, and the *modular j-invariant*

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

which is a modular function of weight 0. This means that the j-invariant is a well-defined holomorphic function $Y(1) \longrightarrow \mathbb{C}$. As mentioned in section 3.2, this gives an analytic isomorphism $j : X(1) \longrightarrow \mathbb{P}^1(\mathbb{C})$ and means that the field of rational functions on $X(1)$ is $\mathbb{C}(j)$.

Modular parameterization

Finally, we state an important consequence of the famous modularity theorem. The proper statement of this theorem is very subtle and complicated and outside the scope of this document ([Dar03]).

Theorem 3.2.16 (Modularity theorem, [Bru+08]4.4)**.** Let E be an elliptic curve of conductor N. Given an algebraic model of $X_0(N)$, there is a rational map $\Phi_N : X_0(N) \longrightarrow E$ called the *modular parameterization.* There are modular functions $x(\tau), y(\tau)$ for $\Gamma_0(N)$ that parameterize E over $\mathbb{Q}$, this means that if $y^2 = f(x)$ is a Weierstrass equation for E, then $y(\tau)^2 = f(x(\tau))$ for $\tau \in \mathbb{H}$.

3.3 Heegner points

In this section, we will explore a stunning application of complex multiplication and modular parameterization. This is the main idea, albeit with some adaptations, used in the Monsky paper. Consider the singular algebraic model of the modular curve $X_0(N)$. Certain points (E, C_N) on this curve correspond to elliptic curves that have complex multiplication by the same ring for both E and E/C_N. These points turn out to be defined over the Hilbert Class field and can be transported to any elliptic curve of conductor N through the modular parametrization.

Definition 3.3.1. A point $\tau \in \mathbb{H}$ is a *complex multiplication point* if it is the root of a quadratic equation $A\tau^2 + B\tau + C = 0$ with $A, B, C \in \mathbb{Z}$ and $B^2 - AC < 0$. There is a unique such triple (A, B, C) with the condition that $A > 0$ and $\gcd(A, B, C) = 1$, we define the discriminant of τ to be $\Delta(\tau) = B^2 - 4AC$ for this representation. A complex multiplication point τ is called a *Heegner point of level N and discriminant* $D = \Delta(\tau)$ if $\Delta(\tau) = \Delta(N\tau)$ for some $N > 0$.

Proposition 3.3.2.

1. Let $\tau \in \mathbb{H}$ be a complex multiplication point and $\gamma \in \Gamma(1)$ of discriminant D. Then $\gamma\tau$ is also a complex multiplication point of discriminant D.
2. Let $\tau \in \mathbb{H}$ be a Heegner point of level N and discriminant D and $\gamma \in \Gamma_0(N)$, then $\gamma\tau$ is also a Heegner point of level N and discriminant D.

Proof. [Coh07]8.6.2. ■

Remark 3.3.3. This means that complex multiplication points are defined in $X(1)$, and that Heegner points of level N are defined in $X_0(N)$. Since, $X_0(N)$

covers $X(1)$, if there exist Heegner points of level N and discriminant D, they are lifts of the complex multiplication points of discriminant D on $X(1)$.

A *fundamental discriminant* D is an integer that appears as the discriminant of a primitive binary quadratic form. It can be shown that this is equivalent to either $D \equiv 1 \pmod 4$ and square-free, or $D \equiv 8$ or $12 \pmod{16}$. This also coincides with the D that appear as field discriminants of quadratic number fields. We take in this case

$$K = \begin{cases} \mathbb{Q}(\sqrt{D}) & \text{if } D \equiv 1 \pmod 4, \text{or}, \\ \mathbb{Q}\left(\sqrt{\frac{D}{4}}\right) & \text{if } D \equiv 8, 12 \pmod{16}. \end{cases} \tag{3.1}$$

Given a fundamental discriminant D, there is a bijective correspondence between $\mathrm{Cl}(\mathcal{O}_K)$ and the classes of primitive quadratic forms. From now on we assume that D is a fundamental discriminant. By this correspondence, fixed D, there are h_K different complex multiplication points of discriminant D. These give rise to different, and all, elliptic curves with complex multiplication by $\mathcal{O}_K$. The action of $\mathrm{Cl}(\mathcal{O}_K)$ was given in proposition 3.1.5. A similar situation happens in the case of Heegner points. If $\tau \in \mathbb{H}$ is a Heegner point of level N and discriminant D, the condition that $\Delta(\tau) = \Delta(N\tau)$ means that both $\mathbb{C}/\Lambda_\tau$ and $\mathbb{C}/\Lambda_{N\tau}$ have complex multiplication by the same $\mathcal{O}_K$.

Let $N > 1$ and D be a fundamental discriminant. We have talked about Heegner points of level N and discriminant D, but we have not shown that such points actually exist. Not all pairs N, D can give Heegner points, but fixed an N, we can always find infinitely many D such that the corresponding Heegner points exist.

Proposition 3.3.4. Let $\tau \in \mathbb{H}$ be a complex multiplication point of discriminant D represented by the quadratic form (A, B, C). Then τ is a Heegner point of level N if and only if $N|A$ and there is an $F \in \mathbb{Z}$ such that $B^2 - 4NF = D$ with $\gcd(N, B, F) = 1$.

Proof. [Coh07]8.6.3. ■

Remark 3.3.5. Fixed N, let τ be a root of an equation $NA\tau^2 + B\tau + C = 0$, for $A, B, C \in \mathbb{Z}$, $A > 0$ and $\gcd(A, B, C) = 1$. Then both τ and $N\tau$ have discriminant $D = B^2 - 4NAC$. We can therefore always find a D such that there are Heegner points of level N and discriminant D.

Lemma 3.3.6. Let $N > 0$ and let $D < 0$ be a fundamental discriminant, let K be the corresponding imaginary quadratic field. If there is an ideal $\mathfrak{n} \subseteq \mathcal{O}_K$ such that $\mathcal{O}_K/\mathfrak{n} = \mathbb{Z}/N\mathbb{Z}$, then there exist Heegner points of level N and discriminant D.

Proof. The ideal $\mathfrak{n}$ has absolute norm $\mathfrak{N}(\mathfrak{n}) = N$. This implies that there is a binary quadratic form of discriminant D representing N. If a quadratic form represents N, it is equivalent to the form $Nx^2 + Bxy + Cy^2$ for some $B, C \in \mathbb{Z}$ having discriminant D. Then $D = B^2 - 4NC$, by the previous remark, there are Heegner points of level N and discriminant D. The facts on binary quadratic forms can be found in [Cox22]7B. ■

The following proposition introduces a compatibility condition between N and D that implies the existence of such an ideal.

Proposition 3.3.7 (Heegner hypothesis)**.** Let $N > 0$, let $D < 0$ be a fundamental discriminant and K the corresponding imaginary quadratic field. If every prime p dividing N splits in K, then there is an ideal $\mathfrak{n} \subseteq \mathcal{O}_K$ such that $\mathcal{O}_K/\mathfrak{n} \simeq \mathbb{Z}/N\mathbb{Z}$. This is called the Heegner hypothesis, and the previous lemma implies the existence of Heegner points of level N and discriminant D.

Proof. Let $N = p_1^{a_1} \cdots p_r^{a_r}$. Since each p_i splits in $\mathcal{O}_K$, we have that $p_i\mathcal{O}_K = \mathfrak{p}_{i1} \cdots \mathfrak{p}_{is_i}$. Since there is no ramification $\mathcal{O}_K/\mathfrak{p}_{ij}^{a_i} = \mathbb{Z}/p_i^{a_i}$. Now, take $\mathfrak{n} = \prod_i^r \mathfrak{p}_{i1}^{a_i}$.By the Chinese remainder theorem we get that $\mathcal{O}_K/\mathfrak{n} = \mathbb{Z}/N\mathbb{Z}$. ■

We have seen that there is sort of a correspondence between Heegner points of level N and discriminant D, and binary quadratic forms of discriminant D, which in turn are in correspondence with the class group. This means that there in the situations where Heegner points exist, there is a way to lift the h_K complex multiplication points, to h_K Heegner points.

