University of Groningen

Bachelor's Thesis

Mathematics

Applying 2-descent on elliptic curves to prove the non-existence of a certain triangle-rhombus pair

Author:
Sven Cats

First supervisor:
Dr. Steffen Müller
Second supervisor:
Dr. Pınar Kiliçer

July 2019

Abstract

We call a triangle *rational* if its side lengths are rational and we call a rhombus θ-*rational* if both its side length is rational and the sine and cosine of its smallest angle are rational. In this thesis we prove that there do not exist a rational isosceles triangle and a θ-rational rhombus with the same area and the same perimeter. This is already shown in an article by Zhang and Peng, but this thesis contains a fully explicit proof using the underlying theory. To that end, (hyper)elliptic curves, algebraic number theory and p-adic numbers were studied.

Foreword

First and foremost, I would like to thank my supervisor Steffen Müller for his guidance and helpful feedback. He allowed me to explore a lot of new mathematics, while always offering his help and expertise whenever I got stuck or confused. I expect that my time working on this project will prove very useful for me in my future studies, and I am very thankful for that. Secondly, I would like to thank Pınar Kılıçer for being my second supervisor and her helpful comments on the draft version of my thesis. Finally, I would like to thank other members of the Algebra group in Groningen, particularly Stevan Gajović and Jaap Top, for their interest in my progress and their support.

Groningen, July 31, 2019

Contents

1 Introduction

As many mathematics students know, ideas in algebra and geometry can get very abstract very quickly. It is for this reason that some mathematicians find satisfaction and joy in collecting concrete problems in which the theory can be applied. In this thesis we will solve a particularly nice example of such a problem, as well as outline the theory required in its solution. The problem (and a solution) first appeared in a paper by the Chinese mathematicians Yong Zhang and Junyao Peng, see [26]. In order to understand the theory used in the solution various books and lecture notes were studied. In particular, to name the most important ones, notes from a course at the University of Bayreuth, written by Michael Stoll [21] and a textbook on number theory by Kenneth Ireland and Michael Rosen [13] were consulted.

The central problem of this thesis falls into a certain class of geometric problems that have gained popularity over the past few decades. In a nutshell, these problems have the following form: Given two *rational polygons*[1], can they be chosen such that they have both the same area and the same perimeter? If so, in how many ways (up to scaling of course)? Due to its simplicity, it is not unthinkable that the ancient Greeks already considered problems of this kind. Mathematicians such as Diophantus (210-290 AD), for instance, have extensively studied similar problems (for an engaging account, see [11]). The first appearance in the literature, however, seems to be in [10] from 1995, when Richard Guy introduced a problem from fellow mathematician Bill Sands, asking for examples of a rational right triangle and a rational rectangle with equal area and equal perimeter. It turns out that there is no such pair. In the same paper, he showed the surprising fact that if we replace right triangle by isosceles triangle in Bill Sands' request, then all of a sudden there are infinitely many ways to do it. In the decades to follow, many more problems of this kind were proposed and solved. For a short summary, see the introduction of [26]. We highlight the following, because a similar surprising contrast shows up as in the case of Sands and Guy earlier. Namely, Shane Chern, a colleague of Zhang and Peng, showed in 2016 that there are infinitely many rational right triangle and θ-rational rhombus pairs with equal area and equal perimeter [5], where a θ-rational rhombus is a rational rhombus satisfying the additional condition that the sine and cosine of its smallest angle are rational numbers. That brings us to the year 2017, in which Zhang and Peng proved what will be the main topic of this bachelor's thesis:

Theorem 1.1. *There do not exist a rational isosceles triangle and a θ-rational rhombus with the same area and the same perimeter.*

In their paper, Zhang and Peng reduce the problem to one regarding *hyperelliptic curves* by showing that any such triangle-rhombus pair would yield a *rational point* on a certain curve. Using the computer algebra system Magma, they find all these *rational points* and show that none of them can possibly come from a triangle-rhombus pair. The goal of this thesis is to find the points by hand, using the underlying theory, and thus to have a complete "pen and paper"-solution to the problem.

[1] A polygon having the property that the length of each of its sides is a rational number.

The full strategy of the solution is as follows. First, we deduce that any triangle-rhombus pair as above will induce a rational solution to a certain equation. Then, we will show that the rational solutions to the equation cannot possibly come from a triangle-rhombus pair. To that end, suppose that we have a triangle-rhombus pair as above. Since the area of the θ-rational rhombus is rational, the area of the isosceles triangle is also rational, so its height must be rational. Therefore, the rational isosceles triangle is simply two rational right triangles glued together. By the Pythagorean Theorem, and by rescaling if necessary, we may label the sides of the shapes as in the picture.

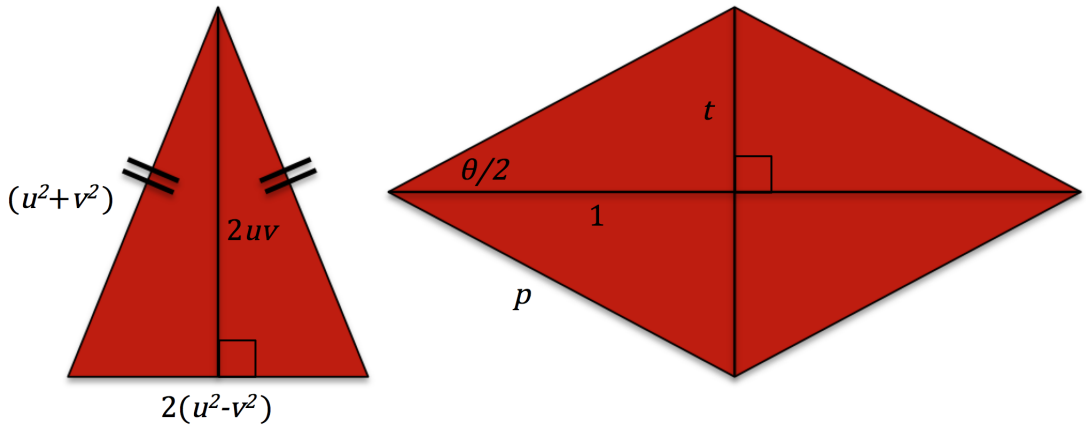

Figure 1: A rational isosceles triangle and an θ-rational rhombus

If we equate the areas and perimeters, we obtain the following system of equations.

$$\begin{cases} 2uv(u^2 - v^2) = p^2 \sin\theta, \\ 4u^2 = 4p \end{cases}.$$

Setting $\sin\theta = 2t/(t^2+1)$ and substituting the second equation into the first yields

$$v(u^2 - v^2)t^2 - u^3 t + v(u^2 - v^2) = 0, \tag{1}$$

so we find that any triangle-rhombus pair gives rise to rational numbers $u, v, t > 0$ satisfying equation (1). We will show that such numbers do not exist. To that end, note that we may view equation (1) as a quadratic equation in t, so if there is a rational solution t, the quadratic formula implies that the discriminant must the square of some rational number w, that is,

$$u^6 - 4u^4v^2 + 8u^2v^4 - 4v^6 = w^2. \tag{2}$$

If we now substitute $x = u/v$ and $y = w/v^3$, then we find that any triangle-rhombus pair induces an *affine rational point* on the curve

$$C: \quad y^2 = x^6 - 4x^4 + 8x^2 - 4,$$

where, for now, an affine rational point is simply a pair of rational numbers (x, y) satisfying the equation above.

In chapter 6, we will find all rational points of C, and we will show that each of them implies that either $u = 0$ or $t = 0$. A quick look at Figure 1 above shows that this solves the problem, because in that case at least one of the shapes has one of its sides equal to zero. Alternatively, we could say that, therefore, there exist no positive rational numbers u, v, t satisfying (1), in which case we are also done.

Finding all rational points on C, however, requires quite a bit of theory. In particular, C is a so-called *hyperelliptic curve*. We will therefore start in chapter 2 with some introductory theory on hyperelliptic curves. There we will also study *elliptic curves*, because it will turn out that we will be able to restrict to an elliptic curve in chapter 6. In order to study (hyper)elliptic curves, the fields of *algebraic number theory* and *p-adic numbers* are useful. We will introduce these fields and some concepts and results from them in chapters 3 and 4, respectively. Finally, the computation of the *2-Selmer group* will be paramount in finding all rational points on C, and we will introduce this group in chapter 5. In chapter 6 we will put all this of theory together to solve the problem.

2 Elliptic and hyperelliptic curves

In this chapter we will introduce *elliptic* and *hyperelliptic curves*. The study of these curves, and in particular the *points* on them, is the domain of arithmetic geometry. It is customary for introductory texts in this field to first treat elliptic curves separately (see for instance [18] or chapters 18 and 19 in [13]), before (if at all) moving on to the more general theory of hyperelliptic curves. However, it is interesting to see the similarities between them right from the start, to emphasise how the former are really a simpler case of the latter. In fact, the main text upon which this chapter is based is a collection of lecture notes on the arithmetic of hyperelliptic curves [21]. The present author studied these and in this chapter the introductory theory will be outlined, along with its simplifications to the theory of elliptic curves.

2.1 The basics

Before we can give the precise definitions of the curves we will be studying, we define a suitable space in which they live.

Definition 2.1. Let g be a nonnegative integer. We define the *weighted projective plane* $\mathbb{P}^2_g$ to be the geometric object for which the points over a field k are equivalence classes of triples $(\xi, \eta, \zeta) \in k^3 \setminus \{(0,0,0)\}$. Here, two triples $(\xi, \eta, \zeta), (\xi', \eta', \zeta')$ are equivalent if $(\xi', \eta', \zeta') = (\lambda\xi, \lambda^{g+1}\eta, \lambda\zeta)$ for some nonzero $\lambda \in k$. The corresponding point over k is written $(\xi : \eta : \zeta)$. The set of points over k is called the *k-rational points* and is denoted by $\mathbb{P}^2_g(k)$.

Definition 2.2. The *coordinate ring* of $\mathbb{P}^2_g$ over k is $k[x, y, z]$, where the grading is as follows. x and z are assigned to have degree 1 and y degree $g + 1$. A polynomial $f \in k[x, y, z]$ is *homogeneous* of total degree d if all its terms have total degree d with respect to the aforementioned grading.

As for the normal projective plane (which we get for $g = 0$), there is a bijection between the points $(\xi : \eta : \zeta) \in \mathbb{P}^2_g$ with $\zeta \neq 0$ and the points of the affine plane $\mathbb{A}^2(k)$:

$$(\xi : \eta : \zeta) \mapsto \left(\frac{\xi}{\zeta}, \frac{\eta}{\zeta^{g+1}}\right) \text{ with inverse } (\xi, \eta) \mapsto (\xi : \eta : 1).$$

Similarly, there is a bijection between the points with $\xi \neq 0$ and $\mathbb{A}^2(k)$. This gives rise to the following definition.

Definition 2.3. The two subsets of $\mathbb{P}^2_g$ determined by $\zeta \neq 0$ and $\xi \neq 0$ are called the *standard affine patches* of $\mathbb{P}^2_g$.

The union of the standard affine patches covers all of $\mathbb{P}^2_g$ except the point $(0 : 1 : 0)$, but as it turns out we will never need it. We can now define (hyper)elliptic curves. In the following definition and afterwards, the field k is understood to be of characteristic different from 2, unless otherwise specified. For a treatment of the characteristic 2 case, see section 14.5 of [6].

Definition 2.4. Let $g > 1$. A *hyperelliptic curve of genus g* over a field k is the solution set over $\mathbb{P}^2_g$ of an equation of the form $y^2 = F(x, z)$, where $F \in k[x, z]$ is homogeneous of degree $2g + 2$ and is squarefree. If we denote the hyperelliptic curve by C, then its set of *k-rational points* is given by

$$C(k) = \{(\xi : \eta : \zeta) \in \mathbb{P}^2_g \,|\, \eta^2 = F(\xi, \zeta)\}.$$

In case $g = 1$, the similarly defined curve is an *elliptic curve*, usually denoted by E.

Note that $C(k)$ is well-defined, for suppose that (ξ', η', ζ') is another representative for the point $(\xi : \eta : \zeta) \in C(k)$. Then, there exists nonzero $\lambda \in k$ such that $(\xi', \eta', \zeta') = (\lambda\xi, \lambda^{g+1}\eta, \lambda\zeta)$. We hence have

$$\eta'^2 = (\lambda^{g+1}\eta)^2 = \lambda^{2g+2}F(\xi, \zeta) = F(\lambda\xi, \lambda\zeta) = F(\xi', \zeta'),$$

because F is homogeneous of degree $2g + 2$. In the sense of Definition 2.2, the polynomial $y^2 - F(x, z) \in k[x, y, z]$ is homogeneous of total degree $2g + 2$.

The intersections between C and the standard affine patches are called the *standard affine patches* of C. They are the given by $y^2 = F(x, 1)$ and $y^2 = F(1, z)$. We write $f(x) = F(x, 1)$ and we will usually define a curve C as

$$C: \quad y^2 = f(x),$$

but we keep in the back of our mind that this represents the projective curve defined by $y^2 = F(x, z)$. In order to recover F from f, we need that f has degree $2g + 1$ or $2g + 2$. Under certain mild conditions, elliptic curves can be defined by an equation of the form $y^2 = x^3+ax+b$, called the *Weierstrass form*. For a detailed account of the conditions under which this can be done and a method of how to do it, we refer to section 1.3 of [18].

Now consider the curve C defined by $y^2 = F(x, z)$, where

$$F(x, z) = f_{2g+2}x^{2g+2} + f_{2g+1}x^{2g+1}z + \cdots + f_1xz^{2g+1} + f_0z.$$

The points on the first standard affine patch of C have the form $(\xi : \eta : 1)$; we will usually denote such points by (ξ, η). We do this because (ξ, η) is a solution to the equation $y^2 = f(x) := F(x, 1)$. The remaining points on C are called the *points at infinity*. They can be found by solving $y^2 = F(1, 0) = f_{2g+2}$. If $f_{2g+2} = 0$, there is one point at infinity, written as $\infty = (1 : 0 : 0)$. If $f_{2g+2} = s^2$, for some $s \in k^\times$, there are two points at infinity, written as $\infty_{\pm s} = (1 : \pm s : 0)$. Otherwise, there are no k-rational points at infinity. Here we also see why we never need the point $(0 : 1 : 0)$, because it is never a k-rational point on C.

Remark. In introductory texts, points on elliptic curves are usually defined over the standard projective plane $\mathbb{P}^2$ instead of the weighted projective plane $\mathbb{P}^2_1$. Namely, for an elliptic curve over $\mathbb{Q}$ defined in Weierstrass form $E: \ y^2 = x^3 + ax + b$, the homogenisation of the defining equation with respect to the grading of the coordinate ring of $\mathbb{P}^2$ is given by $y^2z = x^3+axz^2+bz^3$. Then, we find the point $(0 : 1 : 0) \in E(\mathbb{Q})$; it is not singular, because the partial derivative with respect to z does not vanish. For curves defined by an equation of higher total degree, this does not work, because then the point $(0 : 1 : 0)$ is in fact singular. This is solved by considering the weighted projective plane, as described above.

Example 2.5. Consider the curve $C: \ y^2 = x^6 - 4x^4 + 8x^2 - 4$ over the field $\mathbb{Q}$. The degree of the defining polynomial is 6, so the genus $g = 2$, and the projective form of the equation is $y^2 = x^6 - 4x^4z^2 + 8x^2z^4 - 4z^6$. Hence there are two points at infinity, $\infty_{\pm 1} = (1 : \pm 1 : 0)$. Moreover, we can find the affine points $(1, 1), (1, -1), (-1, 1)$ and $(-1, -1)$. In this thesis we will show that these are all the $\mathbb{Q}$-rational points on the curve C.

We end this section with the following definition.

Definition 2.6. Let $C: \ y^2 = F(x, z)$ be a (hyper)elliptic curve of genus g over the field k. We define the *coordinate ring* of C over k to be the quotient $k[C] = k[x, y, z]/(y^2 - F(x, z))$. Since $y^2 - F(x, z)$ is irreducible and homogeneous, $k[C]$ is an integral domain which inherits the grading defined in Definition 2.2. Moreover, we define $k(C)$ to be the subfield of the field of fractions of $k[C]$ consisting of elements of degree zero. We call $k(C)$ the *function field* of C over k. Its elements are called *rational functions* on C over k.

2.2 Divisors and the Picard group

In this section we will see why elliptic curves are such a simplification compared to hyperelliptic curves, (other than the fact that they have smaller genus and are hence 'simpler' curves in this literal sense). We will do so by introducing *divisors* and the *Picard group*, which will lead us to the so-called *Jacobian variety* J. For a hyperelliptic curve C defined over $\mathbb{Q}$, we can embed the rational points $C(\mathbb{Q})$ into $J(\mathbb{Q})$, which carries a group structure, and there we can do computations. For an elliptic curve E, however, this embedding is surjective, so in some sense we can directly do computations with the points. As we will see, this induced group structure on $E(\mathbb{Q})$ has an elegant geometric interpretation.

We start by defining the *divisor group*. In the following definition, k^{sep} is the *separable closure* of a field k, that is, the subfield of the algebraic closure $\overline{k}$ consisting of the separable elements.

Definition 2.7. Let C be a (hyper)elliptic curve over a field k. The *divisor group* of C, Div_C, is the free abelian group with the set of k^{sep}-points on C as basis. The elements of Div_C are called *divisors*. We write a divisor D as $D = \sum_P n_P \cdot P$, where the sum is over $P \in C(k^{\text{sep}})$ and the $n_P \in \mathbb{Z}$ with at most finitely many $n_P \neq 0$. The *degree* of a divisor D is defined by $\deg(D) = \sum_P n_P$. The set of divisors of degree zero forms a subgroup Div_C^0 of Div_C.

Now consider a nonzero rational function $\phi \in k^{\text{sep}}(C)$. Since it can be represented by a quotient of polynomials, ϕ has finitely many zeros and poles on C. Thus, we can define the following.