Proposition 3.3.8. Suppose N and D are such that the corresponding Heegner points exist. There is a one-to-one correspondence between classes modulo $\Gamma_0(N)$ of Heegner points of discriminant D and level N, and pairs $(\beta, \mathfrak{a})$ where $\beta \in \mathbb{Z}/2N\mathbb{Z}$ is such that $D \equiv b^2 \pmod{4N}$ for any lift b of β to $\mathbb{Z}$ and $\mathfrak{a}$ is an ideal class of $\mathcal{O}_K$.

Proof. See [Coh07]8.6.6 for the proof and the explicit correspondence. ■

The usefulness and purpose of Heegner points is clear from the following two propositions. As mentioned above, the fact that τ and $N\tau$ have the same discriminant means that the corresponding curves have complex multiplication by the same ring. Therefore their j-invariants are defined over the same Hilbert class field, and they are acted on by the same Galois group.

Proposition 3.3.9. Let $\tau \in \mathbb{H}$ be a Heegner point of level N and discriminant D. Let H be the Hilbert class field of the K defined in (3.1). Then $\tau \in X_0(N)(H)$ in the singular algebraic model of $X_0(N)$ over $\mathbb{Q}$ mentioned in remark 3.2.10.

Proof. Since $\mathbb{C}/\Lambda_\tau$ and $\mathbb{C}/\Lambda_{N\tau}$ have complex multiplication by $\mathcal{O}_K$, we have by the main theorem of complex multiplication (theorem 3.1.8), that $j(\tau), j(N\tau) \in H$. We mentioned in remark 3.2.10 that the singular algebraic model of $X_0(N)$ has coordinates $(j(\tau), j_N(\tau))$ outside of the singular points. We assume (sadly with loss of generality, the remaining discussion is out of the scope of this document) that τ is not one of those, so in this model $\tau \in X_0(N)(H)$. ■

Proposition 3.3.10. Let $N > 0$ and $D < 0$ satisfying the Heegner hypothesis. Let K be as defined in (3.1) and $\tau_{\mathfrak{a}_1}, \ldots, \tau_{\mathfrak{a}_{h_K}}$ be the Heegner points of level N and discriminant D corresponding to each ideal class. The class group $\mathrm{Cl}(\mathcal{O}_K) = \mathrm{Gal}(H|K)$ acts on the τ_i as follows,

$$\sigma_{\mathfrak{b}}(\tau_{\mathfrak{a}}) = \tau_{\mathfrak{b}^{-1}\mathfrak{a}}.$$

Proof. We take the representation of $X_0(N)$ as the moduli space of $(\varphi : E \longrightarrow E')$ isogenies where E, E' have complex multiplication by the same order and cyclic kernel of order N. By the Heegner hypothesis there is an ideal $\mathfrak{n} \subseteq \mathcal{O}_K$ such that $\mathcal{O}_K/\mathfrak{n} = \mathbb{Z}/N\mathbb{Z}$. Given $\mathfrak{a} \in \mathrm{Cl}(K)$, $(\mathbb{C}/\mathfrak{a} \longrightarrow \mathbb{C}/\mathfrak{a}\mathfrak{n}^{-1})$ can be shown to be corresponding Heegner point of discriminant D and level N. Then, for $\mathfrak{b} \in \mathrm{Cl}(K)$, the main theorem of complex multiplication gives

$$\sigma_{\mathfrak{b}}(\tau_{\mathfrak{a}}) = (\mathbb{C}/\mathfrak{b}^{-1}\mathfrak{a} \longrightarrow \mathbb{C}/\mathfrak{b}^{-1}\mathfrak{a}\mathfrak{n}^{-1}) = \tau_{\mathfrak{b}^{-1}\mathfrak{a}}).$$

■

We put everything together now. Let E be an elliptic curve of conductor N, by the Modularity theorem there is a morphism of algebraic curves $\Phi_N : X_0(N) \longrightarrow E$, defined over $\mathbb{Q}$. Let $D < 0$ be a fundamental discriminant satisfying the Heegner hypothesis for N and K the imaginary quadratic field defined in (3.1). Then there exist $\tau_1, \ldots, \tau_{h_K} \in \mathbb{H}$ Heegner points of level N and discriminant D, we may see them as their class in $X_0(N)$. By proposition 3.3.9, $\tau_i \in X_0(N)(H)$ for the singular algebraic model of $X_0(N)$. Since the map Φ_N is algebraic, $\Phi_N(\tau_i) \in E(H)$, and since it is defined over $\mathbb{Q}$, the action of $\mathrm{Gal}(H|K)$ on the τ_i is preserved. We summarize this in the following theorem.

Theorem 3.3.11. Let E be an elliptic curve of conductor N, Φ_N its modular parameterization, and D and K as defined in the previous paragraph. There are points $P_1, \ldots, P_{h_K} \in E(H)$ such that for $\sigma_{\mathfrak{b}} \in \mathrm{Gal}(H|K)$, $\sigma_{\mathfrak{b}} P_{\mathfrak{a}} = P_{\mathfrak{b}^{-1}\mathfrak{a}}$. Moreover,

$$P = \sum_{i=1}^{h_K} P_i \in E(K).$$

Proof. This comes from the preceding discussion. Similar presentations of this result can be found in [Coh07],[Gal11] or [Dar03]. ■

Thus we have found a way to construct a K-rational point in E. Sometimes this point will even be $\mathbb{Q}$-rational. This construction does however not guarantee that P has infinite order.

Remark 3.3.12. This section has dealt mainly with the case D being a fundamental discriminant satisfying the Heegner hypothesis for N. Different sources define Heegner points differently. We have given the definition in [Coh07]. The paper *Mock Heegner points and congruent numbers*, that we present in the next chapter, takes the definition to be points arising from a D satisfying the Heegner hypothesis. The curve $y^2 = x^3 - x$ has conductor 32, and the points are obtained evaluating modular functions at quadratic number fields where 2 ramifies, so the discriminant of the field does not satisfy the Heegner hypothesis. The construction still yields points defined over the corresponding Hilbert class field and they call them *Mock Heegner points* since the hypothesis is not satisfied.

CHAPTER 4

Mock Heegner points and congruent numbers

In this final chapter, we discuss the paper "Mock Heegner points" by Monsky ([Mon90]). We present the theoretical framework for the case where $D \equiv 1 \pmod 4$. We provide detailed proofs of how this framework can be applied to show that the numbers $p \equiv 5 \pmod 8$ and $2p$, where $p \equiv 3 \pmod 8$, are congruent. Additionally, we include some straightforward computations in Mathematica to make the construction more explicit.

We denote by E the elliptic curve with affine model $y^2 = x^3 - x$, and by E_N the curves $Ny^2 = x^3 - x$. The curves E_N are isomorphic over $\mathbb{Q}$ to the curves $y^2 = x^3 - N^2x$, so we are studying the same problem. The goal of this paper is to show the existence of points of infinite order on the elliptic curves E_N for some N, generally prime or product of two primes. This will give the most general result on the congruence of prime numbers (mod 8) and products of two primes. The idea can be summarized informally in the following steps:

1. We parameterize the curve E with modular functions. More precisely, we parameterize the curve $C : 2Y^2 = X^4 + 1$, which is $\mathbb{Q}$-isomorphic to E but easier to work with.

2. We show that certain subgroups Λ_N of points of C defined over quadratic extensions $\mathbb{Q}(\sqrt{N})$ are isomorphic to the $\mathbb{Q}$-rational points of E_N.

3. We construct points on C, and therefore on E, by evaluating the modular functions at imaginary quadratic arguments in the imaginary quadratic field $\mathbb{Q}(\omega)$ for $\omega = i\sqrt{2D}$.

4. These points are defined over the Hilbert class field of the $\mathbb{Q}(\omega)$ and are permuted by the action of the Galois group. We call them mock Heegner points, by remark 3.3.12.

5. Certain linear combinations of these points can be shown to be in the Λ_N and in some cases can be shown to have infinite order. And therefore N will be congruent.

Let's make the points 2 and 3 a bit more precise. We will study imaginary quadratic fields generated by an element $\omega = i\sqrt{2D}$, where D is an odd square-free positive integer. We will further assume that there is a factorization $2D = NN^*$, with some congruence conditions on these factors, and we will study whether the N appearing here is a congruent number or not. It is convenient to distinguish the two cases $D \equiv 1 \pmod 4$ and $D \equiv 3 \pmod 4$. The paper treats both, but for the sake of simplicity, this chapter will treat in detail only the first case and give a short overview of the second.

4.1 The curve $2Y^2 = X^4 + 1$

Let $E : y^2 = x^3 - x$ be the elliptic curve corresponding to the congruent number problem for 1. We know that E has rank 0, but studying it over the field extension $\mathbb{Q}(\sqrt{N})$ will give us a connection with the curves E_N. Instead of studying E however, we study another curve that is $\mathbb{Q}$-isomorphic to it. Consider the affine curve $2y^2 = x^4 + 1$, its projectivization is singular but by blowing up we can obtain a non-singular model. Let C be its the complete non-singular model, which can be given an abelian variety structure with origin $(1, 1)$.

Proposition 4.1.1.

1. The morphism $(x, y) \mapsto (x^{-1}, yx^{-2})$ is an endomorphism of C of order 2 and therefore corresponds to multiplication by -1. The fixed points are $(1, -1)$,$(-1, 1)$ and $(-1, -1)$, and they constitute the 2-torsion subgroup.

2. The maps $(x, y) \mapsto (x^{-1}, -yx^{-2})$, $(x, y) \mapsto (-x^{-1}, yx^{-2})$ and $(x, y) \mapsto (-x, -y)$ are the translations by $(1, -1)$,$(-1, 1)$ and $(-1, -1)$ respectively.

Proof. The proof is an easy exercise in algebraic manipulation. ■

Proposition 4.1.2. The curve C is isomorphic to E over $\mathbb{Q}$.

Proof. Consider the rational map given by

$$(x, y) \longmapsto \left(\left(\frac{x^2 + 1}{x^2 - 1}\right)^2, \frac{4xy(x^2 + 1)}{(x^2 - 1)^3} \right).$$

It extends to a morphism $\psi : C \longrightarrow E$ defined over $\mathbb{Q}$. If we suppose that this is also a group morphism, we can compute its kernel. We see that $\ker \psi$ is the

2-torsion in C, therefore ψ is a 4-to-1 map and it is $\psi = 2\varphi$ for an isomorphism φ. ■

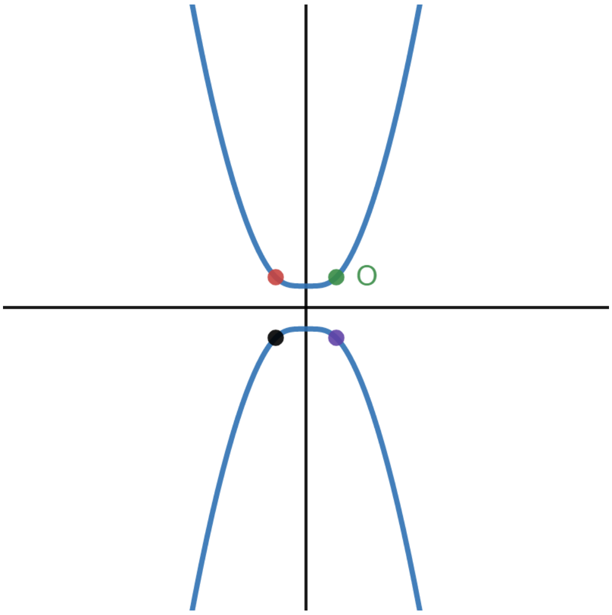

Figure 4.1: Plot of the affine curve $2y^2 = x^4 + 1$ with the origin and 2-torsion points.

As mentioned before, we can use points of C (or E) defined over quadratic field number fields to study the rational points on E_N. Remember that we are in the case $D \equiv 1 \pmod 4$, and suppose that we can factorize $2D$ as $2D = NN^*$ with $N \equiv 5$ or $6 \pmod 8$ and $N^* \equiv 2$ or $3 \pmod 8$.

Definition 4.1.3. Let Λ_N be the subgroup of C consisting of the points rational over $\mathbb{Q}(\sqrt{N})$ that are transformed into their negatives (in the sense of the group law) by the involution of $\mathbb{Q}(\sqrt{N})$.

Proposition 4.1.4. Let T be the group of 2-torsion on C. Then,

1. Λ_N is isomorphic to the $\mathbb{Q}$-rational points of E_N.
2. If $P \in \Lambda_N$ and $P \notin T$, then P has infinite order and N is a congruent number.

Proof.

(1) Let $P = (u, v)$ be a point on $E(\mathbb{Q}(\sqrt{N}))$, this means $u = u_1 + u_2\sqrt{N}$ and $v = v_1 + v_2\sqrt{N}$ with $u_1, u_2, v_1, v_2 \in \mathbb{Q}$. The points of E that are transformed into their negatives by the involution of $\mathbb{Q}(\sqrt{N})$ are those

that satisfy $-P = (u, -v) = (u_1 - u_2\sqrt{N}, v_1 - v_2\sqrt{N})$. This means $u_2 = v_1 = 0$. Therefore $u, v/\sqrt{N} \in \mathbb{Q}$, which is the same as a $\mathbb{Q}$-rational point on E_N. Composing the isomorphism φ with the correspondence $(u, v) \mapsto (u, v/\sqrt{N})$ yields the isomorphism between Λ_N and $E_N(\mathbb{Q})$.

(2) The only torsion in $E_N(\mathbb{Q})$ is the 2-torsion, so if $P \notin T$ then it has infinite order.

■

Remark 4.1.5. Let $P \in \Lambda_N$ and $P \notin T$. If we have that the rank of E_N is bounded by 1, then it will be equal to 1. Moreover, T and P generate a finite index subgroup of Λ_N. If $P \notin 2\Lambda_N \oplus T$ then the index must be odd.

Remark 4.1.6. We have assumed a factorization $2D = NN^*$ with some congruence conditions on N and N^*. These conditions have not been used in the proof of this proposition, and it is in fact true that this isomorphism holds for any N. However, we will construct some points on C dependent on D, and we see in lemma 4.4.6 and proposition 4.4.9 that these assumptions are necessary to assure these points lie in the Λ_N.

4.2 Parametrization of the curve C

The curve C can be parametrized with modular functions X, Y of weight 2 and level 8. These modular functions can be defined in terms of division values of the Weierstrass $\wp$ elliptic function.