Definition 2.8. Let $\phi \in k^{\text{sep}}(C)^\times$. Then, we define the *divisor* of ϕ by

$$\text{div}(\phi) = \sum_P n_P(\phi) \cdot P,$$

where $n_P(\phi)$ is defined by taking a representative quotient of polynomials; if P is a zero of this representative then $n_P(\phi)$ is the multiplicity (in the usual sense), if P is a pole of the representative then $n_P(\phi)$ is minus the order, and it is zero otherwise. A divisor which can be written as the divisor of a rational function is called a *principal divisor*. The subgroup consisting of all principal divisors is denoted by Princ_C. Since Div_C is abelian, we can define the group

$$\text{Pic}_C = \text{Div}_C \,/\, \text{Princ}_C,$$

called the *Picard group* of C.

Lemma 2.9. *Let $\phi \in k^{\text{sep}}(C)^\times$. Then,* $\deg \text{div}(\phi) = 0$.

Proof. This is lemma 4.7 in [21] and we refer to the proof given there. □

From the previous lemma, it follows that $\text{Princ}_C \subset \text{Div}_C^0$. By the homomorphism theorem for groups, deg induces a homomorphism $\text{Pic}_C \to \mathbb{Z}$. We denote the kernel of this homomorphism by Pic_C^0. The following important theorem will be stated without proof.

Theorem 2.10. *Let C be a (hyper)elliptic curve of genus g over a field k. Then, there exists an* abelian variety *J of dimension g over k such that $J(k) = \text{Pic}_C^0(k)$.*

Definition 2.11. The *abelian variety* J is called the *Jacobian* of C.

For $P_0 \in C$, the map $i : C \to J$ given by $P \mapsto [P - P_0]$, where $[P - P_0]$ is the class of the divisor $P - P_0$ modulo principal divisors, turns out (see chapter 4 of [21]) to be injective for $g \geq 1$. Note that we take $P_0 \in C(k)$ because then $i(C(k)) \subset J(k)$. Without getting into the theory of *abelian varieties*, we thus see that the points $C(k)$ can be embedded into $J(k)$, which carries a group structure (induced from the Picard group). Finding the set of k-rational points on C hence comes down to finding $J(k) \cap i(C)$, which is an improvement since we can make use of the group structure of $J(k)$. There is a deep theorem which tells us even more about $J(k)$. Its general form, as proved by André Weil, see [25], is as follows.

Theorem 2.12. *Let k be a* number field[2] *and let J be the Jacobian of a curve over k. Then, $J(k)$ is a finitely generated abelian group.*

For elliptic curves, the situation is even better. In proposition 3.4 of chapter III in [17], it is shown that the map i above is in fact a bijection. That is, instead of working with $J(k)$, Theorem 2.10 implies that $\mathrm{Pic}^0_E(k)$ induces a group structure on the points $E(k)$ themselves! Then, in particular, we have

Theorem 2.13. *Let E be an elliptic curve over $\mathbb{Q}$. Then, $E(\mathbb{Q})$ is a finitely generated abelian group.*

This is the version of Theorem 2.12 that Louis Mordell proved already in 1922, see [14]. The group law on $E(\mathbb{Q})$ has a beautiful geometric interpretation, which is described in many undergraduate textbooks such as [18] and [13]. For two points $P, Q \in E(\mathbb{Q})$, we obtain their sum $P + Q$ by first considering the line L through P, Q (for $P = Q$, take L to be tangent to E at P) and noting that there will be a third point[3] $R \in L \cap E$. We define $P + Q$ to be the image of R when mirrored in the x-axis, see the figure below.

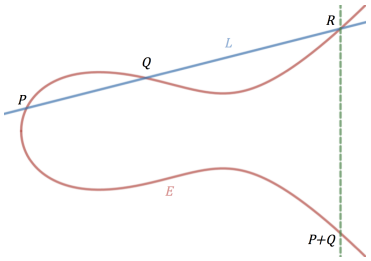

Figure 2: Group law on an elliptic curve

It is rather remarkable that the abstract algebraic group law on $E(\mathbb{Q})$ induced by $\mathrm{Pic}^0_E(Q)$ corresponds to the elegant geometric definition above. The fact that they are equal is also part of proposition 3.4 of chapter III in [17] mentioned above. This group law on the points is the reason that working with elliptic curves is much more convenient than working with hyperelliptic curves, where we have to embed the points into the Jacobian and work with the abstract group law there.

[2] A finite extension of $\mathbb{Q}$; more on these in the next chapter.

[3] Counting multiplicities, that is. This is a special case of *Bézout's theorem*. It is not strictly necessary to impose this general theorem. For instance, explicit formula's for the third intersection point are given in section 3.1 of [13].

3 Algebraic number theory

Many problems in mathematics, including the central one in this thesis, may be phrased as a problem of finding rational or integer solutions to some equation in several variables. A famous example is Fermat's last theorem, stating that for $k > 2$ the only rational solutions x, y to the equation $x^k + y^k = 1$ satisfy $xy = 0$. Such problems make up the field of *Diophantine equations*. Another example is Lagrange's four-square theorem, which states that for any natural number n, there are integer solutions to the equation $n = a^2 + b^2 + c^2 + d^2$. In the context of Diophantine equations, a field known as *algebraic number theory* arises naturally. For instance, in this thesis we are mostly concerned with finding rational solutions to an equation of the form $y^2 = f(x)$ for some polynomial f. We will see that in this case it is beneficial to consider the ring $\mathbb{Q}[x]/(f)$. If f splits completely over the rationals, then there is not much to it, for then $\mathbb{Q}[x]/(f)$ is simply isomorphic to copies of $\mathbb{Q}$. If, on the other hand, f has irreducible factors of higher degree than one, it gets more interesting. Consider for example the case where f is an irreducible cubic polynomial. Then, $\mathbb{Q}[x]/(f)$ is a cubic extension of $\mathbb{Q}$ and a so-called *number field*. The study of number fields and their subrings is the domain of algebraic number theory. This chapter will serve as a reference for the next chapters, containing concepts and results from algebraic number theory that will be used later. In this chapter we will mostly follow chapter 12 of the book by Ireland and Rosen [13]. Their treatment is special in the sense that they build up the theory differently from other books, in order to prove big results as quickly as possible. A more standard treatment of algebraic number theory can be found, for instance, in the lecture notes by Stevenhagen [19].

3.1 Norm, trace and discriminant

A field K is called a *number field* if it is a finite extension of $\mathbb{Q}$, in which case we usually denote $[K : \mathbb{Q}]$ by n. The theory in this section holds more generally for any finite extension of fields, but since we will only be concerned with number fields we only consider the extension $K/\mathbb{Q}$.

For a basis $\alpha_1, \dots \alpha_n$ of $K/\mathbb{Q}$ and $\alpha \in K$, we have $\alpha\alpha_i = \sum_j a_{ij}\alpha_j$ for some $a_{ij} \in \mathbb{Q}$. There are of course many possibilities for a basis of a field extension, but as we will see some bases are 'better' than others, or at least more natural. These are known as *integral bases*; the following concepts will be useful in the study of these bases.

Definition 3.1. In the notation above, we define the *norm* of α, $N(\alpha)$, to be $\det(a_{ij})$. We define the *trace* of α, $t(\alpha)$, to be $a_{11} + \cdots + a_{nn}$.

By our knowledge from linear algebra, we see that the definition above is independent of the chosen basis, that the norm is multiplicative and that the trace is additive. Let $\sigma_1, \dots, \sigma_n$ be the distinct embeddings of K into some algebraic closure of $\mathbb{Q}$ which fix $\mathbb{Q}$ and write $\alpha^{(j)} = \sigma_j(\alpha)$ for $\alpha \in K$, where $\alpha^{(1)} = \alpha$. Using linear algebra, we see that $t(\alpha) = \alpha^{(1)} + \cdots + \alpha^{(n)}$ and $N(\alpha) = \alpha^{(1)} \cdots \alpha^{(n)}$. If α satisfies a monic polynomial with integer coefficients, then so do the $\alpha^{(i)}$. We will see in section 3 that this implies that $t(\alpha)$ and $N(\alpha)$ are integers.

Definition 3.2. If $\alpha_1, \dots, \alpha_n \in K$, then we define the discriminant $\Delta(\alpha_1, \cdots, \alpha_n)$ to be $\det(t(\alpha_i\alpha_j))$.

When something is called a discriminant, usually something special is the case when it is (not) equal to zero. Indeed, it is not hard to verify, see for instance proposition 12.1.1 of [13], that elements $\alpha_1, \ldots, \alpha_n \in K$ form a basis for $K/\mathbb{Q}$ if and only if $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$. Another useful property is the following.

Proposition 3.3. *Let $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ be bases for $K/\mathbb{Q}$. If $\alpha_i = \sum_j a_{ij}\beta_j$ for some $a_{ij} \in \mathbb{Q}$, then $\Delta(\alpha_1, \ldots, \alpha_n) = \det(a_{ij})^2 \Delta(\beta_1, \ldots, \beta_n)$.*

Proof. We have the identity $\alpha_i\alpha_k = \sum_j \sum_l a_{ij}a_{kl}\beta_j\beta_l$. If we take the trace on both sides and define the matrices $A = (t(\alpha_i\alpha_j)), B = (t(\beta_j\beta_l), C = (a_{ij})$, then we have $A = C^T BT$. Taking determinants in this expression yields the desired result. □

3.2 Ring of integers

Definition 3.4. An *algebraic integer* is a root of a monic polynomial with integer coefficients. For a number field K, we define its *ring of integers* $\mathcal{O}_K$ as the set of algebraic integers in K.

Before we verify that $\mathcal{O}_K$ is indeed a ring, we do a sanity check.

Proposition 3.5. *The ring of integers of* $\mathbb{Q}$ *is* $\mathbb{Z}$.

Proof. We have that $\mathbb{Z} \subset \mathcal{O}_{\mathbb{Q}}$, because any $r \in \mathbb{Z}$ satisfies the polynomial $x - r$. In order to show that $\mathcal{O}_{\mathbb{Q}} \subset \mathbb{Z}$, take $r \in \mathcal{O}_{\mathbb{Q}}$. Then r is the root of a polynomial $x^n + b_1 x^{n-1} + \cdots + b_n$ where $b_i \in \mathbb{Z}$. Assume without loss of generality that $r = c/d$, where $\gcd(c, d) = 1$. Then,

$$c^n + b_1 c^{n-1} d + \cdots + b_n d^n = 0.$$

Reducing this equation modulo d yields that $d \mid c^n$. Since c and d are relatively prime we have $d \mid c$ and hence $r = c/d \in \mathbb{Z}$. □

Now we will show that the ring of integers $\mathcal{O}_K$ of a number field K is indeed a ring. We will do this by showing that the set of all algebraic integers $\Omega \subset \mathbb{C}$ is a ring, from which it follows that $\mathcal{O}_K = K \cap \Omega$ is a ring. First we state the following lemma.

Lemma 3.6. *Suppose that a nonempty subset* $W \subset \mathbb{C}$ *satisfies the following properties:*

(i) For any $\gamma_1, \gamma_2 \in W$, *we have* $\gamma_1 \pm \gamma_2 \in W$.

(ii) There exist $\gamma_1, \ldots, \gamma_l \in W$ *such that every* $\gamma \in W$ *can be written as* $\sum_{i=1}^{l} b_i \gamma_i$ *with* $b_i \in \mathbb{Z}$.

That is, W *is a finitely generated* $\mathbb{Z}$-module. *If* $\omega \in \mathbb{C}$ *is such that* $\omega\gamma \in W$ *for all* $\gamma \in W$, *then* $\omega \in \Omega$.

Proof. Let $\omega \in \mathbb{C}$ be such that $\omega\gamma \in W$ for all $\gamma \in W$. We show that $\omega \in \Omega$. We have that $\omega\gamma_i \in W$ for $i = 1, \ldots, l$, that is, for the elements of which the existence is guaranteed in (ii). For each i, we thus have $\omega\gamma_i = \sum_{j=1}^{l} a_{ij}\gamma_j$, with $a_{ij} \in \mathbb{Z}$. Therefore, $\sum_{j=1}^{l}(a_{ij} - \delta_{ij}\omega)\gamma_j = 0$, where $\delta_{ij} = 0$ if $i \neq j$ and $\delta_{ij} = 1$ if $i = j$. It follows that $\det(a_{ij} - \delta_{ij}\omega) = 0$. By writing out the determinant we see that ω satisfies (possibly up to a sign) a monic polynomial with integer coefficients and hence $\omega \in \Omega$. □

Proposition 3.7. *The ring of integers* $\mathcal{O}_K$ *of a number field* K *is a ring.*

Proof. As mentioned, it suffices to show that Ω is a ring. We will show that Ω is a subring of $\mathbb{C}$. It is clear that $1 \in \Omega$. Let $\omega_1, \omega_2 \in \Omega$. To see that $\omega_1 - \omega_2$ and $\omega_1\omega_2$ are in Ω, suppose that $\omega_1^n + b_1\omega_1^{n-1} + \cdots + b_n = 0$ and $\omega_2^m + c_1\omega_2^{m-1} + \cdots + c_m = 0$ for $b_i, c_j \in \mathbb{Z}$. Let W be the set of all $\mathbb{Z}$-linear combinations of $\omega_1^i\omega_2^j$, where $0 \leq i < n$ and $0 \leq j < m$. Clearly, W is a finitely generated $\mathbb{Z}$-module. If $\gamma \in W$, then $\omega_i\gamma \in W$ for $i = 1, 2$ using the polynomial ω_i satisfies. Therefore $(\omega_1 - \omega_2)\gamma \in W$ and $\omega_1\omega_2\gamma \in W$. By Lemma 3.6, $\omega_1 - \omega_2, \omega_1\omega_2 \in \Omega$. □

3.3 Factorisation

For the rational numbers $\mathbb{Q}$, we have learned already in elementary school the method for 'division with remainder' in the ring of integers $\mathbb{Z}$ of $\mathbb{Q}$. Given nonzero $a, b \in \mathbb{Z}$, the teacher taught us how to find $q, r \in \mathbb{Z}$, with $|r| < |b|$, such that $a = qb + r$. This simple procedure makes $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ into a *Euclidean domain*. In standard algebra texts such as [23] it is shown that this implies that $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ is a *principal ideal domain*, which in turn implies one of the properties of $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ we hold most dearly: it is a *unique factorisation domain*. That is, we can factor any nonzero $n \in \mathbb{Z}$ uniquely (up to sign) as a product of prime numbers (the irreducible elements of $\mathbb{Z}$). This fact is also taught in elementary school, and it has become so familiar to us that (in my personal experience) many people feel that any proof of this fact is unnecessary or even pedantic. However, what these critics probably do not know (and you should tell them when you encounter them!) is that it is not obvious at all; in fact, there are fields K which are in some sense very similar to $\mathbb{Q}$ (read: number fields) for which it fails completely. For example, the ring of integers of the number field $K = \mathbb{Q}(\sqrt{-5})$ is $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, see proposition 13.1.1 in [13], but

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

It is easy to verify that the elements in the factorisation above are irreducible and that the elements on the left cannot be obtained from the ones on the right by multiplying by a unit. This implies that $\mathcal{O}_K$ is not a unique factorisation domain and hence not a principal ideal domain.

Luckily, the situation is not as bad as it seems. Although it does not hold in general that $\mathcal{O}_K$ is a unique factorisation domain, it is a so-called *Dedekind domain*, meaning that each nonzero ideal can be written uniquely as a product of prime ideals. In this section, we will show that $\mathcal{O}_K$ is a Dedekind domain using a method due to Adolf Hurwitz, as outlined in section 12.2 of [13]. Along the way we will encounter the *class number* h_K, which measures 'how far' $\mathcal{O}_K$ is from being a principal ideal domain. We end the section with a theorem by Kummer and Dedekind, which shows how to explicitly factorise certain ideals.

We should not be fooled by the earlier example in thinking that it is always the case that the ring of integers of a field of the form $K = \mathbb{Q}(\alpha)$ is given by $\mathcal{O}_K = \mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{n-1}$, see for example 13.1.1 in [13]. Moreover, there are even extensions $K/\mathbb{Q}$ for which there does not exist any element α such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$, see [19, chapter 3]. However, for any ideal A of $\mathcal{O}_K$ (and so of $\mathcal{O}_K$ itself), we can always find an *integral basis*: a basis $\alpha_1, \ldots, \alpha_n \in A$ for $K/\mathbb{Q}$ such that $A = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$. This is the case precisely when $|\Delta(\alpha_1, \ldots, \alpha_n)|$ is minimal. To show this we first need the following.