Let $z \in \mathbb{H}$ and let Λ_z be the lattice in $\mathbb{C}$ spanned by 1 and z. Let $\wp_z$ be the Weierstrass $\wp$ function associated to Λ_z. This $\wp_z$ and its derivative can be used to parameterize the elliptic curve $\mathbb{C}/\Lambda_z$. Given $u, v \in \mathbb{Z}/8\mathbb{Z}$, not both zero, the numbers $\wp_z(\frac{uz+v}{8})$ are called the *division values* of $\wp$ and correspond to x-coordinates of the 8-torsion points of the curve $\mathbb{C}/\Lambda_z$ in the Weierstrass parameterization. As such, they are algebraic over the field generated by the coefficients of the Weierstrass equation.

Definition 4.2.1. Let $z \in \mathbb{H}$ and let $u, v \in \mathbb{Z}/8\mathbb{Z}$, not both zero. We define $e_{u,v}(z) = \wp_z(\frac{uz+v}{8})$. Note that z appears both in the lattice defining $\wp_z$ and in its argument. For z such that $\mathbb{C}/\Lambda_z$ is defined over a number field, the $e_{u,v}(z)$ will be algebraic numbers.

Remark 4.2.2. We have that $e_{u,v} = e_{-u,-v}$ and, that the action of $\mathrm{SL}(2, \mathbb{Z})$ gives the relation $e_{u,v}(\frac{az+b}{cz+d}) = (cz+d)^2 e_{au+cv,bu+dv}(z)$. If the action is restricted to $\Gamma(8)$, it holds that $au + cv \equiv u \pmod 8$ and $bu + dv \equiv v \pmod 8$, so we have that the $e_{u,v}(z)$ are modular forms of weight 2 and level 8.

Definition 4.2.3. We define the following auxiliary modular functions:

$$\begin{aligned}
E_1 &= e_{0,4} - e_{4,0},\\
E_2 &= e_{4,4} - e_{4,0},\\
E_3 &= E_1 - E_2 = e_{0,4} - e_{4,4},\\
E_4 &= e_{1,0} + e_{1,4} - e_{5,0} - e_{5,4},\\
E_5 &= e_{1,6} + e_{3,6} - e_{5,6} - e_{7,6},\\
E_6 &= e_{2,4} - e_{2,0}.
\end{aligned}$$

We define the modular functions X and Y as follows,

$$\begin{aligned}
X &= \frac{i}{16\sqrt{2}}\frac{E_4E_5}{E_1E_2},\\
Y &= \frac{1}{\sqrt{2}}\frac{E_1+E_2}{E_6}.
\end{aligned}$$

Remark 4.2.4. The functions E_1, E_2 and E_3 are modular functions of level 2, the function E_6 is of level 4 and the functions E_4 and E_5 are of level 8. Therefore X is a modular function of level 8 and Y is of level 4.

Proposition 4.2.5. Let X, Y be the modular functions defined above. Then

1. X, Y are holomorphic on the upper half plane and X has no zeros there.

2. X, Y take positive values on $i\mathbb{R}^+$.

3. $2Y^2 = X^4 + 1$.

4. $X(-2/\lambda)) = X(\lambda)^{-1}$ and $Y(-2/\lambda) = Y(\lambda)X(\lambda)^{-2}$, for any $\lambda \in \mathbb{H}$.

Proof. The proof is relatively straightforward but tedious. It is based on the fact that X can be seen as a meromorphic function on $X(8)$, and Y as a meromorphic function on $X(4)$ and studying their behavior and Fourier expansion at the cusps. ■

We see thus that the X, Y parametrize the C. Through the isomorphism defined in the previous section we can construct points on E by constructing points on C, and we will do this by evaluating the modular functions X, Y at some elements of $\mathbb{Q}(\omega)$.

4.3 Mock Heegner points on C

We will now construct some points on the curve C, these points we will call *mock Heegner points* in the spirit of remark 3.3.12. Remember that $\omega = i\sqrt{2D}$, where

D is an odd square-free positive integer and $D \equiv 1 \pmod 4$. Let $K = \mathbb{Q}(\omega)$. The curve $y^2 = x^3 - x$, and therefore also C, has conductor 32. The discriminant of the field K is $8D$, so the pair 32, $8D$ do not satisfy the Heegner hypothesis. It is nonetheless still possible to find points in $\mathbb{H}$ such that evaluating X and Y at them gives algebraic values.

Let H be the Hilbert class field of K, which as we mentioned in Chapter 3, is the maximal unramified extension of K. By the Artin Reciprocity law, it holds that $\mathrm{Gal}(H|K) \simeq \mathrm{Cl}(K)$. Note also that, since $2D \not\equiv 1 \pmod 4$, then the ring of integers of K is exactly $\mathbb{Z}[\omega]$.

Remark 4.3.1. There is some abuse of notation in this chapter due to the correspondence $\mathrm{Gal}(H|K) \simeq \mathrm{Cl}(K)$. If G is this Galois group, we write automorphisms $\sigma \in G$ and ideal classes $\mathcal{A} \in G$ interchangeably. The automorphism corresponding to $\mathcal{A}$ will be denoted $\sigma_{\mathcal{A}}$.

The following two propositions are consequences of the Shimura reciprocity law ([Cox22]15), which is a generalization of proposition 3.3.10. It is a complicated theory and will not be presented in this thesis.

Proposition 4.3.2 ([Mon90]2.3)**.** Let $D \equiv 1 \pmod 4$ and denote $x = X(\omega), y = Y(\omega)$. Then $x, y \in H$. The point $(x, y) \in C$ is H-rational.

Proposition 4.3.3 ([Mon90]2.4)**.** Let $\mathcal{A}$ be an ideal class of $\mathbb{Z}[\omega]$ represented by an ideal I of odd absolute norm. Let $(a\omega + d, b)$ be a $\mathbb{Z}$-basis of I with $b \equiv 0 \pmod 8$ and $ad > 0$, and norm $\mathfrak{N}(I)$. Let $\eta = (a\omega + b)/d$ and $\sigma_{\mathcal{A}}$ the Artin automorphism. Then

$$\sigma_{\mathcal{A}}^{-1}(x) = \left(\frac{2}{\mathfrak{N}(I)}\right) X(\eta), \quad \text{and} \quad \sigma_{\mathcal{A}}^{-1}(y) = \left(\frac{2}{\mathfrak{N}(I)}\right) Y(\eta).$$

Definition 4.3.4. With the same definitions as above, for the ideal class $\mathcal{A}$ we define the point $P_{\mathcal{A}} = \left(\left(\frac{2}{\mathfrak{N}(I)}\right) X(\eta), \left(\frac{2}{\mathfrak{N}(I)}\right) Y(\eta)\right)$. For the trivial class $\mathcal{O}$ we take $P_{\mathcal{O}} = (x, y)$.

Remark 4.3.5. The points $P_{\mathcal{A}}$ lie on the curve C, and the definition is independent of the representative ideal I, the $\mathbb{Z}$-basis and they are H-rational.

Definition 4.3.6. We denote $C_{\mathbb{R}}$ the points $P \in C$ with $\overline{P} = P$ (the curve represented in Figure 4.1). $C_{\mathbb{R}}^{+}$ consists of the points $(x, y) \in C_{\mathbb{R}}$ with $y > 0$ and $C_{\mathbb{R}}^{-}$ those with $y < 0$. We denote the $\mathfrak{m}$ the maximal ideal $(2, \omega)$ and $P_{\mathfrak{m}}$ the point associated to the class of $\mathfrak{m}$.

Lemma 4.3.7. If $D \equiv 1 \pmod 8$ then $P_{\mathfrak{m}} = -P_{\mathcal{O}}$. If $D \equiv 5 \pmod 8$ then $P_{\mathfrak{m}} = (-1, -1) - P_{\mathcal{O}}$.

Proof. The ideal $\mathfrak{m}$ has an even norm, but it is in the same ideal class as the ideal (D, ω) of odd norm D. Since $\omega/D = -2\omega$ by proposition 4.2.5, we have that $X(\omega/D) = X(\omega)^{-1} = x^{-1}$ and $Y(\omega/D) = Y(\omega)X(\omega)^{-2} = yx^{-2}$. We have now that $P_{\mathfrak{m}} = \left(\left(\frac{2}{D}\right)x^{-1}, \left(\frac{2}{D}\right)yx^{-2}\right)$. By the translation properties in proposition 4.1.1 and the properties of the Jacobi symbol for 2, we get the result. ■

Proposition 4.3.8. If $D \equiv 1 \pmod 4$.

1. Each $P_{\mathcal{A}}$ is H-rational.
2. $\overline{P_{\mathcal{A}}} = P_{\mathcal{A}^{-1}}$. And if J is another ideal class, the Artin automorphism σ_J acts as $\sigma_J P_{\mathcal{A}} = P_{J^{-1}\mathcal{A}}$.
3. $P_{m\mathcal{A}} + P_{\mathcal{A}} = (1,1)$ or $(-1,-1)$ according to $D \equiv 1$ or $5 \pmod 8$, where $m = (\omega, 2)$.
4. Let $q|D$ and $\mathcal{A}$ the class containing (q, ω). Then $P_{\mathcal{A}}$ lies on $C_{\mathbb{R}}^+$ if $q \equiv \pm 1 \pmod 8$ and $C_{\mathbb{R}}^-$ if $q \equiv \pm 3 \pmod 8$.

Proof. (1) and (2) come from the preceding propositions, the action of the Artin isomorphism comes by the construction of the $P_{\mathcal{A}}$. (3) Is a consequence of (2) and the preceding lemma. (4) is consequence of the preceding lemma and the fact that Y takes positive values on $i\mathbb{R}^+$. ■

4.4 The points S_N

In the previous section, we have constructed an H-rational point $P_{\mathcal{A}}$ on C for each ideal class $\mathcal{A}$. By proposition 4.1.4, we can study whether a suitable N appearing in the factorization of $2D$ is a congruent number by finding points on Λ_N, which are $\mathbb{Q}(\sqrt{N})$-rational points. We will construct now, points S_N as sums of some of the $P_{\mathcal{A}}$, where $\mathcal{A}$ runs through a subgroup of $G = \mathrm{Cl}(K) = \mathrm{Gal}(H|K)$. These points will be in the Λ_N and under some conditions we can even show they have infinite order. This requires some careful analysis of the structure of G.

Definition 4.4.1. An ideal class $\mathcal{A} \in G$ is called an *ambiguous class* if its square is the trivial class. That is, $\mathcal{A}$ is in the kernel of the squaring map $G \longrightarrow G^2$.

Fact 4.4.2. For $\mathbb{Z}[\omega]$ and $q|D$ then the class of (q, ω) is ambiguous. All ambiguous classes arise this way, and different divisors of D give rise to different ambiguous classes. Therefore the subgroup of ambiguous classes has order 2^l, where l is the number of primes dividing D. Equivalently $[G : G^2] = 2^l$. The proof can be found in [Cox22]2C.

Definition 4.4.3. Let $p|D$ be prime and $p^* = (-1)^{\frac{p-1}{2}}p$ so that p^* is a square in H. An ideal class $\mathcal{A} \in G$ is in the *principal genus* if $\sigma_{\mathcal{A}}(\sqrt{p^*}) = \sqrt{p^*}$ for all $p|D$. This is equivalent to $\sigma_{\mathcal{A}} \in \mathrm{Gal}(H|K(\sqrt{p_1^*}, \ldots, \sqrt{p_l^*}))$, where the p_i are the primes dividing D. Note that this condition can also be stated in terms of Legendre symbols.

Fact 4.4.4 (Gauss)**.** The principal genus is G^2.

Remark 4.4.5. We will use the parity of the order G^2 in the following discussion. We have that G^2 will have odd order if and only if no ambiguous class but the trivial class lies in G^2, that is, there is no element of order 2 in G^2. The characterization of G^2 as the principal genus allows us to study this through number theory. For example, if D is prime, there is only non-trivial ambiguous class, $\mathfrak{m} = (2, \omega)$, of norm 2. This class lies in the principal genus if and only if 2 is a quadratic residue mod D. By quadratic reciprocity, if $D \equiv \pm 3 \pmod 8$ then 2 is not a quadratic residue mod D and $\mathfrak{m}$ doesn't lie in the principal genus, therefore G^2 has odd order. On the other hand, if $D \equiv \pm 1 \pmod 8$ the opposite happens and G^2 has even order.

We remind that we are assuming a factorization $2D = NN^*$ with $N \equiv 5$ or $6 \pmod 8$ and $N^* \equiv 2$ or $3 \pmod 8$.

Lemma 4.4.6. It holds that $\sqrt{N} \in H$. Denote G_N the subgroup of G consisting of the $\mathcal{A}$ such that $\sigma_{\mathcal{A}}$ fixes $\sqrt{N}$. Then, $\mathfrak{m} \notin G_N$.

Proof.

- Suppose $N \equiv 5 \pmod 8$. Then the prime (2) is inert (and therefore unramified) in $\mathbb{Q}(\sqrt{N})|\mathbb{Q}$, so $\mathfrak{m}$ is inert in $K(\sqrt{N})|K$. The odd primes of K are also unramified in $K(\sqrt{N})|K$, so $\sqrt{N} \in H$. Since 2 is inert, $\sigma_{\mathfrak{m}}(\sqrt{N}) = -\sqrt{N}$.

- Suppose $N^* \equiv 3 \pmod 8$. The same reasoning applies to the extension $K(i\sqrt{N^*})|K$ and we get that $\sqrt{N} \in H$ and that $\sigma_{\mathfrak{m}}(\sqrt{N}) = -\sqrt{N}$.

■

Remark 4.4.7. Through this lemma we can identify $G_N = \mathrm{Gal}(H|K(\sqrt{N}))$. Moreover, since $\sigma_{\mathfrak{m}} \notin G_N$, we have that $\sigma_{\mathfrak{m}}(\sqrt{N}) = -\sqrt{N}$. This means that $\sigma_{\mathfrak{m}}$ restricts to the involution of $\mathbb{Q}(\sqrt{N})$ in $\mathrm{Gal}(\mathbb{Q}(\sqrt{N})|\mathbb{Q})$ (which was important in the definition of the Λ_N in definition 4.1.3).

Definition 4.4.8. We define $S_N = \sum P_{\mathcal{A}}$, where the sum runs over the $\mathcal{A}$ in G_N. This point will be H-rational and, since the $P_{\mathcal{A}}$ are permuted by the G_N, which is identified with $\mathrm{Gal}(H|K(\sqrt{N}))$, the point will be $K(\sqrt{N})$-rational.

Proposition 4.4.9. It holds that $2S_N \in \Lambda_N$ and, if D is composite, $S_N \in \Lambda_N$.

Proof. By proposition 4.3.8, complex conjugation acts as $\overline{P_{\mathcal{A}}} = P_{\mathcal{A}^{-1}}$. Since G_N is a group, $\overline{S_N} = S_N$ and S_N is $\mathbb{Q}(\sqrt{N})$-rational (and so is $2S_N$). By remark 4.4.7, $\sigma_{\mathfrak{m}}$ acts as the involution in $\mathbb{Q}(\sqrt{N})$, and by proposition 4.3.8, $\sigma_{\mathfrak{m}}(P_{\mathcal{A}}) + P_{\mathcal{A}} = (1,1)$ or $(-1,-1)$. This implies that $\sigma_{\mathfrak{m}}(2S_N) = -2S_N$ and therefore that $2S_N \in \Lambda_N$. Since G_N has index 2 in G, if D is composite, $[G : G^2]$ is a power of 2 bigger than 4, so G_N has even order and $\sigma_{\mathfrak{m}}(S_N) = -S_N$. Therefore $S_N \in \Lambda_N$ (summing up $\sigma_{\mathfrak{m}}(P_{\mathcal{A}}) + P_{\mathcal{A}}$ along G_N has an even number of terms). ■

4.5 Congruent numbers

We denote p_i for a prime number such that $p_i \equiv i \pmod 8$. We already have some results on the congruence of the p_i-s. For example, lemma 2.5.2 shows that p_3 is never congruent because the associated elliptic curve always has rank 0. We use the framework developed in this chapter to prove more results.