Lemma 3.8. *Let A be an ideal in $\mathcal{O}_K$. Then, A contains a basis for $K/\mathbb{Q}$.*

Proof. See proposition 12.2.1 of [13]. □

Lemma 3.9. *For $\alpha \in \mathcal{O}_K$, we have $t(\alpha), N(\alpha) \in \mathbb{Z}$.*

Proof. By the discussion following Definition 3.1 and the fact that the ring of integers is indeed a ring, we see that $t(\alpha)$ and $N(\alpha)$ are in the ring of integers of $\mathbb{Q}$. Since they are also in $\mathbb{Q}$, it follows from Proposition 3.5 that they are integers. □

Proposition 3.10. *Let A be an ideal in $\mathcal{O}_K$ and suppose that $\alpha_1, \ldots, \alpha_n \in A$ is a basis for $K/\mathbb{Q}$ with $|\Delta(\alpha_1, \ldots, \alpha_n)|$ minimal. Then, $A = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$.*

Proof. By the preceding lemma and the definition of the discriminant, $|\Delta(\alpha_1, \ldots, \alpha_n)|$ is positive integer, so there is a basis such that it is minimal. Let $\alpha \in A$. Since $\alpha_1, \ldots, \alpha_n \in A$ is a basis for $K/\mathbb{Q}$, we can write $\alpha = \gamma_1\alpha_1 + \cdots + \gamma_n\alpha_n$ for $\gamma_i \in \mathbb{Q}$. We will show that $\gamma_i \in \mathbb{Z}$, proving the desired result. Suppose for contradiction that there is some $\gamma_i \notin \mathbb{Z}$ and assume without loss of generality that $\gamma_1 \notin \mathbb{Z}$. We can write $\gamma_1 = m + \theta$ for some $m \in \mathbb{Z}$ and $0 < \theta < 1$. Define a basis $\beta_1, \ldots, \beta_n \in A$ by $\beta_1 = \alpha - m\alpha_1$ and $\beta_i = \alpha_i$ for $i > 1$. The transition matrix is given by

$$\begin{pmatrix} \theta & \gamma_2 & \gamma_3 & \cdots & \gamma_n \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

By Proposition 3.3, we have $|\Delta(\beta_1, \ldots, \beta_n)| = \theta^2|\Delta(\alpha_1, \ldots, \alpha_n)| < |\Delta(\alpha_1, \ldots, \alpha_n)|$, which contradicts the facts that $|\Delta(\alpha_1, \ldots, \alpha_n)|$ is minimal. Therefore, all $\gamma_i \in \mathbb{Z}$, as desired. □

The discriminant of two integral bases is equal by Proposition 3.3, and we call this common value the *discriminant of* A, denoted by $\Delta(A)$. We use this to define the *discriminant of* $K/\mathbb{Q}$ by $\Delta_K = \Delta(\mathcal{O}_K)$.

In addition, there is a way to quantify 'how large' an ideal A of $\mathcal{O}_K$ is. This is usually done by defining the *norm* of an ideal A by the size of $\mathcal{O}_K/A$. Of course, this only makes sense if $\mathcal{O}_K/A$ is finite; this is what we will show next, using a small auxiliary result.

Lemma 3.11. *Let A be an ideal in $\mathcal{O}_K$. We have that $A \cap \mathbb{Z} \neq \{0\}$.*

Proof. See lemma 2 of section 12.2 of [13]. □

Proposition 3.12. *Let A be an ideal in $\mathcal{O}_K$. Then, $\mathcal{O}_K/A$ is finite.*

Proof. Using the lemma, we can take a nonzero $a \in A \cap \mathbb{Z}$. Let (a) be the ideal generated by a in $\mathcal{O}_K$. Since $(a) \subset A$, it suffices to show that $\mathcal{O}_K/(a)$ is finite. By Proposition 3.10, we may write $\mathcal{O}_K = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$. We claim that $S = \{\sum \gamma_i\omega_i \,|\, 0 \leq \gamma_i < a\}$ is a set of coset representatives for $\mathcal{O}_K/(a)$. To see this, let $\omega = \sum m_i\omega_i \in \mathcal{O}_K$. Writing $m_i = q_ia + \gamma_i$ with $0 \leq \gamma_i < a$ yields that ω is congruent to $\sum \gamma_i\omega_i \in S$ modulo (a), so every coset contains at least one element of S. To that it is exactly one, suppose that $\sum \gamma_i\omega_i, \sum \gamma_i\omega_i \in S$ are congruent modulo (a). Since the ω_i form a basis, they are linearly independent and it follows that $\gamma_i - \gamma_i'$ is divisible by a. Since $0 \leq \gamma_i, \gamma_i' < a$, we have $\gamma_i = \gamma_i'$. Therefore, S is a set of representatives for $\mathcal{O}_K/(a)$. Since S contains a^n elements, it follows that $\mathcal{O}_K/(a)$ does too and hence $\mathcal{O}_K/A$ is finite. □

Now we want to define the *class number* h_K of a number field K as the amount of equivalence classes under a certain equivalence relation. We want the class number to measure, in some sense, how close $\mathcal{O}_K$ is to being a principal ideal domain. Consider the following relation $\sim$ on the ideals of $\mathcal{O}_K$[4]. For two ideals A, B of $\mathcal{O}_K$ we have $A \sim B$ if and only if there exist nonzero

[4]Most texts define $\sim$ on *fractional ideals*, which are $\mathcal{O}_K$-submodules A satisfying $uA \subset \mathcal{O}_K$ for some $u \in \mathcal{O}_K^\times$. Clearly, this includes ideals of $\mathcal{O}_K$ (take $u = 1$).

$\alpha, \beta \in \mathcal{O}_K$ such that $(\alpha)A = (\beta)B$. It is straightforward to check that this is an equivalence relation. We define the following.

Definition 3.13. The equivalence classes under $\sim$ are called *ideal classes*. The number of ideal classes, h_K, is called the *class number* of K.

The following result tells us that h_K indeed measures how close $\mathcal{O}_K$ is to being a principal ideal domain.

Proposition 3.14. *$h_K = 1$ if and only if $\mathcal{O}_K$ is a principal ideal domain.*

Proof. Suppose that $h_K = 1$ and let $A \subset \mathcal{O}_K$ be an ideal. We have that $A \sim \mathcal{O}_K$, so there exist nonzero $\alpha, \beta \in \mathcal{O}_K$ such that $(\alpha)A = (\beta)$ and hence $A = (\beta/\alpha)$ is principal. Conversely, if $\mathcal{O}_K$ is a principal ideal domain and $A, B \subset \mathcal{O}_K$ are ideals, then $A = (\alpha)$ and $B = (\beta)$. Therefore, $(\beta)A = (\alpha)B$ and hence $A \sim B$. □

One of the main results in algebraic number theory is that h_K is finite. A quick way, due to Adolf Hurwitz, to show this is outlined in section 12.2 of [13]. It uses a lemma which is a generalisation of the euclidean algorithm ('division with remainder') mentioned in the introduction of this section above.

Lemma 3.15. *There exists a positive integer M depending only on K such that the following holds. If $\alpha, \beta \in \mathcal{O}_K$ and β is nonzero, then there is an integer t, $1 \leq t \leq M$ and an element $\omega \in \mathcal{O}_K$ such that $|N(t\alpha - \omega\beta)| < |N(\beta)|$.*

Proof. See lemma 5 of section 12.2 of [13]. □

Theorem 3.16. *The class number of K is finite.*

Proof. Let $A \subset \mathcal{O}_K$ be an ideal. By Lemma 3.9, the absolute value of the norm of a nonzero element of A is a positive integer. Take $\beta \in A$ such that $|N(\beta)|$ is minimal. By Lemma 3.15, for any $\alpha \in A$ we can find t between 1 and M (recall that M only depends on K), such that $|N(t\alpha - \omega\beta)| < |N(\beta)|$ for some $\omega \in \mathcal{O}_K$. Since $t\alpha - \omega\beta \in A$, the minimality of $|N(\beta)|$ implies that $t\alpha = \omega\beta$ and hence $M!\alpha = \frac{M!}{t}\omega\beta \in (\beta)$. Therefore, $B = (1/\beta)M!A \subset \mathcal{O}_K$ is an ideal and $M!A = (\beta)B$. Since $\beta \in A$ we have $M!\beta \in (\beta)B$, so $M! \in B$. By Proposition 3.12, $\mathcal{O}_K/(M!)$ is finite, so there are only finitely many ideals B containing $M!$. Thus $A \sim B$ for one of finitely many ideals B, showing that h_K is finite. □

For our purposes, we would also like to be able to find the class number in a concrete example. A useful tool for this is the *Minkowski bound*. We state it here without proof. If the reader is interested in a proof, chapter 5 of [19] contains a proof of Minkowski's theorem regarding the existence of lattice points in symmetric convex bodies and shows how it implies the following result.

Theorem 3.17. *Let $K/\mathbb{Q}$ be an extension of degree n and let s be half the amount of complex embeddings. Then, every ideal class in K contains an ideal A such that the norm of A does not exceed the Minkowski bound given by*

$$M_K = \sqrt{|\Delta_K|}\left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}.$$

In particular, for some number fields the Minkowski bound provides an easy way to show that it has class number 1: if $M_K < 2$, then every ideal class contains $\mathcal{O}_K$ and hence there is only one ideal class.

Before we continue to show that $\mathcal{O}_K$ is a Dedekind domain, we remark that the set of ideal classes is usually called the *ideal class group*, and we will show how to turn it into a group using the following result.

Proposition 3.18. *Let A be an ideal in $\mathcal{O}_K$. There exists an integer k with $1 \leq k \leq h_K$ such that A^k is principal.*

In the proof of this proposition, the following result is used:

Proposition 3.19. *Let A, B be ideals in $\mathcal{O}_K$. If $\omega \in D$ is such that $(\omega)A = BA$, then $(\omega) = B$.*

Its proof can be found under proposition 12.2.4 in [13]. Now we prove Proposition 3.18.

Proof. Consider the set of ideals $\{A^i \,|\, 1 \leq i \leq h_K + 1\}$. By the pigeonhole principle, at least two of them must be equivalent, so $A^i \sim A^j$ for some $i < j$. There exist nonzero $\alpha, \beta \in \mathcal{O}_K$ such that $(\alpha)A^i = (\beta)A^j$. We will show that $B = A^{j-i}$ is principle, proving the proposition. We have that $(\alpha)A^i = (\beta)BA^i$ and hence $(\alpha/\beta)A^i \subset A^i$. Therefore, $\alpha/\beta \in \mathcal{O}_K$. Since $(\alpha/\beta)A^i = BA^i$, it follows from Proposition 3.19 that $B = (\alpha/\beta)$ is principal. □

As promised, we put a group structure on the set of ideal classes of $\mathcal{O}_K$. Since we will neither need this in the rest of this chapter nor in any applications of algebraic number theory later on, we will be brief. Let $\overline{A}$ denote the ideal class of an ideal A of $\mathcal{O}_K$. Then we define the product of $\overline{A}$ and $\overline{B}$ by $\overline{AB}$. One can easily check that this operation is well-defined and associative. The identity element of the group is $\overline{\mathcal{O}_K}$ and Proposition 3.18 shows that the inverse of $\overline{A}$ is $\overline{A^{k-1}}$.
The following two propositions regard 'division' of ideals. They will be helpful in showing that ideals can be factored as the product of prime ideals.

Proposition 3.20. *Let A, B, C be ideals in $\mathcal{O}_K$. If $AB = AC$, then $B = C$.*

Proof. By Proposition 3.18, there exists k such that $A^k = (\alpha)$ for some $\alpha \in \mathcal{O}_K$. Multiplying both sides of $AB = AC$ by A^{k-1} yields $(\alpha)B = (\alpha)C$ and hence $B = C$. □

Proposition 3.21. *Let A, B be ideals in $\mathcal{O}_K$. If $B \supset A$, then there is an ideal C such that $A = BC$.*

Proof. Again by Proposition 3.18, there exists a positive k such that $B^k = (\beta)$ for some $\beta \in \mathcal{O}_K$. Since $A \subset B$, we have $B^{k-1}A \subset B^k = (\beta)$ and hence $C = (1/\beta)B^{k-1}A \subset \mathcal{O}_K$ is an ideal. This C satisfies $BC = (1/\beta)B^kA = (1/\beta)(\beta)A = A$, as desired. □

In this sense, if an ideal contains another ideal, it divides it. We can now prove the following.

Proposition 3.22. *Every ideal in $\mathcal{O}_K$ can be written as a product of prime ideals.*

Proof. Let A be a proper ideal in $\mathcal{O}_K$. Then, it is contained in a maximal ideal $\mathfrak{p}_1$. This is proved using Zorn's lemma, see for example corollary IV.3.4 in [24]. By Lemma 3.21, there exists an ideal B_1 in $\mathcal{O}_K$ such that $A = \mathfrak{p}_1 B_1$. If B_1 is a proper ideal, then it is contained in an maximal ideal $\mathfrak{p}_2$ and there exists B_2 such that $A = \mathfrak{p}_1\mathfrak{p}_2 B_2$. If we continue in this way we obtain the proper inclusions $A \subset B_1 \subset B_2 \cdots$. By Proposition 3.12, $\mathcal{O}_K/A$ is finite, so A is contained in finitely many ideals. Therefore, there exists g such that $B_g = \mathcal{O}_K$ and hence $A = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_g$. Since maximal ideals are prime, this proves the proposition. □

For a prime ideal $\mathfrak{p}$, the chain of inclusions $\mathfrak{p} \supset \mathfrak{p}^2 \supset \mathfrak{p}^3 \cdots$ is proper, because if $\mathfrak{p}^i = \mathfrak{p}^{i+1} = \mathfrak{p}\mathfrak{p}^i$, then $\mathfrak{p} = \mathcal{O}_K$ by Lemma 3.20. The following definition relies on this fact.

Definition 3.23. Let A be an ideal in $\mathcal{O}_K$ and let $\mathfrak{p}$ be a prime ideal. We define $\operatorname{ord}_\mathfrak{p} A$ to be the nonnegative integer t satisfying $\mathfrak{p}^t \supset A$ and $\mathfrak{p}^{t+1} \not\supset A$.

Note the analogy with the integers here. For a nonzero integer n there is also a unique nonnegative integer t such that $p^t | n$ but $p^{t+1} \nmid n$. With this analogy in mind, the following properties will also seem familiar.

Proposition 3.24. *Let A, B be ideals in $\mathcal{O}_K$ and let $\mathfrak{p}, \mathfrak{p}'$ be unequal prime ideals. Then, the following properties hold.*

(i) $\operatorname{ord}_\mathfrak{p} \mathfrak{p} = 1$

(ii) $\operatorname{ord}_\mathfrak{p} \mathfrak{p}' = 0$

(iii) $\operatorname{ord}_\mathfrak{p} AB = \operatorname{ord}_\mathfrak{p} A + \operatorname{ord}_\mathfrak{p} B$.

In the proof of this proposition we will use that prime ideals of $\mathcal{O}_K$ are maximal. This follows from the fact that, for a prime ideal $\mathfrak{p}$, $\mathcal{O}_K/\mathfrak{p}$ is a finite integral domain by Proposition 3.12. It is an exercise in ring theory to show that a finite integral domain R is a field. Since it is a bit off-topic, we will not provide all the details, but it follows from the fact that the map from R to itself given by $x \mapsto rx$ is a bijection for nonzero $r \in R$. Namely, then there exists $s \in R$ such that $rs = 1$ and hence each r in the commutative ring R is a unit, i.e. R is a field.

Proof. Part (i) follows immediately from the definition. To see that (ii) holds, suppose that $\operatorname{ord}_\mathfrak{p} \mathfrak{p}' > 0$. Then, $\mathfrak{p}' \subset \mathfrak{p}$. Since prime ideals of $\mathcal{O}_K$ are maximal, $\mathfrak{p}' = \mathfrak{p}$ which contradicts our assumption that $\mathfrak{p}, \mathfrak{p}'$ are unequal. For part (iii), let $t = \operatorname{ord}_\mathfrak{p} A$ and $s = \operatorname{ord}_\mathfrak{p} A$. By Proposition 3.21, we have $A = \mathfrak{p}^t A_1$, $B = \mathfrak{p}^s B_1$ and $\mathfrak{p} \not\supset A_1$, $\mathfrak{p} \not\supset B_1$. We have $AB = \mathfrak{p}^{s+t} A_1 B_1$, so $\mathfrak{p}^{s+t} \supset AB$ and we will show that $\mathfrak{p}^{s+t+1} \not\supset AB$, proving the proposition. Suppose for contradiction that we do have $\mathfrak{p}^{s+t+1} \not\supset AB$. Then, $AB = \mathfrak{p}^{s+t+1} C$ and hence Proposition 3.20 implies that $\mathfrak{p}C = A_1 B_1$. Therefore $\mathfrak{p} \supset A_1 B_1$ and since $\mathfrak{p}$ is prime it follows that $\mathfrak{p} \supset A_1$ or $\mathfrak{p} \supset B_1$, which gives us a contradiction, as required. □

Theorem 3.25. *Let A be an ideal in $\mathcal{O}_K$. Then, $A = \prod \mathfrak{p}^{a(\mathfrak{p})}$, where the product is over the distinct prime ideals of $\mathcal{O}_K$, and the $a(\mathfrak{p})$ are nonnegative integers of which at most finitely many are nonzero. Moreover, the $a(\mathfrak{p})$ are uniquely determined by $a(\mathfrak{p}) = \operatorname{ord}_\mathfrak{p} A$.*

Proof. The first part follows from Proposition 3.22. Suppose $A = \prod \mathfrak{p}^{a(\mathfrak{p})}$ as in the theorem. Suppose $\mathfrak{p}'$ is a prime ideal in $\mathcal{O}_K$ and we apply $\mathrm{ord}_{\mathfrak{p}'}$ to both sides. Then, by Proposition 3.24, $\mathrm{ord}_{\mathfrak{p}'} A = \sum a(\mathfrak{p}) \mathrm{ord}_{\mathfrak{p}'} \mathfrak{p} = a(\mathfrak{p}')$, as desired. □

Now that we have established unique ideal factorisation in $\mathcal{O}_K$, we might wonder how we can explicitly factorise an ideal. The following important result by Kummer and Dedekind gives us the answer for ideals of the form (p), where p is a prime number. Note that the ring considered in the following theorem is not necessarily the ring of integers, but a ring of the form $\mathbb{Z}[\alpha]$, where $\alpha \in \mathbb{C}$ is an algebraic integer. Such a ring is the ring of integers precisely when all prime ideals in there are *invertible*, see [19, chapter 3]. An ideal A is invertible if there exists an ideal B such that AB is a nonzero principal ideal. It is *singular* if it is not invertible.