Proposition 4.5.1 ([Mon90]3.6)**.** Taking $D = N = p_5$, then $2S_N \notin T$. Therefore p_5 is a congruent number.

Proof. Suppose for the sake of a contradiction that $S_N \in 2\Lambda_N \oplus T$, then $2S_N = 2S + t$, for some $S \in \Lambda_N$ and $t \in T$. The point $A = S_N - S$ is 4-torsion, and since it is $\mathbb{Q}(\sqrt{N})$-rational and $E(\mathbb{Q}(\sqrt{N}))$ only has 2-torsion, then it is 2-torsion. We have that $A \in T$, and in particular $A \in \Lambda_N$, so $\sigma_{\mathfrak{m}}(A) + A = (1,1)$. On the other hand, by proposition 4.3.8, and using that $S \in \Lambda_N$ and so $\sigma_{\mathfrak{m}}(S) = -S$, we get the following:

$$\begin{aligned}\sigma_{\mathfrak{m}}(A) + A &= \sigma_{\mathfrak{m}}(S_N) + S_N \\ &= \sum_{\mathcal{A} \in G_N} (\sigma_{\mathfrak{m}}(P_{\mathcal{A}}) + P_{\mathcal{A}}) \\ &= \sum_{\mathcal{A} \in G_N} (-1,-1).\end{aligned}$$

In this case, G_N, is the principal genus, and, by remark 4.4.5, it has odd order. Thus, $\sigma_{\mathfrak{m}}(A) + A = (-1,-1)$. We have reached a contradiction, so $2S_N \notin 2\Lambda_N \oplus T$ and it has infinite order. ■

Proposition 4.5.2 ([Mon90]3.9)**.** Let $D = p_3p_3'$ and $N = 2p_3$, then $S_N \notin 2\Lambda_N \oplus T$. Therefore $2p_3$ is a congruent number.

Proof. The proof of this case is a bit more complicated since D has more than one factor. We break down the proof into several points.

- The number D has two prime factors, so $[G : G^2] = 4$, and since $G^2 \subseteq G_N$, we have that $[G_N : G^2] = 2$. This means that we can decompose S_N as follows,

$$S_N = \sum_{\mathcal{A}\in G^2} P_{\mathcal{A}} + \sum_{\mathcal{A}\notin G^2} P_{\mathcal{A}}. \tag{4.1}$$

  We denote by R the first sum. We claim that the point $S_N - (R + \sigma_{\mathfrak{m}}(R))$ lies in $C_{\mathbb{R}}^-$. Since $D \equiv 1 \pmod 8$, by proposition 4.3.8, we have that $R + \sigma_{\mathfrak{m}}(R) = (1, 1)$, so $S_N - (R + \sigma_{\mathfrak{m}}(R)) = S_N$. There are 4 ambiguous classes: the principal class, $\mathfrak{m}$, (ω, p_3) and (ω, p_3'). Since $[G : G_N] = 2$, there is only one ambiguous class in G_N aside from the principal class. By lemma 4.4.6, $\mathfrak{m} \notin G_N$, so it must be one of the other two. Regardless of which one, by proposition 4.3.8, the points corresponding to these classes lie in $C_{\mathbb{R}}^-$, so we suppose without loss of generality that it is (ω, p_3). Now, the elements in G_N such that $\mathcal{A} \neq \mathcal{A}^{-1}$, that is, the ones corresponding to non-ambiguous classes, come in conjugate pairs, so

$$S_N = P_{\mathcal{O}} + P_{(\omega,p_3)} + \sum P_{\mathcal{A}} + \overline{P_{\mathcal{A}}}.$$

  For any point $P \in C$, $P + \overline{P}$ is real, and it lies in $C_{\mathbb{R}}^+$. Then, since all terms but one lie in $C_{\mathbb{R}}^+$, we get that $S_N \in C_{\mathbb{R}}^-$.

- Let $N' = 2p_3'$, we can define the corresponding $G_{N'}$, $\Lambda_{N'}$ and $S_{N'}$. Both G_N and $G_{N'}$ have index 2 in G and contain G^2 as an index 2 subgroup. Taking $I \in G_N \setminus G^2$, the decomposition in (4.1) can be seen as,

$$\begin{aligned} S_N &= \sum_{\mathcal{A}\in G^2} P_{\mathcal{A}} + \sum_{\mathcal{A}\notin G^2} P_{\mathcal{A}} = R + \sum_{\mathcal{A}\in I^{-1}G^2} P_{\mathcal{A}} \\ &= R + \sum_{\mathcal{A}\in G^2} \sigma_I(P_{\mathcal{A}}) \\ &= R + \sigma_I(R). \end{aligned}$$

  Since $\mathfrak{m}I \in G_{N'} \setminus G^2$, we also have that $S_{N'} = R + \sigma_{\mathfrak{m}I}(R)$. By proposition 4.3.8, $\sigma_I(R) - \sigma_{\mathfrak{m}I}(R) = \sigma_I(R) - \sigma_{\mathfrak{m}}(\sigma_I(R))$ is a torsion point, so it holds that $S_N + S_{N'} - 2R \in T$. Since $T \subseteq \Lambda_{N'}$, subtracting $S_{N'}$ we get that $S_N - 2R \in \Lambda_{N'}$.

- Suppose for the sake of contradiction that $S_N \in 2\Lambda_N \oplus T$, that is, $S_N = 2S + t$, for some $S \in \Lambda_N$ and $t \in T$. We have that $2(S - R) = (S_N - 2R) - t \in \Lambda_{N'}$. The point S is $\mathbb{Q}(\sqrt{N})$-rational by definition, and the point R is H-rational and fixed by G^2, so it is $K(\sqrt{N}, \sqrt{N'})$-rational, it even is $\mathbb{Q}(\sqrt{N}, \sqrt{N'})$-rational because $R = \overline{R}$. We have thus that $S - R$ is $\mathbb{Q}(\sqrt{N}, \sqrt{N'})$-rational and its double is $\mathbb{Q}(\sqrt{N'})$-rational. The curve C only has bad reduction at 2 so, given a number field K and a point $P \in E(\overline{K})$ such that $2P \in E(K)$, the extension $K(P)|K$ is unramified at all odd primes, by proposition 2.3.3. Since $\mathbb{Q}(\sqrt{N}, \sqrt{N'})|\mathbb{Q}(\sqrt{N'})$ ramifies at some odd prime above p_3, we have that $S - R$ must be $\mathbb{Q}(\sqrt{N'})$-rational.