Theorem 3.26. *Let $\alpha \in \mathbb{C}$ be a root of a monic irreducible polynomial $f \in \mathbb{Z}[x]$, and let p be a prime number. Let the ring $R = \mathbb{Z}[\alpha] = \mathbb{Z}[x]/(f)$, and let $g_i \in \mathbb{Z}[x]$ be monic polynomials such that the factorisation of f modulo p is $\overline{f} = \prod_{i=1}^{s} \overline{g}_i^{e_i}$ in $\mathbb{F}_p[x]$. Here, the e_i are positive integers and the irreducible $\overline{g}_i$ are pairwise distinct. Then,*

(i) The prime ideals of R that lie above p (that is, that divide (p)) are $\mathfrak{p}_i = pR + g_i(\alpha)R$.

(ii) $pR = \prod \mathfrak{p}_i^{e_i}$ if and only if every $\mathfrak{p}_i$ is invertible.

(iii) If $r_i \in \mathbb{Z}[x]$ is the remainder of f upon division by g_i, then $\mathfrak{p}_i$ is nonsingular if and only if $e_i > 1$ and $p^2 | r_i$.

We will use this theorem to compute prime ideals above certain primes in section 6.3.

3.4 Ramification and degree

For a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, the ideal $\mathfrak{p} \cap \mathbb{Z}$ is nonzero by Lemma 3.11. Since this is a prime ideal of $\mathbb{Z}$, it is generated by a prime number p. We define the numbers e and f as follows.

Definition 3.27. The *ramification index* e of a prime ideal $\mathfrak{p}$ is defined to $e = \mathrm{ord}_{\mathfrak{p}}(p)$. Since $\mathcal{O}_K/\mathfrak{p}$ is a finite field containing $\mathbb{F}_p$, the number of elements of $\mathcal{O}_K/\mathfrak{p}$ is p^f for some positive integer f. We define the *residue class degree* of $\mathfrak{p}$ to be this number f.

Let p be a prime number and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ be the prime ideals dividing (p). If e_i, f_i are the ramification index and residue class degree of $\mathfrak{p}_i$, respectively, then we have $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$. We will show that there is a beautiful relation between the numbers e_i, f_i and $n = [K : \mathbb{Q}]$, namely $\sum_{i=1}^{g} e_i f_i = n$. First, we need the following result.

Lemma 3.28. *Let P be a prime ideal in $\mathcal{O}_K$ and let p^f be the number of elements of $\mathcal{O}_K/P$. Then, the number of elements in $\mathcal{O}_K/P^e$ is p^{ef}.*

Proof. See proposition 12.3.2 in [13]. □

Theorem 3.29. *With notations as before, the following relation between e_i, f_i and $n = [K : \mathbb{Q}]$ holds:*

$$\sum_{i=1}^{g} e_i f_i = n.$$

Proof. If we write $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ as before, then it follows from Proposition 3.24 that $\mathfrak{p}_i^{e_i} + \mathfrak{p}_j^{e_j} = \mathcal{O}_K$ for $i \neq j$. By the Chinese Remainder Theorem,

$$\mathcal{O}_K/(p) \cong \mathcal{O}_K/\mathfrak{p}_1^{e_1} \oplus \cdots \oplus \mathcal{O}_K/\mathfrak{p}_g^{e_g}.$$

In the proof of Proposition 3.12, we have seen that $\mathcal{O}_K/(p)$ contains p^n elements. Therefore, by Lemma 3.28,

$$p^n = p^{e_1 f_1} \cdots p^{e_g f_g},$$

and the result follows. □

3.5 Units

Although the aim of this project is to solve the geometric problem from the introduction by leaving as few black boxes as possible, we will state the following vital result without proof. It is known as the Dirichlet's unit theorem. For a proof, we refer to chapter 5 of [19].

Theorem 3.30. *Let K be a number field with ring of integers $\mathcal{O}_K$. Suppose that K admits r real and $2s$ complex embeddings. Then, the group of units of D is a finitely generated abelian group of rank $r + s - 1$.*

Finding r and s can be done as follows. If $K = \mathbb{Q}(\alpha)$, then the minimal polynomial of α over $\mathbb{Q}$ has r real roots and $2s$ complex roots. In this thesis, we will only need that Theorem 3.30 holds for $r = s = 1$. This is shown in chapter 7 of the bachelor's thesis [22] by Van Timmeren. In the proof he uses Minkowski's theorem, which can be found in chapter 5 of [19]. This theorem asserts the existence of a nonzero lattice point in a certain subset of euclidean space, and Van Timmeren uses this lattice point to construct a $u \in \mathcal{O}_K^\times$ such that any $v \in \mathcal{O}_K^\times$ can be written as $v = \pm u^k$ for some k. This implies that $\mathcal{O}_K^\times \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, as desired.

4 p-adic numbers

In this chapter we will consider the p-adic numbers. They will be very useful in what is to come and considering them will be key to solving the main problem of this thesis. First we will define what they are, then we will give some insight by displaying which p-adics are squares and afterwards we will explain how they are used in the study of hyperelliptic curves. We end the chapter with some theory on extensions of the p-adics, because we will need this later on.

4.1 The field $\mathbb{Q}_p$ and the ring $\mathbb{Z}_p$

As seen in various undergraduate courses, the real numbers $\mathbb{R}$ can be constructed from the rational numbers $\mathbb{Q}$ as follows. Consider the metric on $\mathbb{Q}$ induced by the standard absolute value, that is $d(a,b) = |a-b|$. Then, $\mathbb{R}$ is the ring of Cauchy sequences in $\mathbb{Q}$ modulo the maximal ideal of sequences converging to 0. For an arbitrary field k with an *absolute value* we can do the same procedure and the result is the *completion* of k with respect to the absolute value. It is shown in, for example, a first course in metric spaces that this yields a complete metric space containing k as a dense subset. In this way, we will construct the p-adic numbers as the completion of $\mathbb{Q}$ with respect to some absolute value. To this end, we first define the notion *absolute value* more generally and then present the so-called *p-adic absolute value* with which we will do the construction.

Definition 4.1. Let k be a field. An *absolute value* on k is a map $|\cdot| : k \to \mathbb{R}_{\geq 0}$, such that for all $a, b \in k$ the following hold:

(i) $|a| = 0 \Leftrightarrow a = 0$ (positive-definiteness)

(ii) $|ab| = |a| \cdot |b|$ (multiplicativity)

(iii) $|a+b| \leq |a| + |b|$ (triangle inequality)

Example 4.2. Clearly, the standard absolute value on $\mathbb{Q}$ is an absolute value in the sense of the definition above.

Example 4.3. Let p be a prime number. We can write $a \in \mathbb{Q}$ uniquely as $a = \frac{r}{s}\, p^n$ for some $r, s, n \in \mathbb{Z}$ with $p \nmid rs$. We define the *p-adic valuation* v_p by $v_p(a) = n$. It is readily verified that the map $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ defined by

$$|a|_p = \begin{cases} 0 & \text{if } a = 0, \\ p^{-v_p(r)} & \text{if } a \neq 0 \end{cases}$$

is an absolute value. It is called the *p-adic absolute value*. In particular, it satisfies a stronger version of the triangle inequality, given by

$$|a+b| \leq \max\{|a|, |b|\}.$$

Absolute values satisfying this *ultrametric triangle inequality* are called *non-archimedean*.

Remark. In some sense, Examples 4.2 and 4.3 give all possible absolute values on $\mathbb{Q}$. More precisely, two absolute values $|\cdot|_1, |\cdot|_2$ on a field k are said to be *equivalent* if there exists $\alpha > 0$ such that $|x|_2 = |x|_1^\alpha$ for all $x \in k$. It is the content of Ostrowski's Theorem that every nontrivial absolute value on $\mathbb{Q}$ is equivalent to either the standard absolute value or the p-adic absolute value for some prime number p. For a proof of this theorem, see section 2.2 in [3].

Now we move on to the definition of the p-adic numbers, as anticipated at the start of this section.

Definition 4.4. The field $\mathbb{Q}_p$ of *p-adic numbers* is the completion of $\mathbb{Q}$ with respect to the *p-adic absolute value*. The ring $\mathbb{Z}_p$ of *p-adic integers* is the topological closure[5] of $\mathbb{Z}$ in $\mathbb{Q}_p$.

Remark. By extending v_p and $|\cdot|_p$ to $\mathbb{Q}_p$, we could have also defined the ring $\mathbb{Z}_p$ as the elements of $\mathbb{Q}_p$ with nonnegative valuation (or absolute value at most one). Usually, this is how we think of $\mathbb{Z}_p$ in practice.

Ever since we have learned how to count, we have used the decimal expansion of numbers. A number such as 1998 is understood to mean $8 \cdot 10^0 + 9 \cdot 10^1 + 9 \cdot 10^2 + 1 \cdot 10^3$. Instead of 10, we can of course use any positive integer; the choice of 2, for example, yields the binary expansion of a number. For a prime p, then, we can write any $x \in \mathbb{Z}$ as $x = \sum_{n=0}^{N} a_n p^n$ for some N and where the $a_n \in \{0, 1, \ldots, p-1\}$. Truncation of this sum after $n-1$ terms gives the residue class $x \bmod p^n$. The p-adic integers $\mathbb{Z}_p$ can, in some sense, be reduced $\bmod p^n$ for all n and they can be written in the form $\sum_{n=0}^{\infty} a_n p^n$, where the $a_n \in \{0, 1, \ldots, p-1\}$. Elements of $\mathbb{Q}_p$ also have such a 'series expansion', but they also allow negative exponents, that is, an element of $\mathbb{Q}_p$ can be written as $\sum_{n=-k}^{\infty} a_n p^n$ for some $k \geq 0$. This is made more precise in Theorem 3.4 of [9]. If we write an $a \in \mathbb{Z}_p$ as $\sum_{n=0}^{\infty} a_n p^n$, then sending $a \mapsto \overline{a}_0 \in \mathbb{F}_p$ gives a homomorphism $\mathbb{Z}_p \to \mathbb{F}_p$, usually denoted by $a \mapsto \overline{a}$. Its kernel is $p\mathbb{Z}_p$, so we find that $\mathbb{Z}_p / p\mathbb{Z}_p \cong \mathbb{F}_p$. In the next section we will see Hensel's Lemma, which allows us to answer questions about $\mathbb{Q}_p$ and $\mathbb{Z}_p$ using information from $\mathbb{F}_p$.

4.2 Hensel's Lemma and squares in $\mathbb{Q}_p$

Lemma 4.5. *Let $h \in \mathbb{Z}_p[x]$ be a polynomial and suppose that $a \in \mathbb{F}_p$ is such that a is a simple root of $\overline{h} \in \mathbb{F}_p[x]$, where $\overline{h}$ is obtained by reducing the coefficients modulo p. Then, h has a unique root $\alpha \in \mathbb{Z}_p$ with $\overline{\alpha} = a$.*

Proof. The strategy for this proof resembles Newton's method, and can be found under theorem 3.8 in [21]. □

As an application of Hensel's Lemma, we find the squares in $\mathbb{Q}_p$ for primes the odd primes.

Corollary 4.6. *Let $p > 2$ be prime and let $\alpha = p^n u \in \mathbb{Q}_p$, where $u \in \mathbb{Z}_p^\times$. Then, α is a square in $\mathbb{Q}_p$ if and only if n is even and $\overline{u}$ is a square in $\mathbb{F}_p$.*

Note that in the result above it is implicitly claimed that any $\alpha \in \mathbb{Q}_p$ can be written as $p^n u$, where $n \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$. This follows from writing $\alpha = \sum_{i=-k}^{\infty} a_i p^i$, see the previous section, and observing that there is precisely one $m \in \mathbb{Z}$ such that $p^m \alpha = \sum_{j=0}^{\infty} a_j p^j$ with $a_0 \neq 0$. That is, such that $p^m \alpha$ is a unit. For $n = -m$ we thus have $\alpha = p^n u$ for some unit u. More generally, an element π which takes the role of p is this discussion is called a *uniformiser*; we come back to this in the section 4.4.

[5] Where the topology is induced by the metric $d(x, y) = |x - y|_p$.

Proof. Suppose that α as above is a square. Then, there exists $\beta = p^m v \in \mathbb{Q}_p$, with $v \in \mathbb{Z}_p^\times$, such that $\beta^2 = \alpha$. It follows that $n = 2m$, so n is even. Moreover, $\overline{u} = \overline{v}^2$, so $\overline{u}$ is a square in $\mathbb{F}_p$. Conversely, if $\alpha = p^n u$ as above is such that n is even and $\overline{u}$ is a square in $\mathbb{F}_p$, then clearly p^n is a square, so it suffices to show that u is a square. Consider the polynomial h defined by $h(x) = x^2 - u$. By assumption, $\overline{h}$ has a root. The root is simple, because $p > 2$ and hence $\pm\overline{u}$ are distinct. Therefore, Hensel's Lemma implies that h has a root in $\mathbb{Z}_p$, meaning that u is a square. □

For the prime $p = 2$ the condition is that n is even and that $u \equiv 1 \mod 8$. This is proved, for instance, in section 4 of the notes by Keith Conrad [7], using a stronger version of Hensel's lemma. We will see this result later as a corollary of an algorithm by Stoll, see section 3 of [20].

4.3 Applications to (hyper)elliptic curves

Definition 4.7. Let $C : y^2 = F(x, z)$ be a (hyper)elliptic curve over $\mathbb{Q}_p$ such that F has coefficients in $\mathbb{Z}_p$. Then, by reducing the coefficients modulo p we obtain a homogeneous polynomial $\overline{F} \in \mathbb{F}_p[x, z]$. If $\overline{F}$ is squarefree, then we say that C has *good reduction*. If C is defined over $\mathbb{Q}$, then we say that C has *good reduction at p* if it has good reduction as a curve over $\mathbb{Q}_p$. Otherwise, C is said to have *bad reduction at p*.

Having good reduction at p is equivalent to p not dividing the discriminant of the polynomial F (since p dividing the discriminant means that $\overline{F}$ has discriminant zero and is hence not squarefree). An important consequence of having good reduction is the following.

Theorem 4.8. *Let E be an elliptic curve over $\mathbb{Q}$. If E has good reduction at a prime p, then the reduction map $E(\mathbb{Q}) \to E(\mathbb{F}_p)$ restricts to an injective group homomorphism on $E(\mathbb{Q})_{\text{tors}}$.*

Proof. The proof can be found above theorem 4.4 in [18]. □

In other words, if E has good reduction at a prime p, then we can embed the torsion subgroup of $E(\mathbb{Q})$ into $E(\mathbb{F}_p)$. The latter is easy to find, because we only need to check p^2 pairs $(x, y) \in \mathbb{F}_p^2$. This will be very useful to us in section 6.2, where we find the torsion subgroup in a concrete example.

4.4 Extensions of $\mathbb{Q}_p$

In the solution presented in chapter 6, we also consider extensions L_p of $\mathbb{Q}_p$. In particular, we will encounter *totally ramified extensions*. In the language of Definition 3.27, this means[6], $e = [L_p : \mathbb{Q}_p]$ and $f = 1$. A *uniformiser* for L_p is an element $\pi \in L_p$ such that any other $\alpha \in L_p$ can be written as $\alpha = \pi^n u$, where n is an integer and u is a unit in the ring of integers of L_p, see section 2.2 of [8]. If $\alpha = \pi^n u$ as above, then a *normalised valuation* v_{L_p} is given by $v_{L_p}(\alpha) = n$. For the trivial extension $\mathbb{Q}_p/\mathbb{Q}_p$, we thus have that p is a uniformiser and $v_{\mathbb{Q}_p}$ is the standard p-adic valuation from section 4.1. The following proposition is based on proposition 12.1 from the lecture notes by Dokchitser [8]. We will apply it in section 6.4.

[6]Where we assume that the theory from chapter 3 on the extension $K/\mathbb{Q}$ can also be developed for extensions of p-adic fields. This is true, see chapters 9 and 10 of [8].

Proposition 4.9. *Suppose that $L_p/\mathbb{Q}_p$ is totally ramified of degree e, that π is a uniformiser for L_p and that v_{L_p} is a normalised valuation. Then,*

(i) π satisfies an Eisenstein polynomial of degree e over $\mathbb{Z}_p$.

(ii) $\mathcal{O}_{L_p} = \mathbb{Z}_p[\pi]$.

Conversely, if $g \in \mathbb{Z}_p[x]$ is Eisenstein, then $L_p = \mathbb{Q}_p[x]/(g)$ is totally ramified over $\mathbb{Q}_p$ and if $g(a) = 0$ then a is a uniformiser for L_p with $v_{L_p}(a) = 1$.