- Both σ_I and $\sigma_{\mathfrak{m}}$ restrict to the involution of $\mathbb{Q}(\sqrt{N'})$. Then,

$$\begin{aligned} S_N &= R + \sigma_I(R), \\ &= R + \sigma_I(R - S) + S, \quad \text{since } S \in \Lambda_N \text{ and } \sigma_I \in G_N, \\ &= R + \sigma_{\mathfrak{m}}(R - S) + S, \quad \text{since } \sigma_{\mathfrak{m}} = \sigma_I \text{ over } \mathbb{Q}(\sqrt{N'}), \\ &= (R + \sigma_{\mathfrak{m}}(R)) + (S + \overline{S}), \quad \text{since } S \text{ is real and so } S = \overline{S}. \end{aligned}$$

Therefore $S_N - R - \sigma_{\mathfrak{m}}(R) = (S + \overline{S}) \in \mathbb{C}_{\mathbb{R}}^{+}$, which is a contradiction with the first point. We conclude that S_N has infinite order and $2p_3$ is a congruent number. ■

This strategy, although with some additional complications, can be applied to prove the other cases. We summarize it in the following proposition.

Proposition 4.5.3 ([Mon90]3.9)**.** In each of the following cases, $S_N \notin 2\Lambda_N \oplus T$:

1. $D = p_5 p_5'$ and $N = p_5$,
2. $D = p_3 p_7$ and $N = p_3 p_7$,
3. $D = p_3 p_7$ and $N = 2p_7$,
4. $D = p_1 p_5$ and $N = p_1 p_5$ if $\left(\frac{p_1}{p_5}\right) = -1$.

4.6 Some comments on the case $D \equiv 3 \pmod 4$

We finally give a quick overview without proofs of the case $D \equiv 3 \pmod 4$. Let now $\omega = i\sqrt{2D}$, with $D \equiv 3 \pmod 4$, let $K = \mathbb{Q}(\omega)$ and H be its Hilbert class field. This case is a bit more complicated because the point $(X(\omega), Y(\omega))$ is no longer H-rational but $H(i)$-rational. The definition of the points $P_{\mathcal{A}}$ has to be adjusted as well.

Proposition 4.6.1 ([Mon90]2.3-2.4)**.** Let $D \equiv 3 \pmod 4$.

1. Let $x = X(\omega)$, $y = Y(\omega)$. Then $x \in H$ and $iy \in H$. The point (x, y) is $H(i)$-rational.

2. Let I be an ideal of odd norm representing an ideal class $\mathcal{A}$ of $\mathbb{Z}[\omega]$. Let $(a\omega + d, b)$ be a $\mathbb{Z}$-basis of I with $b \equiv 0 \pmod 8$ and $ad > 0$. Let $\eta = (a\omega + b)/d$ and $\sigma_{\mathcal{A}}$ the Artin automorphism. Then
$$\sigma_{\mathcal{A}}^{-1}(x) = \left(\frac{2}{\mathfrak{N}(I)}\right) X(\eta), \quad \text{and} \quad \sigma_{\mathcal{A}}^{-1}(iy) = \left(\frac{-2}{\mathfrak{N}(I)}\right) iY(\eta).$$

3. For each ideal class $\mathcal{A}$ we define the $P_{\mathcal{A}} = \left(\left(\frac{2}{\mathfrak{N}(I)}\right) iX(\eta), \left(\frac{-2}{\mathfrak{N}(I)}\right) Y(\eta)\right)$, which are $H(i)$-rational.

Now, $\mathrm{Gal}(H(i)|K) \neq \mathrm{Cl}(K)$, but it contains it as an index 2 subgroup. The action on the points will be a bit more complicated because we also have to consider the involution in $\mathrm{Gal}(H(i)|H)$. The following proposition is the analog of proposition 4.3.8.

Proposition 4.6.2 ([Mon90]2.11)**.**

1. Complex conjugation acts as $\overline{P_{\mathcal{A}}} = (-1, 1) - P_{\mathcal{A}^{-1}}$ and the involution of $H(i)|H$ sends $P_{\mathcal{A}}$ to $P_{\mathcal{A}} + (-1, -1)$.

2. If $\sigma \in \mathrm{Gal}(H(i)|K)$ is trivial on $K(i)$, then it restricts to H to an element $\sigma \in \mathrm{Gal}(H|K) = \mathrm{Cl}(K)$ corresponding to an ideal class J. Then $\sigma(P_{\mathcal{A}}) = P_{J^{-1}\mathcal{A}}$.

3. Action of $\mathfrak{m}$: $P_{\mathfrak{m}\mathcal{A}} - P_{\mathcal{A}} = (1, -1)$ or $(-1, 1)$ if $D \equiv 3$ or $7 \pmod 8$.

In this case proposition 4.1.4 is a bit different, we now assume a factorization of $2D = NN^*$ with $N \equiv 6$ or $7 \pmod 8$ and $N^* \equiv 1$ or $8 \pmod 8$. The isomorphism between C and E is of course the same since it does not depend on N, but the subgroup Λ_N has to be defined differently. In this case, it holds that $i\sqrt{N} \in H$, and the G_N is $\mathrm{Gal}(H|K(i\sqrt{N}))$. The subgroup Λ_N of $\mathbb{Q}(i\sqrt{N})$-rational points on C that are transformed into their negatives by complex conjugation will become now isomorphic to the $\mathbb{Q}$-rational points on E_N. The point S_N is defined similarly to the case $D \equiv 1 \pmod 4$ albeit with some additional complications.

Proposition 4.6.3 ([Mon90]5.14)**.** In each of the following cases, $S_N \notin 2\Lambda_N \oplus T$:

1. $D = p_1 p_7$ and $N = 2D$ if $\left(\frac{p_1}{p_7}\right) = -1$.

2. $D = p_1 p_7$ and $N = D$ if $\left(\frac{p_1}{p_7}\right) = -1$.

3. $D = p_3p_5$ and $N = D$.

4. $D = p_3p_5$ and $N = 2D$.

5. $D = p_1p_3$ and $N = 2D$ if $\left(\frac{p_1}{p_3}\right) = -1$.

6. $D = p_5p_7$ and $N = 2D$.

7. $D = p_5p_7$ and $N = p_7$.

4.7 Conclusion

We have seen how the modular parameterization can be used to construct rational points on an elliptic curve. We have studied the congruent number elliptic curves associated to some particular cases of N through the curve C. The results obtained in the paper [Mon90] are collected in the following theorem, which can be summarized by saying that any $N \equiv 5, 6, 7 \pmod 8$ with at most two odd prime factors is a congruent number except possibly $N = pq$ or $N = 2pq$ with $p \equiv 1 \pmod 8$ and $(\frac{p}{q}) = 1$.

Theorem 4.7.1 ([Mon90]5.13-5.14)**.** Denote by p_i a prime number such that $p \equiv i \pmod 8$.

1. The numbers p_5,p_7,$2p_7$, $2p_3$, p_3p_7, p_3p_5, $2p_3p_5$ and $2p_5p_7$ are congruent numbers.

2. The number p_1p_5 is congruent if $(\frac{p_1}{p_5}) = -1$. The numbers p_1p_7 and $2p_1p_7$ are congruent if $(\frac{p_1}{p_7}) = -1$. The number $2p_1p_3$ is congruent when $(\frac{p_1}{p_3}) = -1$.

4.8 Computations

This final section uses Mathematica and SAGE to explicitly compute these points in the very simple cases $p = 5$, $p = 29$. We see that the points obtained have infinite order. The complications of applying this method, in general, are showcased by taking $p = 1237$, in this case, the associated Hilbert class field is not quadratic over the corresponding imaginary quadratic field and it is not straightforward to compute the values $X(\omega)$, $Y(\omega)$.