Proof. The proof of (a slight generalisation of) this proposition can be found under proposition 12.1 in [8]. □

In the next chapter we will see that for an extension L_p of $\mathbb{Q}_p$ we would like to understand the group $L_p^\times/(L_p^\times)^2$. Suppose $L_p = \mathbb{Q}_p[x]/(f)$ for some polynomial $f \in \mathbb{Q}_p[x]$. Then, if f splits as $f = f_1 \cdots f_m$ in $\mathbb{Q}_p[x]$, where the f_i are irreducible, and if $L_{p,i}$ denotes $\mathbb{Q}_p[x]/f_i$, we have

$$L_p^\times/(L_p^\times)^2 \cong \prod_{i=1}^{m} L_{p,i}^\times/(L_{p,i}^\times)^2.$$

These groups are briefly explained in section 3 of an article by Stoll [20]. For odd p this situation is relatively straightforward. In this case, each $L_{p,i}^\times/(L_{p,i}^\times)^2$ is a two-dimensional $\mathbb{F}_2$-vector space V. The image of $\alpha \in L_{p,i}^\times$ in V is obtained by writing $\alpha = \pi^n u$ for some uniformiser π and unit u. The first coordinate of its image in V is determined by the parity of n, and the second by whether u is a square in the residue field, cf. Corollary 4.6. For $p = \infty$, it depends on whether $L_{\infty,i}$ is real or complex. If it is complex, then $L_{\infty,i}^\times/(L_{\infty,i}^\times)^2$ is trivial; if $L_{\infty,i}$ is real, then $L_{\infty,i}^\times/(L_{\infty,i}^\times)^2$ is a one-dimensional $\mathbb{F}_2$-vector space and the image of $\alpha \in L_{\infty,i}^\times$ in it is determined by the sign. For $p = 2$ it is more complicated. Suppose K is an extension of $\mathbb{Q}_2$. Then, as a vector space V over $\mathbb{F}_2$, $K^\times/(K^\times)^2$ has dimension $d = [K : \mathbb{Q}_2] + 2$. We identify V with $\mathbb{F}_2^d$. The following algorithm by Stoll, presented in section 3 of [20], gives us the image of $\alpha \in K^\times$ in $\mathbb{F}_2$ under this identification. Here, π is a uniformiser in K, v is a normalised valuation, e_k, f_k are as before, k is the residue field, $B \subset \mathcal{O}_K^\times$ is a lifting of an $\mathbb{F}_2$-basis for k.

```
Input:  α ∈ K^×
Output:  s ∈ V = F_2^d, where d = [K : Q_2] + 2

mod_squares_2(α, K) :
  va := v(α); s[1] := va mod 2; i := 2;
  u := α/π^va mod 4π  (∈ O/4πO); u := u^(2^(f_K) − 1);
  for j := 1 to e_K :
    // Here, u ≡ 1 mod π^(2j−1)
    r := (u − 1)/π^(2j−1) mod π  (∈ k);
    for h := 1 to f_K :
      s[i] := coefficient(r, h); i := i+1;
      if coefficient(r, h) ≠ 0 then
        u := u (1 + B[h] π^(2j−1));
    // Here, u ≡ 1 mod π^(2j)
    if j < e_K then
      r := (u − 1)/π^(2j) mod π  (∈ k); r := √r  (∈ k);
      R := Σ_{h=1}^{f_K} coefficient(r,h) B[h] mod π^(2e_K+1−2j);
      u := u (1 + R π^j)^2;
    else
      r := (u − 1)/4 mod π  (∈ k);
      s[i] := trace_{k/F_2}(r);
  return s.
```

Figure 3: Stoll's algorithm, taken from section 3 of [20]

We now give two small applications of the algorithm to explain how it works. In order to keep things simple we consider the trivial extension $K = \mathbb{Q}_2$ of $\mathbb{Q}_2$ (so $\mathcal{O}_K = \mathbb{Z}_p$, $\pi = 2$, $e_K = f_K = 1$). For a more involved example, see Proposition 6.8.

Corollary 4.10. *The group $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ is generated by the images of $2, 3$ and -1.*

Proof. As seen in the discussion above, we can regard $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ as a three-dimensional vector space V over $\mathbb{F}_2$. Therefore, it suffices to show that the images of $2, 3$ and -1 are linearly independent, given the identification of V with $\mathbb{F}_2^3$ implied by the algorithm. We first input 2 into the algorithm. Since 2 is the uniformiser in this case, the first step of the algorithm gives $s[1] = 1$ and $u = 1$. Applying the other steps to $u = 1$ quickly yields $s[2] = s[3] = 0$, so the image of 2 in $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ is identified with the vector $(1, 0, 0)$. Now we take 3 as input. Since 2 and 3 are coprime, $s[1] = 0$. Before starting the second step for $u = 3$, we see that indeed $u = 3 \equiv 1 \mod 2^{2\cdot 1-1}$. The second step yields $s[2] = 1$ and hence we redefine u as $u = 3(1 + 2) = 9$ and we see indeed that $u = 9 \equiv 1 \mod 2^2$. The final step yields $s[3] = 0$. Finally, for an input of -1 we also see that $s[1] = 0$ and $s[2] = 1$. However, now we redefine u as $u = -1(1 + 2) = -3$. Then the final step yields $s[3] = 1$. Since $(1, 0, 0), (0, 1, 0), (0, 1, 1)$ are linearly independent, the desired statement follows. □

Corollary 4.11. *Let $\alpha = 2^n u \in \mathbb{Q}_2$, where $u \in \mathbb{Z}_2^\times$. Then, α is a square in $\mathbb{Q}_2$ if and only if n is even and $u \equiv 1 \mod 8$.*

Proof. The part concerning the parity of n is clear, cf. the proof of Corollary 4.6. It suffices to show that $u \in \mathbb{Z}_2^\times$ is a square if and only if $u \equiv 1 \mod 8$. We apply the algorithm with $K = \mathbb{Q}_2$. Being a square is equivalent to getting $(0, 0, 0)$ as output upon inputting u in the algorithm. We have $s[1] = 0$, because u is a unit. From the algorithm, we further observe that $s[2] = 0$ and $s[3] = 0$ if and only if $(u - 1)/4 \mod 2 \equiv 0$, which is equivalent to $u \equiv 1 \mod 8$. □

5 The 2-Selmer group

In chapter 2 we have seen Mordell's theorem, stating that the group of rational points on an elliptic curve is a finitely generated abelian group. This is usually proved in two parts: the first part, known as the Weak Mordell theorem, states that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. The second part involves applying the theory of *heights* to the generators of $E(\mathbb{Q})/2E(\mathbb{Q})$ to show that $E(\mathbb{Q})$ is finitely generated. Many introductory texts on elliptic curve such as [13],[18] and [4], contain the proof of Mordell's theorem. These texts were studied by the author and were very useful in getting an intuitive idea of how the theorem is proved. In particular, the proof of the Weak Mordell theorem turned out be important in solving the central problem of this thesis. The introductory texts mentioned before helped reduce the problem to a big computational one, potentially requiring very clever substitutions, which the author was unable to carry out by hand, see for instance the second example in chapter 15 of the book by Cassels [4]. A rather more general perspective, as presented in Stoll's lecture notes [21], which concerned Jacobians of hyperelliptic curves, helped the author understand the underlying theory a bit better, which eventually lead to the solution of the central problem of this thesis. This section will therefore include a proof of the Weak Mordell theorem, but from a more general point of view than in most introductory texts on elliptic curves. The theory will be developed as in [21], but simplified to elliptic curves. Particularly in the first section the proofs are specifically for elliptic curves. The proofs in the first section will mostly follow [13].

Our goal will be to embed $E(\mathbb{Q})/2E(\mathbb{Q})$ into a finite group which we can compute, the so-called *2-Selmer group*. In particular, this will prove the Weak Mordell theorem, but it also gives a bound on the size of $E(\mathbb{Q})/2E(\mathbb{Q})$. In some cases, it will even allow us to find $E(\mathbb{Q})/2E(\mathbb{Q})$ explicitly. For instance, in chapter 6 we will show that that for some elliptic curve the 2-Selmer group is trivial, in which case it follows that $E(\mathbb{Q})/2E(\mathbb{Q})$ is trivial as well. In order to define this finite and computable 2-Selmer group, we first define a homomorphism δ from $E(\mathbb{Q})$ to some group G, and show that δ has kernel $2E(\mathbb{Q})$, showing that $E(\mathbb{Q})/2E(\mathbb{Q}) \cong \operatorname{im}\delta$. We will then cut down the group G until we are left with a finite and computable subgroup of G, which contains $\operatorname{im}\delta$, and that subgroup will be called the 2-Selmer group.

5.1 The map δ

In this section, $E: y^2 = f(x)$ will be an elliptic curve in Wierstrass form, so f is monic cubic polynomial without repeated roots. As announced at the start of chapter 3, we will have to consider the ring defined by $A = \mathbb{Q}[x]/(f)$. Let θ be the image of x in A, so that $A = \mathbb{Q}[\theta]$. If $f = f_1 \cdots f_n$ is a product of monic irreducibles, then the f_i are distinct because E is an elliptic curve. By the Chinese remainder theorem,

$$A \cong \bigoplus_{i=1}^{n} \mathbb{Q}[x]/(f_i).$$

In our case, n is either $1, 2$ or 3 depending on whether f is irreducible, a product of a linear and an irreducible quadratic polynomial or product of three linear polynomials over $\mathbb{Q}$, respectively. We now define a map $\delta: \ E(\mathbb{Q}) \to A^\times/(A^\times)^2$. First of all, we let $\delta(\infty) = 1\ (A^\times)^2$. If $P = (\xi, \eta) \in E(\mathbb{Q})$ is not a point of order 2, so $\eta \neq 0$, then we define $\delta(P) = (\xi - \theta)\ (A^\times)^2$.

Finally, if $P = (\xi, 0) \in E(\mathbb{Q})$ is a point of order two, then we write $f(x) = (x - \xi)g(x)$, where g is not necessarily irreducible. We have

$$A \cong \mathbb{Q}[x]/(x - \xi) \oplus \mathbb{Q}[x]/(g) \cong \mathbb{Q} \oplus \mathbb{Q}[x]/(g), \tag{3}$$

where the isomorphism $\mathbb{Q}[x]/(x - \xi) \cong \mathbb{Q}$ is given by $\theta \mapsto \xi$. Since f has no double roots, $(f'(\xi), (x - \xi) \mod g) \in \mathbb{Q} \oplus \mathbb{Q}[x]/(g)$ is a unit. It corresponds to some $h(\theta) \in A$. We then define $\delta(P) = h(\theta)\ (A^\times)^2$. Sometimes we denote an element of $A^\times/(A^\times)^2$ simply by a representative in $A^\times$. In these cases it is understood that we mean the image of the element under the canonical homomorphism to $A^\times/(A^\times)^2$.

Lemma 5.1. *The map $\delta :\ E(\mathbb{Q}) \to A^\times/(A^\times)^2$ is a homomorphism.*

Proof. We have to show that for $P, Q \in E(\mathbb{Q})$, it holds that $\delta(P + Q) = \delta(P)\delta(Q)$. For any $P = (\xi, \eta) \in E(\mathbb{Q})$, the map δ defined above is independent of η, so $\delta(P) = \delta(-P)$. Since we are working modulo squares, $\delta(P + Q) = \delta(P)\delta(Q)$ is equivalent to

$$\delta(P + Q)\delta(-P)\delta(-Q) = \delta(P + Q)\delta(P)\delta(Q) = \delta(P + Q)^2 = 1$$

in $A^\times/(A^\times)^2$. That is, to show that δ is a homomorphism it suffices to show that $P+Q+R = \infty$ in $E(\mathbb{Q})$ implies

$$\delta(P)\delta(Q)\delta(R) = 1 \tag{4}$$

in $A^\times/(A^\times)^2$. By the geometric group law on elliptic curves, $P+Q+R = \infty$ means that P, Q, R are colinear. Let $P = (\xi_1, \eta_1)$, $Q = (\xi_2, \eta_2)$ and $R = (\xi_3, \eta_3)$ be distinct points on E. If $\xi_1 = \xi_2$, then these points are $P, -P$ and ∞ and the result follows from $\delta(P) = \delta(-P)$. Now, suppose that $\xi_1 \neq \xi_2$ and that P, Q, R do not have order 2. Then, P, Q, R lie on a line $y = lx + m$ as well as on $y^2 = f(x)$. Therefore,

$$f(x) - (lx + m)^2 = (x - \xi_1)(x - \xi_2)(x - \xi_3) \tag{5}$$

and hence

$$\delta(P)\delta(Q)\delta(R) = (\xi_1 - \theta)(\xi_2 - \theta)(\xi_3 - \theta) = (l\theta + m)^2 - f(\theta) = 1 \tag{6}$$

in $A^\times/(A^\times)^2$, as desired. Now suppose that exactly one of the points has order 2. Without loss of generality assume that $P = (\xi_1, 0)$. As in (3), we write $A \cong \mathbb{Q} \oplus \mathbb{Q}[x]/(g)$ and we check 4 in each component separately. It holds in the second component, because $g|f$ and hence the result follows as in (6). As for the first component, it follows from (5) that $f'(\xi_1) = (\xi_1 - \xi_2)(\xi_1 - \xi_3)$. Therefore, the first component of $\delta(P)\delta(Q)\delta(R)$ reads

$$f'(\xi_1)(\xi_1 - \xi_2)(\xi_1 - \xi_3) = f'(\xi_1)^2,$$

as required. Finally, suppose that $P = (\xi_1, 0)$, $Q = (\xi_2, 0)$ and $R = (\xi_3, 0)$. Similar to the previous, we find that, under the canonical identification $A \cong \mathbb{Q}^3$, the three components of $\delta(P)\delta(Q)\delta(R)$ are $f'(\xi_1)^2$, $f'(\xi_2)^2$ and $f'(\xi_3)^2$. □

Lemma 5.2. *The homomorphism $\delta :\ E(\mathbb{Q}) \to A^\times/(A^\times)^2$ has kernel $2E(\mathbb{Q})$.*

Proof. The inclusion $2E(\mathbb{Q}) \subset \ker \delta$ is easy, since $\delta(2P) = \delta(P)^2 = 1$ in $A^\times/(A^\times)^2$. We will prove $\ker \delta \subset 2E(\mathbb{Q})$. We have $\infty \in \ker \delta$ and $\infty = 2\infty \in 2E(\mathbb{Q})$, so we only have to consider points in the kernel different from ∞. Let $P = (\xi, \eta) \in \ker \delta$ be different from ∞. Then, $\xi - \theta$ is a square in $A = \mathbb{Q}[\theta]$, so

$$\xi - \theta = (c_2\theta^2 + c_1\theta + c_0)^2 \tag{7}$$

for some $c_i \in \mathbb{Q}$. Note that E is defined in Weierstrass form ($y^2 = x^3 + ax + b =: f(x)$), so we can write

$$d_1\theta + d_0 = (c_2\theta^2 + c_1\theta + c_0)(-c_2\theta + c_1) \tag{8}$$

for some $d_1, d_0 \in \mathbb{Q}$. Since $1, \theta, \theta^2$ are linearly independent, we see from (7) that $c_2 \neq 0$. Therefore, by squaring (8) and substituting (7), we get

$$(d\theta + d')^2 = (\xi - \theta)(e - \theta)^2$$

for some $d, d', e \in \mathbb{Q}$. Therefore, $(dx + d')^2 - (\xi - x)(e - x)^2$ is a multiple of $f(x)$. Since both polynomials are monic, we even have

$$f(x) = (dx + d')^2 - (\xi - x)(e - x)^2.$$

This means that the line $y = dx + d'$ intersects E at either $(\xi, \pm\eta)$ and it intersects $Q = (e, e')$ twice, where $e' = \pm(de + d')$. By the geometric group law on E, we have

$$\pm P + 2Q = \infty,$$

which implies that $P \in 2E(\mathbb{Q})$. □

5.2 The group H

As announced in the introduction of this chapter, our course of action is to cut down the group $A^\times/(A^\times)^2$ until we are left with a finite and computable subgroup which contains the image of δ. In this section we perform the first step in this process: we show that the image of δ is contained in a certain group H which, roughly speaking, is already much smaller than $A^\times/(A^\times)^2$. It is the kernel of the norm map defined in section 3.1. Note that Definition 3.1 still makes sense for a product of field extensions over $\mathbb{Q}$ (or over another field k). The proof of the following lemma is a specialised version of the proof of lemma 5.6 in [21] and uses some insight from section 1.0 in [2].

Lemma 5.3. *Let $E: y^2 = x^3 + ax + b =: f(x)$ be an elliptic curve in Weierstrass form over a field k of characteristic zero. Define $A = k[x]/(f)$ and $\delta : E(k) \to A^\times/(A^\times)^2$ as before.*[7] *Then, the image of δ is contained in the kernel of $N: A^\times/(A^\times)^2 \to k^\times/(k^\times)^2$.*

Proof. We will show that for any $P \in E(\mathbb{Q})$, the norm of $\delta(P)$ is a square in k. For $P = \infty$ this is clear. Now assume that $P = (\xi, \eta)$ is not of order 2. We have $(\xi - \theta) \cdot 1 = \xi - \theta$, $(\xi - \theta) \cdot \theta = \xi\theta - \theta^2$ and $(\xi - \theta) \cdot \theta^2 = \xi\theta^2 - \theta^3 = b + a\theta + \xi\theta^2$, so

[7] Technically, we should justify why, over any field k, the map δ as defined earlier is still a homomorphism. This is true, and in the proofs from the previous section we may replace $\mathbb{Q}$ with any field k of characteristic zero and they still work. Since we will later set $k = \mathbb{Q}$ and $k = \mathbb{Q}_p$, this is enough for us.

$$N(\delta(P)) = N(\xi - \theta) = \det \begin{pmatrix} \xi & 0 & b \\ -1 & \xi & a \\ 0 & -1 & \xi \end{pmatrix} = f(\xi) = \eta^2. \tag{9}$$

If $P = (\xi, 0)$ is of order 2, then we write $f(x) = (x - \xi)g(x)$ and identify $A = \mathbb{Q} \oplus \mathbb{Q}[x]/(g)$ in the natural way, cf. (3). We defined $\delta(P)$ to be the image in $A^\times/(A^\times)^2$ of the element of A corresponding to $(f'(\xi), (\xi - x) \mod g)$. The norm of $\xi - \theta$ from $\mathbb{Q}[x]/(g)$ is $g(\xi)$, as in (9). Since $f'(\xi) = g(\xi)$, we see that $N(\delta(P)) = f'(\xi)g(\xi) = g(\xi)^2$. □

In fact, the reason we defined δ this way for points of order 2 is that we want Lemma 5.3 to hold. See for example section 1.0 of the paper by Cassels [2]. We define the group H to be the kernel of $N: A^\times/(A^\times)^2 \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

5.3 The group H'

From here on, we will restrict to the case where E is an elliptic curve over $\mathbb{Q}$ defined by an irreducible cubic polynomial f, such that $A = \mathbb{Q}[x]/(f)$ is a number field with class number 1. We do this because we will deal with such a case in chapter 6. However, the following results also hold more generally. If f splits, then A is a product of number fields and we have to do the following argument in each of the components separately. If the number field does not have class number 1, the argument becomes a bit more involved, but can be fixed due to the finiteness of the class number. Now to the argument. Recall that we were in the process of cutting down $A^\times/(A^\times)^2$ to a finite and computable group containing the image of δ. In the previous section, we did the first step in this process by introducing the group H. We can do even better: define the subgroup U of $A^\times/(A^\times)^2$ by

$$U = \langle \varepsilon_1, \ldots, \varepsilon_r, q_1, \ldots, q_n \rangle,$$

where $\varepsilon_1, \ldots, \varepsilon_r$ generate the unit group of $\mathcal{O}_A$, cf. Theorem 3.30, and $q_1, \ldots, q_n$ are the generators of the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ that lie above the prime numbers dividing the discriminant. Here we use the assumption that A has class number 1. If it did not, we would also need representatives of generators of the class group in the definition of U.