Implementation

The modular functions X, Y defined in definitions 4.2.1 and 4.2.3 are implemented in Mathematica using the *WeierstrassP* function and the *WeierstrassInvariants* function:

```
e[u_, v_, z_] :=  WeierstrassP[(u*z + v)/8, WeierstrassInvariants[{1/2, z/2}]]
E1[z_] := e[0, 4, z] - e[4, 0, z]
E2[z_] := e[4, 4, z] - e[4, 0, z]
E3[z_] := E1[z] - E2[z]
E4[z_] := e[1, 0, z] + e[1, 4, z] - e[5, 0, z] - e[5, 4, z]
E5[z_] := e[1, 6, z] + e[3, 6, z] - e[5, 6, z] - e[7, 6, z]
E6[z_] := e[2, 4, z] - e[2, 0, z]
X[z_] := (-1)^(1/2)/(16*(2)^(1/2)) (E4[z]*E5[z])/(E1[z]*E2[z])
Y[z_] := (1/(2)^(1/2))*(E1[z] + E2[z])/E6[z]
```

The following code in SAGE is used to compute class groups, class numbers, and Hilbert class fields:

```
K.<y> = NumberField(x^2+10)
K.class_group()
L = K.hilbert_class_field('z')
```

Computation for $p = 5$

The case $p = 5$ is the simplest case of a congruent prime $p \equiv 5 \pmod 8$, and the application of the procedure in this chapter is very simple. The corresponding imaginary quadratic field is $K = \mathbb{Q}(\omega)$, for $\omega = \sqrt{-10}$. Through SAGE, we can see that its class number is 2, and that the Hilbert class field is $H = K(\sqrt{5}) = \mathbb{Q}(\sqrt{-2}, \sqrt{5})$. To find a point in the curve $5y^2 = x^3 - x$ we compute the point S_5 in the curve $C : 2Y^2 = X^4 + 1$ defined over $\mathbb{Q}(\sqrt{5})$. Since the class number is 2, the sum in the definition of the S_5 only involves the point corresponding to the trivial class, so we need only evaluate X and Y at ω.

We compute $X(\omega)$ and $Y(\omega)$ using the Mathematica functions defined above. The implementation of the *WeierstrassP* function is numerical and it only computes an approximation, however, taking enough decimals, Wolfram Alpha can find closed form approximations. We find that the values are

$$X(\omega) = 2 + \sqrt{5}, \text{and,}$$
$$Y(\omega) = 6 + 3\sqrt{5}.$$

We can check that the point $P_{\mathcal{O}} = (X(\omega), Y(\omega))$ is indeed on C and it clearly is H-rational. Proposition 4.4.9 states that $2P_{\mathcal{O}} \in \Lambda_5$, so it will lead to a point in $5y^2 = x^3 - x$. The proof of proposition 4.1.4 gave us an isomorphism $2\varphi = \psi$, where ψ is the morphism defined in the proof. Thus $\varphi(2P_{\mathcal{O}}) = \psi(P_{\mathcal{O}}) = (\frac{5}{4}, \frac{3\sqrt{5}}{8})$, which is a point in $y^2 = x^3 - x$. Composing with the map $(u, v) \longmapsto (u, v/\sqrt{5})$ we obtain $(\frac{5}{4}, \frac{3}{8})$, a $\mathbb{Q}$-rational point in $5y^2 = x^3 - x$, and this can be transformed into a point in the curve $y^2 = x^3 - 25x$ through the map $(x, y) \longmapsto (5x, 25y)$. The resulting point is $(\frac{25}{4}, \frac{75}{8})$, which is not one of the torsion points. Therefore we have found a non-torsion $\mathbb{Q}$-rational point on $y^2 = x^3 - 25x$.

Computation for $p = 29$

The same procedure can be applied with $p = 29$, which is the second prime $p \equiv 5 \pmod 8$. In this case we take $\omega = \sqrt{-58}$, and fortunately the class number of $K = \mathbb{Q}(\omega)$ is also 2. It suffices to compute the point $P_{\mathcal{O}} = (X(\omega), Y(\omega))$. Using the Mathematica functions and the closed form provided by Wolfram Alpha we obtain the following values:

$$\begin{aligned} X(\omega) &= 70 + 13\sqrt{29}, \text{and,} \\ Y(\omega) &= 6930 + 1287\sqrt{29}, \end{aligned}$$

which as before can be easily checked to be in C. In this case, the Hilbert class field turns out to be $K(\sqrt{29}) = \mathbb{Q}(\sqrt{-2}, \sqrt{29})$, so we see that the point is H-rational. As before, the point $S_{29} = P_{\mathcal{O}}$ and the theorem states that $2P_{\mathcal{O}} \in \Lambda_{29}$. Through the isomorphism we get the point $(\frac{4901}{4900}, \frac{1287\sqrt{29}}{34300})$ in $y^2 = x^3 - x$ which is $\mathbb{Q}(\sqrt{29})$-rational. Through the same transformations applied in the case $p = 5$ we obtain the point

$$\left(\frac{142129}{4900}, \frac{1082367}{343000}\right)$$

in $y^2 = x^3 - 29^2 x$.

Computation for $p = 1237$

The impracticality of this method in general appears now. The prime 1237 is the third prime $p \equiv 5 \pmod 8$, and it is a congruent number by proposition 4.5.1. The computations involved in the procedure become too complicated. The class number of the corresponding imaginary quadratic field is 78, which means that H is not quadratic over K. Moreover, the values $X(\omega)$,$Y(\omega)$ become too big, so WolframAlpha cannot find symbolic approximations (which in any case would not have a nice closed form with square roots as before).

Bibliography

[Ben02] Bennett, M. A. ‘Lucas’ square pyramid problem revisited’. In: *Acta Arithmetica* vol. 105 (2002), pp. 341–347.

[Bir04] Birch, B. ‘Heegner Points: The Beginnings’. In: *Heegner Points and Rankin L-Series*. Cambridge University Press, June 2004, pp. 1–10.

[Bru+08] Bruinier, J. H. et al. *The 1-2-3 of Modular Forms*. Ed. by Ranestad, K. Springer Berlin Heidelberg, 2008.

[Cha06] Chahal, J. S. ‘Congruent Numbers and Elliptic Curves’. In: *The American Mathematical Monthly* vol. 113, no. 4 (Apr. 2006), p. 308.

[Coh07] Cohen, H. *Number Theory, Volume I: Tools and Diophantine Equations*. Springer New York, 2007.

[Con] Conrad, K. *The congruent number problem*. Available at https://kconrad.math.uconn.edu/blurbs/ugradnumthy/congnumber.pdf.

[Cox22] Cox, D. *Primes of the Form $x^2 + ny^2$*. American Mathematical Society, Nov. 2022.

[Dar03] Darmon, H. *Rational Points on Modular Elliptic Curves*. American Mathematical Society, Dec. 2003.

[DS05] Diamond, F. and Shurman, J. *A First Course in Modular Forms*. Springer New York, 2005.

[Gal11] Gala, F. ‘Heegner points on $X_0(N)$’. en. In: (2011).

[Joh10] Johnstone, J. A. ‘Congruent numbers and elliptic curves’. en. In: (2010).

[Loz11] Lozano-Robledo, Á. *Elliptic Curves, Modular Forms, and Their L-functions*. American Mathematical Society, Feb. 2011.

[Mil06] Milne, J. *Elliptic Curves*. BookSurge Publishers, 2006.

[Mon90] Monsky, P. ‘Mock heegner points and congruent numbers’. In: *Mathematische Zeitschrift* vol. 204, no. 1 (Dec. 1990), pp. 45–67.

[She21] Sheth, A. *Heegner points*. Available at https://warwick.ac.uk/fac/sci/maths/people/staff/sheth/heegnerpoints.pdf. 2021.

[Sil09] Silverman, J. H. *The Arithmetic of Elliptic Curves*. Springer New York, 2009.

[Sil94] Silverman, J. H. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer New York, 1994.

[Tun83] Tunnell, J. B. ‘A classical Diophantine problem and modular forms of weight 3/2’. In: *Inventiones Mathematicae* vol. 72, no. 2 (June 1983), pp. 323–334.