Proposition 5.4. *The image of δ is contained in U.*

In order to prove this proposition we will specialise the argument in section 19.4 of [13] to our specific case. For $P = (\alpha/\beta, \eta) \in E(\mathbb{Q})$, where $\gcd(\alpha, \beta) = 1$, we define a principal ideal (γ_P) as follows. Write $A = \mathbb{Q}[\theta]$ as before, so that $f(x) = (x - \theta)g(x)$ for some quadratic polynomial g. Then, $\alpha - \beta\theta, g(\alpha/\beta)\beta^2 \in \mathcal{O}_A$. Since we have assumed that A has class number 1, the ideal $(\alpha - \beta\theta, g(\alpha/\beta)\beta^2)$ can be generated by one element, which we call γ_P.

Lemma 5.5. *An ideal of the form γ_P lies above a prime dividing the discriminant.*

Proof. The quadratic polynomial $g(x) - g(\theta)$ has θ as a root, so $g(x) - g(\theta) = (x - \theta)t(x)$ for some linear polynomial $t \in \mathbb{Z}[\theta][x]$. Substituting $x = \alpha/\beta$ gives $g(\alpha/\beta) - g(\theta) = (\alpha/\beta - \theta)t(\alpha/\beta)$; hence, $g(\theta)\beta^2 = g(\alpha/\beta)\beta^2 - (\alpha - \beta\theta)t(\alpha/\beta)\beta$. Therefore, $g(\theta)\beta^2 \in (\gamma_P)$. Similarly, see page lemma 1 on page 328 of [13] for details, $g(\theta)\alpha^2 \in (\gamma_P)$. We conclude that (γ_P) divides the

ideal $(g(\theta)\alpha^2, g(\theta)\beta^2)$ and since α, β are coprime, (γ_P) divides the ideal $(g(\theta))$. Therefore, modulo γ_P, θ is a double root of f, meaning that the ideal (γ_P) lies above a prime dividing the discriminant. □

It is easy to see that β must be a square if $P \in E(\mathbb{Q})$, see for instance page 328 in [13]. On the same page, it is also shown that this implies that the ideal $(\alpha - \beta\gamma) = (\gamma_P)C^2$ for some ideal C. We use this in our proof that $\delta(P) \in U$.

Proof. Since the class number of A is assumed to be 1, there exist $\sigma, \tau \in \mathcal{O}_A$ such that $\sigma C = (\tau)$, where C is as in the lemma above. Then, $(\sigma^2(\alpha - \beta\theta)) = (\gamma_P)\sigma^2 C^2 = (\gamma_P \tau^2)$. We find that the element $\sigma^2(\alpha - \beta\theta) = u\gamma_P\tau^2$ for some unit u. As mentioned before, the integer β is a square, so by the lemma

$$\delta(P) = \left(\frac{\alpha}{\beta} - \theta\right) \ (A^\times)^2 = u\gamma_P \frac{\tau^2}{\beta\sigma^2} \ (A^\times)^2 = u\gamma_P \ (A^\times)^2 \in U,$$

as required. □

If we recall that we work modulo squares, it is clear that the group U is finite. This already implies the Weak Mordell theorem, because Lemma 5.2 and the first isomorphism theorem from group theory imply that

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong \delta(E(\mathbb{Q})) \subset U.$$

Hence $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

By Proposition 5.4 above, we can cut down H further by defining the group $H' = H \cap U$, which still contains the image of δ. In the next section, we will cut down H' to the so-called *2-Selmer group*. The main advantages of this group are that it gives a rather tight upper bound on the size of $E(\mathbb{Q})/2E(\mathbb{Q})$ (which is apparent from the amount of cutting down we will have done) and there is a finite procedure which guarantees that we can compute the 2-Selmer group.

5.4 The group $\mathrm{Sel}^{(2)}(E)$

Let $E: \ y^2 = f(x)$ be an elliptic curve over $\mathbb{Q}$. For a prime p we define $A_p = \mathbb{Q}_p[x]/(f)$ and H_p as the corresponding kernel of $N: \ A_p^\times/(A_p^\times)^2 \to \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$. This also includes $p = \infty$, where we have $\mathbb{Q}_\infty = \mathbb{R}$. The inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ yields a homomorphism $\rho_p: \ H \to H_p$. Let δ_p be the map $E(\mathbb{Q}_p) \to H_p$, that is, the map δ defined for the field $k = \mathbb{Q}_p$. Then, the following diagram commutes.

$$\begin{array}{ccc} E(\mathbb{Q}) & \xrightarrow{\ \delta\ } & H \\ \big\downarrow & & \big\downarrow{\scriptstyle \rho_p} \\ E(\mathbb{Q}_p) & \xrightarrow{\ \delta_p\ } & H_p \end{array}$$

We can now cut down the group H to a finite group which we can always compute, called the 2-Selmer group.

Definition 5.6. With notations as before, we define the *2-Selmer group* of E to be

$$\mathrm{Sel}^{(2)}(E)' = \{\alpha \in H' \mid \forall p : \rho_p(\alpha) \in \operatorname{im} \delta_p\}.$$

Proposition 5.7. *The image of δ is contained in the 2-Selmer group and the 2-Selmer group is finite.*

Proof. From the commutativity of the diagram above it follows that for $P \in E(\mathbb{Q})$, we have $\rho_p(\delta(P)) = \delta_p(P) \in \operatorname{im} \delta_p$. Since we already know that $\delta(P) \in H'$, we find $\delta(P) \in \mathrm{Sel}^{(2)}(E)'$. The finiteness of $\mathrm{Sel}^{(2)}(E)'$ is clear from the finiteness of H'. □

In the remainder of this section, we will state a few facts without proof, because their proofs require rather advanced theory which the author was not able to fully grasp within the given time for this thesis. They are (at least partly) justified in chapter 5 of [21]. First of all, the 2-Selmer group is usually defined as

$$\mathrm{Sel}^{(2)}(E) = \{\alpha \in H \mid \forall p : \rho_p(\alpha) \in \operatorname{im} \delta_p\}.$$

However, it turns out that $\mathrm{Sel}^{(2)}(E) \subset H'$ and hence the two definitions coincide. From now on, we will simply write $\mathrm{Sel}^{(2)}(E)$ for the 2-Selmer group. The main advantage of $\mathrm{Sel}^{(2)}(E)$ as compared to $\delta(E(\mathbb{Q}))$ is that it is always possible to compute it. Namely, for the primes p that do not divide the discriminant, $\alpha \in H'$ already implies that $\rho_p(\alpha) \in \operatorname{im} \delta_p$; hence, there are only finitely many primes p (2, ∞ and the p that do divide the discriminant) for which we must find the $\alpha \in H'$ that satisfy $\rho_p(\alpha) \in \operatorname{im} \delta_p$. The following formula, proved in chapter 5 of [21], allows us to do this.

$$\dim_{\mathbb{F}_2} \delta_p(E(\mathbb{Q}_p)) = \dim_{\mathbb{F}_2} \delta_p(E(\mathbb{Q}_p))[2] + \begin{cases} g & \text{if } p = 2, \\ -g & \text{if } p = \infty, \\ 0 & \text{otherwise.} \end{cases} \tag{10}$$

Namely, we can compute $\dim_{\mathbb{F}_2} \delta_p(E(\mathbb{Q}_p))[2]$ from the factorisation of f, cf. lemma 5.2 in [21], and then we can compute images of randomly chosen points in $E(\mathbb{Q})$ until they generate a subspace of the right dimension. This yields the image of δ_p. We then find the image under ρ_p of H' and see how it intersects the image of δ_p using linear algebra. Doing this for $p = 2, \infty$ and all primes p dividing the discriminant then yields the 2-Selmer group. In these computations, the kernel of ρ_p will also play a role, because clearly $\ker \rho_p \subset \rho_p^{-1}(\operatorname{im} \delta_p)$. The computation of the 2-Selmer group is illustrated in the next section.

5.5 Examples

In this section we will see examples of how the theory can be applied. First, we will do a simple example of an elliptic curve whose defining polynomial splits completely over $\mathbb{Q}$. Afterwards, we will turn our attention to a maybe even more intriguing geometric problem than the one we focus on in this thesis.

Example 5.8. Consider the elliptic curve E defined by

$$E: \quad y^2 = x(x-1)(x+3) =: f(x).$$

We will determine the group $E(\mathbb{Q})$ using the theory we have introduced so far. The primes dividing the discriminant (which is 144) are 2 and 3. Since the defining polynomial splits completely over $\mathbb{Q}$, we have

$$A = \mathbb{Q}[x]/(x) \oplus \mathbb{Q}[x]/(x-1) \oplus \mathbb{Q}[x]/(x+3) \cong \mathbb{Q}^3.$$

We first treat the 2-torsion points. By the definition of δ, we have

$$\begin{aligned}\delta(0,0) &= (f'(0), 0-1, 0+3) = (-3,-1,3)\\ \delta(1,0) &= (1-0, f'(1), 1+3) = (1,4,4) = (1,1,1)\\ \delta(-3,0) &= (-3-0, -3-1, f'(-3)) = (-3,-4,12) = (-3,-1,3)\end{aligned}$$

in $A^\times/(A^\times)^2$. Therefore, $\delta(E(\mathbb{Q})[2])$ in H' is generated by $(-3,-1,3)$. By (10), the image of δ_∞ has dimension 1; we see that it is generated by $(-1,-1,1)$. Using $\pm 1, \pm 3$ as representatives of $\mathbb{Q}_3^\times/(\mathbb{Q}_3^\times)^2$, the image of $E(\mathbb{Q})[2]$ under δ_3 is generated by $(-3,-1,3)$. From (10), we see that $\operatorname{im}\delta_3$ has dimension 2, and hence we need another generator. Since $f(3) = 36$, we have that $P = (3,6) \in E(\mathbb{Q})$. Then, $\delta(P) = (3,2,6)$ and hence $\delta_3(P) = \rho_3(\delta(P)) = (3,-1,-3)$. It follows that $\operatorname{im}\delta$ is mapped onto $\operatorname{im}\delta_3$ under ρ_3. Therefore, any element of $\mathrm{Sel}^{(2)}(E)$ must be of the form $\alpha\beta$, where $\alpha \in \langle(-3,-1,3),(3,2,6)\rangle$ and $\beta \in \ker\rho_3$. Moreover, such an $\alpha\beta \in \mathrm{Sel}^{(2)}(E)$ if and only if $\rho_p(\beta) \in \operatorname{im}\delta_p$ for $p = 2$ and $p = \infty$.

We show that $\mathrm{Sel}^{(2)}(E) \cap \ker\rho_3$ is trivial. To that end, suppose $\beta \in \mathrm{Sel}^{(2)}(E) \cap \ker\rho_3$. Then, $\beta \in H'$ and hence it can be represented by squarefree integers only divisible by the primes 2 and 3, that is, β can be represented by a triple consisting of elements of $\{\pm 1, \pm 2, \pm 3, \pm 6\}$. The fact that $\beta \in \ker\rho_3$ then implies that each of the triple is either 1 or -2. The fact that $\rho_\infty(\beta) \in \operatorname{im}\delta_\infty$ implies that the only possibilities are $(1,1,1)$ and $(-2,-2,1)$. We show that the latter is not possible by showing that its image under ρ_2 is not in the image of δ_2. By (10), $\operatorname{im}\delta_2$ has dimension 3 and by Stoll's algorithm, we can take $\pm 1, \pm 2, \pm 3, \pm 6$ as representatives of $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ (together they cover all outputs in $\mathbb{F}_2^3$). Therefore, two of the generators of $\operatorname{im}\delta_2$ are given by

$$(-3,-1,3) \text{ and } (3,2,6).$$

By trying a bit, we find $(-1,2) \in E(\mathbb{Q})$. Unfortunately, its image under δ_2 does not give a point independent from the ones above. By Corollary 4.11, however, we find that $f(11) = 11 \cdot 10 \cdot 14 = 1540 = (8 \cdot 48 + 1) \cdot 2^2$ is a square in $\mathbb{Q}_2$. Suppose $\eta \in \mathbb{Q}_2$ satisfies $\eta^2 = 1540$, then $(11,\eta) \in E(\mathbb{Q}_2)$. By applying Stolls algorithm, we find that

$$\delta_2(11,\eta) = (11,10,14) = (3,-6,-2)$$

in $A_2^\times/(A_2^\times)^2$. This one is independent from the subspace we found before. Therefore, $\operatorname{im}\delta_2$ is generated by

$$(-3,-1,3),\ (3,2,6) \text{ and } (3,-6,-2).$$

We conclude that $\rho_2(-2,-2,1) = (-2,-2,1) \notin \operatorname{im}\delta_2$ and hence, indeed, that $\mathrm{Sel}^{(2)}(E) \cap \ker\rho_3$ is trivial. Therefore,

$$\mathrm{Sel}^{(2)}(E) = \langle(-3,-1,3),(3,2,6)\rangle$$

is generated by $\delta(E(\mathbb{Q})[2])$ and $\delta(P)$. By the geometric group law, $2P = (1,0)$ and hence $4P = \infty$ and hence P is a torsion point, so $E(\mathbb{Q})$ has rank zero. We find $\#E(\mathbb{F}_5) = 8$ by

checking the 25 options separately. It follows from Theorem 4.8 that $E(\mathbb{Q})$ is generated, for instance, by the element P of order 4 and the element $(-3, 0)$ of order 2. So

$$E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z},$$

and using the geometric group law we can find all the points:

$$E(\mathbb{Q}) = \{\infty, (-3, 0), (-1, \pm 2), (0, 0), (1, 0), (3, \pm 6)\}.$$

Example 5.9. In this example we will consider another problem of the type described in the introduction of this thesis. We ask the question: Up to similarity, how many pairs of a rational right triangle and a rational isosceles triangle exist such that they have a common perimeter and a common area? Remarkably, the answer is 'one'. This was shown earlier this year (2019) by the Japanese mathematicians Hirakawa and Matsumura in their paper [12]. The result even got some media attention here in the Netherlands: Dutch matematics enthusiast Alex van den Brandhof wrote an article about it in the national newspaper NRC Handelsblad [1]. In the honest opinion of the author, this result by Hirakawa and Matsumura is more interesting and beautiful than the one by Zhang and Peng which we consider in this thesis, and for this reason we devote some time to it here. The reason that the 'triangle-triangle problem' is not the central problem of this thesis is that the computations that would be necessary to get a fully explicit solution (as we have set out to do for the triangle-rhombus problem) are much more involved and require a bit more general theory. In the remainder of this section, we will look at how the triangle-triangle problem is solved, without diving into the details.

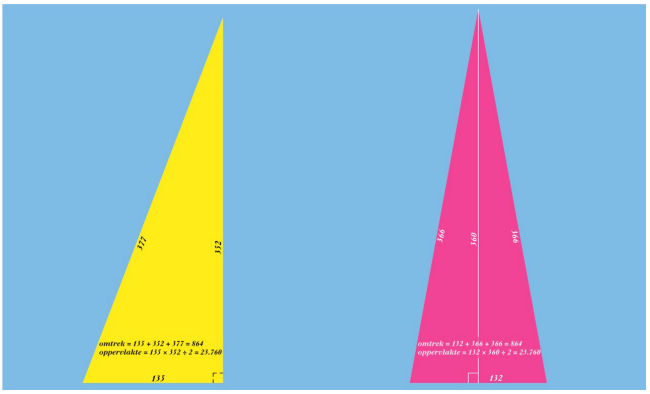

Figure 4: A unique pair of triangles, taken from [1]

In Figure 4 above, we see that there exist a rational right triangle and a rational isoscles triangle with the same are and the same perimeter. Let us see why this is the only such pair, up to similarity of course. Following a method similar to the one in the introduction of this thesis, we first label the sides of the shapes in a clever way and find out that any such triangle-triangle pair would yield rational numbers x, k satisfying

$$2xk^2 + (-3x^3 - 2x^2 + 6x - 4)k + x^5 = 0.$$

Again very similar to the method from the introduction, we observe that this can be seen as a quadratic equation in k, and if it is to have a rational solution, its discriminant should be

the square of some rational number y. We see that pair of triangles satisfying the discription induces a rational point on the curve

$$C: \quad y^2 = (x^2 - 2)(x^4 + 12x^3 - 30x^2 + 24x - 8) =: f(x).$$

The polynomial f splits into a quadratic and quartic polynomial; they are irreducible over $\mathbb{Q}$ and have no repeated roots over $\mathbb{C}$, so C defines a hyperelliptic curve of genus 2. This was also the case in the introduction. However, as we will see in the next chapter, we will be able to make a great simplification (to an elliptic curve) in that case, but unfortunately that is not possible in the present example. The strategy to solving this problem is similar: we find all the points on C and show that only one of them can possibly come from a triangle-triangle pair. This can be done using the following powerful result, which is due to Robert Coleman. The proof can be found in chapter 6 of [21].

Theorem 5.10. *Let C be a hyperelliptic curve of genus g over $\mathbb{Q}$ with Jacobian J. Assume that the rank r of the Mordell-Weil group $J(\mathbb{Q})$ is strictly less than g. Let p be a prime of good reduction for C such that $p > 2g$. Then,*

$$\#C(\mathbb{Q}) \leq \#C(\mathbb{F}_p) + 2g - 2.$$

We can easily check that C has good reduction at $p = 5$ and that $C(\mathbb{F}_p) = 8$. If we can show that the rank r of $J(\mathbb{Q})$ is at most 1, then the bound above tells us that $C(\mathbb{Q}) \leq 10$. Now another remarkable feature of this example comes in: we can find 10 rational points on C! They are given by

$$\{\infty_{\pm 1}, (0, \pm 4), (1, \pm 1), (2, \pm 8), (12, \pm 868)\}.$$

Therefore, solving the problem eventually boils down to showing that the rank of $J(\mathbb{Q})$ is at most 1. Hirakawa and Matsumura use Magma for this, see [12]. The way to (in principle) to it explicitly is to use the theory developed in this chapter to compute the 2-Selmer group, which is defined similarly for Jacobians of hyperelliptic curves. The computations, however, become rather involved for two main reasons. First, the ring A is given by the product of a (real) quadratic- and a quartic number field. The difficulty comes from the quartic number field. Luckily, you could say, it has class number 1, which simplifies the computations, but the unit group of its ring of integers has rank 2. For this reason, we cannot use a trick which we will apply in the proof of Lemma 6.9. Moreover, by Formula (10), the dimension of the image of δ_2, which we will need in order to calculate $\mathrm{Sel}^{(2)}(J)$, is 4. Hence we need to find genuine 2-adic points on C to fill up this image, and they are rather difficult to manipulate. These computations are possible, in principle, but the case treated in the next chapter still illustrates a lot of the theory discussed and is more insightful as the computations are more manageable. Hopefully, the following chapter, which contains an explicit solution to the triangle-rhombus problem, will provide the reader with a lot of joy and entertainment, as it has done for the author.

6 Application to the triangle-rhombus problem

In this chapter we will use the theory from the previous chapters to solve the geometric problem from the introduction. That is, we will show that it is not possible for a rational isosceles triangle and a θ-rational rhombus to have the same area and the same perimeter. As opposed to the original paper [26], all computations[8] have been done by hand, yielding a complete "pen and paper"-solution to the problem.

As shown in the introduction of this thesis, a triangle-rhombus pair would give rise to a rational point on the hyperelliptic curve of genus 2 given by

$$C: \quad y^2 = x^6 - 4x^4 + 8x^2 - 4.$$

The goal of this chapter is to show that there are only finitely many points on this curve, and that none of them can possibly correspond to a triangle-rhombus pair. We will do this by breaking the problem up into pieces. In each subsection, we deal with one such piece, and in the end we put it all together to solve the problem.

6.1 The curve $E : y^2 = x^3 + 8x^2 + 16x + 16 =: f(x)$

We start with a trivial observation, which can be found in [16], for instance. If we have two curves C, D over a field k and a non-constant morphism, see [16], $\phi : C \to D$, then $\phi(C(k)) \subset D(k)$. If we determine $D(k)$ to be finite, then we can find $C(k)$. In our case, the curve C over $\mathbb{Q}$ has a particular form, and the observant reader may have already noticed that the morphism defined by $(x, y) \mapsto (x^2, y)$ maps C to an the elliptic curve defined by

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

This looks promising, for in chapter 2 we have seen that it is easier to deal with elliptic curves than with hyperelliptic curves. Unfortunately, this elliptic curve has rank 1 and hence its group of rational points is infinite, which can be seen by using the command 'Rank(E)' in Magma. There is, however, a different morphism which is more fruitful: ϕ defined by $\phi(x, y) = (-4/x^2, 4y/x^3)$ maps C to the elliptic curve

$$E: \quad y^2 = x^3 + 8x^2 + 16x + 16 =: f(x).$$

We will show that $E(\mathbb{Q})$ is finite, from which it will follow that $C(\mathbb{Q})$ is finite as well.

[8] All computations that directly lead to the solution, that is. With the help of his supervisor, a computer was used to guide the author along the way, and in particular to avoid dead ends, see for instance section 6.1.

6.2 The group $T = E(\mathbb{Q})_{\text{tors}}$

By the Mordell-Weil Theorem, $E(\mathbb{Q})$ is finitely generated and hence $E(\mathbb{Q}) \cong \mathbb{Z}^r \times T$, where $r \in \mathbb{Z}_{\geq 0}$ and $T = E(\mathbb{Q})_{\text{tors}}$ is the finite torsion subgroup. In this section, we will determine T. First of all, the discriminant of f is given by $-2816 = -2^8 \cdot 11$, so E has good reduction at $p = 3$, as seen in section 4.3.

Lemma 6.1. *The group T is isomorphic to $\mathbb{Z}/5\mathbb{Z}$.*

Proof. Since E has good reduction at 3, we get from Theorem 4.8 that the reduction map $E(\mathbb{Q}) \to E(\mathbb{F}_3)$ restricts to an injective group homomorphism on T. That is,

$$T \hookrightarrow E(\mathbb{F}_3).$$

By simply considering the 9 values for (x, y) over $\mathbb{F}_3$ (3 for x, 3 for y), and adding the point at infinity, we find that

$$E(\mathbb{F}_3) = \{\infty, (0,1), (0,2), (2,1), (2,2)\},$$

and hence $\#T|5$. We can show that T is not trivial by considering $P = (-4, 4) \in E(\mathbb{Q})$. Namely, by the geometric group law, $2P = (0, -4)$, $3P = (0, 4)$, $4P = (-4, -4)$ and $5P = \infty$, so $P \in T$. We conclude that $\#T = 5$ and since there is only one group of order 5, $T \cong \mathbb{Z}/5\mathbb{Z}$. □

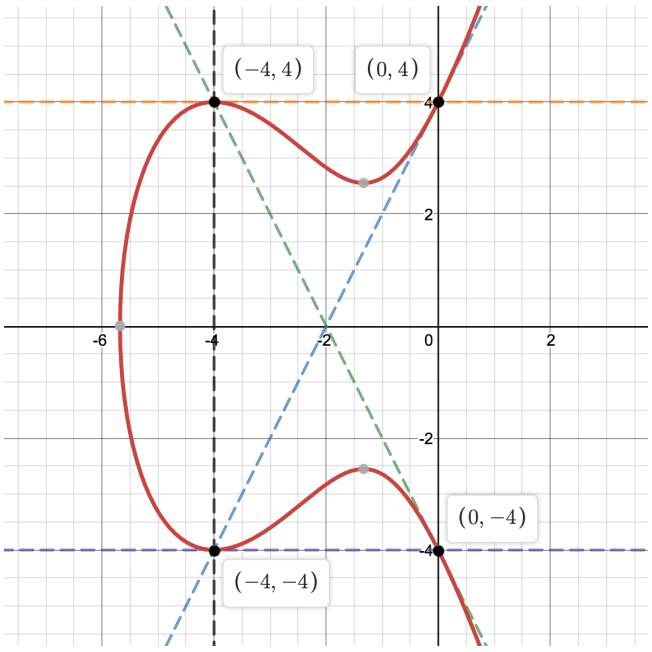

Figure 5: The curve $E : y^2 = x^3 + 8x^2 + 16x + 16$

By Lemma 3.1, $E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{Z}/5\mathbb{Z}$ for some $r \in \mathbb{Z}_{\geq 0}$. Our goal is to show that $r = 0$, for then indeed $E(\mathbb{Q})$ would be finite. Since 2 and 5 are coprime, $E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r$. Therefore, if we can show that $E(\mathbb{Q})/2E(\mathbb{Q})$ has only one element, then $r = 0$ and we are done. Before we continue our main line of reasoning, however, we take some time to study the field $\mathbb{Q}[x]/(f)$ in which our computations will take place.

6.3 The field $A = \mathbb{Q}[x]/(f)$

As an important intermezzo, we use some algebraic number theory from chapter 3 to analyse $A = \mathbb{Q}[x]/(f)$. Since f is irreducible over $\mathbb{Q}$, A is a cubic number field. If θ is the image of x in A, we may write the field as $A = \mathbb{Q}[\theta]$. In this section, we will determine its ring of integers, its class number and the prime ideals above 2 and 11 in this ring of integers. Finally, we will show that $1 + a$ is a unit which is not a square, since we will need such an element later.

Proposition 6.2. *The ring of integers of A is $\mathbb{Z}[a]$, where $a = \theta/2$.*

Proof. Let R be the ring of integers of A. First of all, we see that $a \in R$, because it satisfies the monic polynomial with integer coefficients g given by

$$g(x) = x^3 + 4x^2 + 4x + 2.$$

This follows from $g(a) = g(\theta/2) = f(\theta)/8 = 0$. Incidentally, g is the minimal polynomial of a, because it is an Eisenstein polynomial and hence irreducible.

We will show that there are no singular prime ideals in $\mathbb{Z}[a]$ using the Kummer-Dedekind Theorem 3.26 (for readability purposes, it would be useful to take a look at this theorem while reading this proof). To that end, take g to be the monic irreducible polynomial in Theorem 3.26 with a as a zero and suppose for contradiction that $\mathfrak{p}$ is singular. Then, $\mathfrak{p}$ lies above a rational prime p for which $\overline{g} = \overline{h}_1^2 \overline{h}_2$ modulo p for some polynomials $h_1, h_2 \in \mathbb{Z}[x]$. Therefore, p divides the discriminant of g, which is $-44 = -2^2 \cdot 11$.
Suppose $p = 2$. We can take $h_1(x) = h_2(x) = x$; the remainder of g upon division by x is 2, which is not divisible by $2^2 = 4$, contradicting the singularity of $\mathfrak{p}$.
Suppose $p = 11$. We can take $h_1(x) = x + 8$ and $h_2(x) = x + 10$. Note that $x^3 + 4x^2 + 4x + 2 = (x^2 - 4x + 36) - 286$, so the remainder of g upon division by $x + 8$ is $-286 = -2 \cdot 11 \cdot 13$, which is not divisible by $11^2 = 121$, again contradicting the singularity of $\mathfrak{p}$. Therefore, we may conclude that there are no singular prime ideals in $\mathbb{Z}[a]$. Since there are no singular primes in $\mathbb{Z}[a]$, it follows that $R = \mathbb{Z}[a]$. □

Corollary 6.3. *A has class number 1.*

Proof. By Proposition 6.2, the ring of integers of A is $\mathbb{Z}[a]$. We show that $\mathbb{Z}[a]$ is a principal ideal domain. By theorem 4.10 in [19], the discrimant of A is $\Delta_A = \Delta(g) = -44$. Since f has only one real root, A has one real embedding and hence 2 complex embeddings. Therefore, by Theorem 3.17 the Minkowski bound is

$$M_A = \sqrt{44}\,\frac{4}{\pi}\,\frac{3!}{3^3} < 2$$

and hence $\mathbb{Z}[a]$ is a principal ideal domain. □

Proposition 6.4. *The prime ideal above 2 is (a).*

Proof. Again we use the Kummer-Dedekind Theorem with the monic irreducible polynomial g with zero a. Reducing modulo $p = 2$, the polynomial g factors as $\overline{g} = \overline{x}^3$ and hence the ideal $\mathfrak{p} = 2\mathbb{Z}[a] + a\mathbb{Z}[a]$ lies above 2. By Proposition 3.2, $\mathfrak{p}$ is not singular, so $2\mathbb{Z}[a] = \mathfrak{p}^3$. Finally, since $2 = a(-a^2 - 4a - 4)$, we have that $\mathfrak{p} = a\mathbb{Z}[a]$, proving the result. □

Proposition 6.5. *The prime ideals above 11 are* $(2a^2+7a+5)$ *and* $(a-1)$.

Proof. We use the Kummer-Dedekind Theorem once more with the polynomial g with a as a zero. Reducing modulo $p=11$, the polynomial g factors as $\overline{g}=\overline{h}_1^2\,\overline{h}_2$, where $h_1(x)=x+8$ and $h_2(x)=x-1$. By Theorem 3.26 the ideals $\mathfrak{p}_1=11\mathbb{Z}[a]+(a+8)\mathbb{Z}[a]$ and $\mathfrak{p}_2=11\mathbb{Z}[a]+(a-1)\mathbb{Z}[a]$ lie above 11 and by Proposition 6.2 they are not singular. Therefore $11\mathbb{Z}[a]=\mathfrak{p}_1^2\mathfrak{p}_2$. Since $11=(a-1)(-a^2-5a-9)$, we have that $\mathfrak{p}_2=(a-1)\mathbb{Z}[a]$. As for $\mathfrak{p}_1$, note that $2a^2+7a+5=7\cdot 11+(2a-9)(a+8)$, so $(2a^2+7a+5)\mathbb{Z}[a]\subset\mathfrak{p}_1$. Moreover, we have that $11=(-a^2-7a-3)(2a^2+7a+5)$ and that $a+8=(-a^2-5a-2)(2a^2+7a+5)$. This yields $\mathfrak{p}_1=(2a^2+7a+5)\mathbb{Z}[a]$, as desired. □

Proposition 6.6. $1+a$ *is a unit which is not a square.*

In the proof of this result, we will use that an element of $\mathcal{O}_K$ with norm equal to ± 1 is a unit. To see this, let $\alpha\in\mathcal{O}_K$ and suppose that $N_{K/\mathbb{Q}}(\alpha)=\pm 1$. Then, the characteristic polynomial of α is $x^n+c_{n-1}x^{n-1}+\cdots+c_1x\pm 1$, for some $c_i\in\mathbb{Z}$. Therefore, $\mp(\alpha^{n-1}+c_{n-1}\alpha^{n-2}+\cdots+c_1)\in\mathcal{O}_K$ is the inverse of α, so $\alpha\in\mathcal{O}_K^*$.

Proof. Note that $1,\theta,\theta^2$ is a basis for $A/\mathbb{Q}$. We have $(1+a)\cdot 1=1+\frac{1}{2}\theta$, $(1+a)\cdot\theta=\theta+\frac{1}{2}\theta^2$ and $(1+a)\theta^2=\theta^2+\frac{\theta^3}{2}=-8-8\theta-3\theta^2$. Recall that the norm of an element is the determinant of the multiplication map and so we compute

$$N(1+a)=\det\begin{pmatrix}1 & 0 & -8\\ 1/2 & 1 & -8\\ 0 & 1/2 & -3\end{pmatrix}=-1.$$

Therefore, $1+a$ is a unit. It is not a square, because the norm map is multiplicative. □

6.4 The group $A_2^\times/(A_2^\times)^2$

We continue our journey to show that $E(\mathbb{Q})/2E(\mathbb{Q})$ is trivial. In section 5.3, we have seen that it suffices to show that $\mathrm{Sel}^{(2)}(E) = \{\alpha \in H | \forall p : \rho_p(\alpha) \in \mathrm{im}\,\delta_p\}$ is trivial. It is a known result, see for instance Corollary 4.7 in [20], that we only have to look at the primes 2, ∞ and the p for which p^2 divides the discriminant. Since the discriminant in our case is $-2^8 \cdot 11$, this leaves us only with 2 and ∞. However, since the theory required to prove this result is a bit beyond the author's level at this stage, and since we would like to leave as few black boxes as possible, we will not make explicit use of this fact. We can, however, simply start working with $p = 2$ and see whether this gives us enough information to show that $\mathrm{Sel}^{(2)}(E)$ has but one element. Since we have to work in H_2 for this, and since H_2 itself is a subgroup of $A_2^\times/(A_2^\times)^2$, we need to study the group $A_2^\times/(A_2^\times)^2$ more closely. In section 4.4, we have seen that $A_2^\times/(A_2^\times)^2$ can be identified with an $\mathbb{F}_2$-vector space of dimension $[A_2 : \mathbb{Q}_2] + 2 = 5$. We will find, using Stoll's algorithm, the representatives of $A_2^\times/(A_2^\times)^2$ that correspond to the five standard basis vectors under this identification (in fact, any five independent vectors would do). These representatives generate $A_2^\times/(A_2^\times)^2$ and they will help us to compute $\mathrm{Sel}^{(2)}(E)$ in the next section. First, we need to know the following about A_2 in order to apply Stoll's algorithm.

Lemma 6.7. *A uniformiser for A_2 is given by a, the ring of integers of A_2 is $\mathbb{Z}_2[a]$ and the residue field is $\mathbb{F}_2$.*

Proof. This follows from Proposition 4.9 and the fact that the polynomial g is Eisenstein. □

Proposition 6.8. *The images of $a, 1+a, -1, 1+2a, -3 \in A_2^\times$ in $A_2^\times/(A_2^\times)^2$ generate $A_2^\times/(A_2^\times)^2$.*

Proof. As announced, we use Stoll's algorithm to compute the representation in $\mathbb{F}_2^5$ of the images of the proposed elements. In the algorithm, we take $K = A_2$ with uniformiser $\pi = a$ and ring of integers $\mathcal{O} = \mathbb{Z}_2[a]$. The residue field is $k \cong \mathbb{F}_2$ and hence we can take $B = \{1\}$. Applying Stoll's algorithm to a yields the vector $(1, 0, 0, 0, 0)$. Inspired by the fact that 2, -1 and 3 generate $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$, see Corollary 4.10, we apply the algorithm to -1 and 3. This yields new vectors $(0, 0, 1, 0, 0)$ and $(0, 0, 1, 0, 1)$. For aesthetic purposes, we use -3 instead of 3, because -3 gives $(0, 0, 1, 0, 0) + (0, 0, 1, 0, 1) = (0, 0, 0, 0, 1)$. As seen in Proposition 6.6, $1 + a$ is a unit, so $v(1 + a) = 0$. Carrying out the rest of the algorithm for $1 + a$ yields another new vector: $(0, 1, 0, 0, 0)$. This leaves us with the task of finding an element that gives a nonzero fourth component after applying the algorithm. After trying many different ones, it turns out that $1 + 2a$ works. It is a unit, for if it would have positive valuation, then so would $(1 + 2a) - a = 1 + a$, which we know is not the case. Carrying out the rest of the steps is straightforward and yields $(0, 0, 0, 1, 0)$. In summary, the group $A_2^\times/(A_2^\times)^2$ is generated by the images of the proposed elements. □

It may seem that finding these generators by hand is a rather trivial and unnecessary exercise. Recall, however, that the goal of this project is to have a complete "pen and paper"-solution and computing the generators as above, while taking some effort and many tedious computations, turns out to be absolutely key to the solution. Namely, we now have the following identification of $A_2^\times/(A_2^\times)^2$ with $\mathbb{F}_2^5$.

$\mathbb{F}_2^5$	$A_2^\times/(A_2^\times)^2$
$(1,0,0,0,0)$	$a \quad (A_2^\times)^2$
$(0,1,0,0,0)$	$(1+a) \quad (A_2^\times)^2$
$(0,0,1,0,0)$	$-1 \quad (A_2^\times)^2$
$(0,0,0,1,0)$	$(1+2a) \quad (A_2^\times)^2$
$(0,0,0,0,1)$	$-3 \quad (A_2^\times)^2$

Table 1: Identification of $A_2^\times/(A_2^\times)^2$ with $\mathbb{F}_2^5$

Showing that two subgroups of $A_2^\times/(A_2^\times)^2$ intersect trivially hence amounts to finding their corresponding subspaces in $\mathbb{F}_2^5$ and showing that they are linearly independent.

6.5 The group $\mathrm{Sel}^{(2)}(E)$

In this section we will use what we have done so far to show that the 2-Selmer group is trivial. It will read a bit like a detective story: we start with a rather long list of suspects that can potentially be in the 2-Selmer group. By making several deductions, we keep reducing this list until only one element is left.

Lemma 6.9. *We have the following inclusion:*

$$\mathrm{Sel}^{(2)}(E) \subset \langle -1, 1+a, a, 2a^2+7a+5, 1-a \rangle.$$

Proof. The proof of Theorem 5.7 tells us that $\mathrm{Sel}^{(2)}(E)$ is contained in the subgroup generated by the units and the primes above the rational primes dividing the discriminant. It follows from Theorem 3.30 that the group of units has rank 1 and the presence of a real root ensures that that the torsion part of the unit group is simply $\{\pm 1\}$. By Proposition 6.6, $1+a$ is a unit which is not a square, so if η generates the free part of the unit group, then $1+a$ must be an odd power of η. Modulo squares, then, we can take $1+a$ as the generator for the free part of the unit group[9]. By applying Propositions 6.4 and 6.5, we find that the suggested inclusion holds. □

Since the 2-Selmer group consists of elements of H which are in the kernel of the norm map, we can get more information by considering the norms.

[9]In fact, $1+a$ is a generator of the free part of the unit group of the ring of integers of A, but this takes some effort to show and as mentioned we do not need it.

Lemma 6.10. *We have the following inclusion:*

$$\mathrm{Sel}^{(2)}(E) \subset \langle -1-a, 3a^2+10a+9\rangle.$$

Proof. As in the proof of Proposition 6.6, we can compute

$$\begin{aligned} N(-1) &= -1 \\ N(1+a) &= -1 \\ N(a) &= 2 \\ N(2a^2+7a+5) &= 11 \\ N(1-a) &= 11. \end{aligned}$$

For a product of these elements to be in H, the norm needs to be a square. Since we are working modulo squares, this leaves $-1\cdot(1+a) = -1-a$ and $(2a^2+7a+5)(1-a) = 3a^2+10a+9$. □

We can get more information on the 2-Selmer group by simply using the following easy fact:

$$\mathrm{Sel}^{(2)}(E) = \{\alpha \in H | \, \forall p: \ \rho_p(\alpha) \in \operatorname{im}\delta_p\} \subset \{\alpha \in H | \, \rho_2(\alpha) \in \operatorname{im}\delta_2\}.$$

Lemma 6.11. *We have the following inclusion:*

$$\mathrm{Sel}^{(2)}(E) \subset \langle 3a^2+10a+9\rangle.$$

Proof. The previous Lemma 6.10 implies that any $\alpha \in \mathrm{Sel}^{(2)}(E)$ can be represented as

$$\alpha = (-1-a)^{\varepsilon_1}(3a^2+10a+9)^{\varepsilon_2},$$

where $\varepsilon_i = 0, 1$. Applying Stoll's algorithm and the identification displayed in Table 1, we find that $\rho_2(-1-a) = (0,1,1,0,0)$ and $\rho_2(3a^2+10a+9) = (0,0,0,1,0)$, so

$$\rho_2(\alpha) = \varepsilon_1(0,1,1,0,0) + \varepsilon_2(0,0,0,1,0).$$

A necessary condition for α to be in the 2-Selmer group is that $\rho_2(\alpha) \in \operatorname{im}\delta_2$. In order to compute the image of δ_2 we use formula (10) from section 5.4. Since there is no 2-adic 2-torsion, the dimension of the image of δ_2 as an $\mathbb{F}_2$-vector space is 1. We can compute this image in $A_2^\times/(A_2^\times)^2$ under our usual identification by simply exhibiting a point in $E(\mathbb{Q}_2)$ that has a nontrivial image under δ_2. Note that $f(1) = 41$. By Corollary 4.11, 41 is a square in $\mathbb{Q}_2$. Let $\eta \in \mathbb{Q}_2$ be such that $\eta^2 = 41$. Then, $(1,\eta) \in E(\mathbb{Q}_2)$ and $\delta_2(1,\eta) = (1-\theta)\,(A_2^\times)^2 = (1-2a)\,(A_2^\times)^2$. Applying Stoll's algorithm shows that

$$\operatorname{im}\delta_2 = \langle (0,0,0,1,0)\rangle.$$

Therefore, $\varepsilon_1 = 0$ and the assertion follows. □

At this point we have pretty much exhausted the information coming from the prime $p = 2$. If we want to bound the 2-Selmer group even further, we will have to look at other primes as well. It follows from formula (10) that the image of δ_∞ is trivial, so considering the infinite prime will not give us any additional information. For the last step we will hence consider $p = 11$.

Proposition 6.12. *The group* $\mathrm{Sel}^{(2)}(E)$ *is trivial.*

Proof. Using Lemma 6.11 we only have to show that the coset represented by $3a^2+10a+9$ is not in the 2-Selmer group. For this, we consider the prime $p=11$. Note that $f(3)=163\in\mathbb{Z}_{11}^\times$ is a square in $\mathbb{Q}_{11}$, because $163\equiv 9 \mod 11$ is a square in $\mathbb{F}_{11}$, cf. Corollary 4.6. If $\eta\in\mathbb{Q}_{11}$ is such that $\eta^2=163$, then $(3,\eta)\in E(\mathbb{Q}_{11})$. Its image under δ_{11} will turn out to be nontrivial and therefore, by formula (10), generates $\operatorname{im}\delta_{11}$. In order to show that $3a^2+10a+9\notin\mathrm{Sel}^{(2)}(E)$, it suffices to show that $\rho_{11}(3a^2+10a+9)\notin\operatorname{im}\delta_{11}$. We will do this by showing that $\delta_{11}(3,\eta)=(3-2a)\,(A_{11}^\times)^2$ is linearly independent from $(3a^2+10a+9)\,(A_{11}^\times)^2$, under some identification with an $\mathbb{F}_2$-vector space. In order to get such an identification, we note that, by the proof of Proposition 6.5,

$$A_{11}^\times/(A_{11}^\times)^2\cong K_{11,1}^\times/(K_{11,1}^\times)^2\oplus K_{11,2}^\times/(K_{11,2}^\times)^2$$

for some fields $K_{11,i}$, where $K_{11,1}\cong\mathbb{Q}_{11}$ and $K_{11,2}$ is a quadratic extension of $\mathbb{Q}_{11}$. By the p-adic version of Theorem 3.29, the extension $K_{11,2}/\mathbb{Q}_{11}$ is totally ramified. Let φ_i denote the natural maps from A_{11} to $K_{11,i}$. Then, a uniformiser for $K_{11,2}$ is given by $\pi_2=\varphi_2(2a^2+7a+5)$, which follows from the isomorphism asserted in proposition 4.3 from [15]. By section 3 of Stoll's paper [20], $K_{11,2}^\times/(K_{11,2}^\times)^2$ is a two-dimensional $\mathbb{F}_2$-vector space V, and the image of $\alpha\in K_{11,2}^\times$ in V is found by writing $\alpha=\pi_2^n u$, where u is a unit. The first coordinate in V is determined by the parity of n, and the second by whether or not the image of u in the residue field is a square. Since $K_{11,2}/\mathbb{Q}_1 1$ is totally ramified, the residue field is simply $\mathbb{F}_{11}$. We will show that the images in V of $\varphi_2(3-2a)$ and $\varphi_2(3a^2+10a+9)$ are linearly independent, proving the desired result. First, note that that $3a^2+10a+9=(2a^2+7a+5)(1-a)$ and hence $\varphi_2(3a^2+10a+9)=\pi_2\varphi_2(1-a)$, so (using the proof of Proposition 6.5) $v_{\pi_2}(\varphi_2(3a^2+10a+9))=1$. Thus the first component of the image of $\varphi_2(3a^2+10a+9)$ in V is 1. On the other hand, we claim that $v_{\pi_2}(\varphi_2(3-2a))=0$. To see this, suppose for contradiction that $v_{\pi_2}(\varphi_2(3-2a))\neq 0$. Then, since $3-2a\in\mathcal{O}_{K_{11,2}}$, it follows that $v_{\pi_2}(\varphi_2(3-2a))>0$. However, this cannot be, because then the equality

$$9=(2a^2+7a+5)-11+(3-2a)(5+a)$$

implies that $v_{\pi_2}(9)>0$, which is not true since $v_{11}(9)=0$. So for, we have shown that the images in V of $\varphi_2(3-2a)$ and $\varphi_2(3a^2+10a+9)$ differ in the first coordinate. In order to establish linear independence, it therefore suffices to show that $\varphi_2(3-2a)$ is not a square. We have shown that it is a unit, so what is left is to show that its image in the residue field $\mathbb{F}_{11}$ is not a square. This is seen by writing

$$3-2a=8+(2a^2+7a+5)(a^2+3a+1),$$

so

$$\varphi(3-2a)=8+\pi_2\,\varphi(a^2+3a+1).$$

Hence the image of $\varphi(3-2a)$ in the residue field $\mathcal{O}_{K_{11,2}}/\pi_2\mathcal{O}_{K_{11,2}}\cong\mathbb{F}_{11}$ is $\overline{8}$, which is indeed not a square in $\mathbb{F}_{11}$. Therefore, the images in V of $\varphi_2(3-2a)$ and $\varphi_2(3a^2+10a+9)$ are linearly independent, which implies that $\delta_{11}(3,\eta)=(3-2a)\,(A_{11}^\times)^2$ is linearly independent from $(3a^2+10a+9)\,(A_{11}^\times)^2$, under the identification of $A_{11}^\times/(A_{11}^\times)^2$ with the four-dimensional $\mathbb{F}_2$-vector space presented in section 3 of [20]; hence, the coset in $A^\times/(A^\times)^2$ represented by $3a^2+10a+9$ is not in the 2-Selmer group. It follows that $\mathrm{Sel}^{(2)}(E)$ is trivial, as desired.

□

Corollary 6.13. *The group $E(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$.*

Proof. By the Mordell-Weil theorem and Lemma 6.1, we already know that $E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{Z}/5\mathbb{Z}$ for some nonnegative integer r. Therefore, by Lemma 5.2,

$$\delta(E(\mathbb{Q})) \cong E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r,$$

cf. the discussion following Lemma 6.1. The image $\delta(E(\mathbb{Q})$ is contained in the 2-Selmer group by Theorem 5.7. From Proposition 6.12 it follows that $\delta(E(\mathbb{Q})$ is trivial and hence that $r = 0$, as desired. □

6.6 The solution

We return to the triangle-rhombus problem. We now have everything we need to prove the following.

Theorem 1.1. *There do not exist a rational isosceles triangle and a θ-rational rhombus with the same area and the same perimeter.*

Proof. Recall that a rational isosceles triangle and a θ-rational rhombus with equal area and equal perimeter would give rise to positive rational numbers u, v, t satisfying

$$v(u^2 - v^2)t^2 - u^3t + v(u^2 - v^2) = 0 \tag{11}$$

and that, hence, when viewing this as a quadratic equation in t, its discriminant must be the square of some rational number w, that is,

$$u^6 - 4u^4v^2 + 8u^2v^4 - 4v^6 = w^2. \tag{12}$$

By substituting $x = u/v$ and $y = w/v^3$, we noticed that such a triangle-rhombus pair necessarily corresponds to a rational point on the hyperelliptic curve

$$C: \quad y^2 = x^6 - 4x^4 + 8x^2 - 4.$$

We are now in a position to determine $C(\mathbb{Q})$ and thus whether any such triangle-rhombus pairs exist. In the start of this chapter we have seen that the morphism ϕ defined by $\phi(x, y) = (-4/x^2, 4y/x^3)$ maps C to the elliptic curve E which has been the main topic of this chapter. We thus have $\phi(C(\mathbb{Q})) \subset E(\mathbb{Q})$ and hence $C(\mathbb{Q}) \subset \phi^{-1}(\phi(C(\mathbb{Q}))) \subset \phi^{-1}(E(\mathbb{Q}))$. At the end of the previous section we managed to show that $E(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$ and by Lemma 6.1 the rational points on E are given by

$$E(\mathbb{Q}) = \{\infty, (0, \pm 4), (-4, \pm 4)\}.$$

This tells us that the following inclusion holds:

$$C(\mathbb{Q}) \subset \phi^{-1}(E(\mathbb{Q})) = \{\infty_{\pm 1}, (\pm 1, \pm 1)\},$$

so the finite rational points on C have both x- and y-coordinate equal to ± 1. Since we made the substitutions $x = u/v$ and $y = w/v^3$, we find that any solution $u, v, w \in \mathbb{Q}$ of (12) satisfies $u = \pm v$, $w = \pm v^3$. Together with (11), this implies that $u^3t = 0$, so (11) has no solutions in the positive rationals. Therefore, there exist no rational isosceles triangle and a θ-rational rhombus with the same area and the same perimeter. □

7 Discussion and conclusion

In conclusion, the fields of (hyper)elliptic curves, algebraic number theory and p-adic numbers were studied to solve a geometric problem first solved by Zhang and Peng. In the end, chapter 6 contains a fully explicit solution to the problem, leaving only a few results as black boxes. The goal set in the introduction was thus achieved.

In the process there were some ups and downs. Particularly, the initial objective was to focus on the problem outlined in Example 5.9, but for the reasons given there it did not seem feasible to carry out all computations by hand within the time set for this thesis (if at all). The problem of Zhang and Peng, however, is also beautiful and since we have succesfully been able to solve it, the author is happy with the result. In addition, it has been a pleasure to study so much theory that is usually treated in master's courses. This will certainly help the author in his future studies.

References

[1] Alex van den Brandhof. Wat maakt deze twee driehoeken zo uniek? *NRC Handelsblad*, 2019.

[2] John William Scott Cassels. The Mordell-Weil group of curves of genus 2. *Arithmetic and geometry*, pages 27–60, 1983.

[3] John William Scott Cassels. *Local fields*, volume 3. Cambridge University Press Cambridge, 1986.

[4] John William Scott Cassels. *LMSST: 24 Lectures on Elliptic Curves*, volume 24. Cambridge University Press, 1991.

[5] Shane Chern. Integral right triangle and rhombus pairs with a common area and a common perimeter. *arXiv preprint arXiv:1602.02844*, 2016.

[6] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren. *Handbook of elliptic and hyperelliptic curve cryptography*. Chapman and Hall/CRC, 2005.

[7] Keith Conrad. *Hensels lemma*. Lecture notes, University of Connecticut, 2015.

[8] Tim Dokchitser. *Local Fields*. Lecture notes, University of Cambridge, 2007.

[9] Jan-Hendrik Evertse. *p-Adic Numbers*. Lecture notes, Leiden University, 2011.

[10] Richard K Guy. My favorite elliptic curve: a tale of two types of triangles. *The American mathematical monthly*, 102(9):771–781, 1995.

[11] Thomas Little Heath. *Diophantus of Alexandria: A study in the history of Greek algebra*. CUP Archive, 1910.

[12] Yoshinosuke Hirakawa and Hideki Matsumura. A unique pair of triangles. *Journal of Number Theory*, 194:297–302, 2019.

[13] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84. Springer Science & Business Media, 2013.

[14] Louis Mordell. On the rational solutions of the indeterminate equation of the third and fourth degree. In *Proc. Camb. Phil. Soc.*, volume 21, pages 179–192, 1992.

[15] Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.

[16] Samir Siksek. *Chabauty and the Mordell-Weil Sieve.* Lecture notes, University of Warwick, 2015.

[17] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

[18] Joseph H Silverman and John Torrence Tate. *Rational points on elliptic curves*, volume 9. Springer, 1992.

[19] Peter Stevenhagen. *Number Rings*. Lecture notes, Leiden University, 2012.

[20] Michael Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arithmetica-Warszawa*, 98(3):245–277, 2001.

[21] Michael Stoll. *Arithmetic of Hyperelliptic Curves*. Lecture notes, University of Bayreuth, August 2014.

[22] E.J. van Timmeren. *Eenhedengroep van de ring* $\mathbb{Z}[\sqrt[3]{m}]$. Bachelor's thesis, University of Groningen, July 2012.

[23] Jaap Top. *Algebraic Structures*. Lecture notes, University of Groningen, 2016.

[24] Jaap Top. *Advanced Algebraic Structures*. Lecture notes, University of Groningen, 2017.

[25] André Weil et al. L'arithmétique sur les courbes algébriques. *Acta mathematica*, 52:281–315, 1929.

[26] Yong Zhang and Junyao Peng. Heron triangle and rhombus pairs with a common area and a common perimeter. *arXiv preprint arXiv:1707.00526*, 2017.