# Ranks in Diophantus' family of elliptic curves

Kootwijk, Bart van

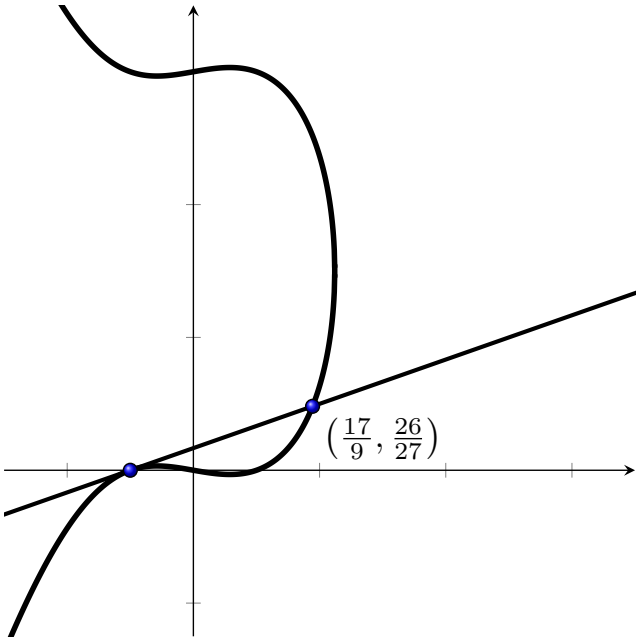
University of Leiden

MSc Mathematics Thesis

# Ranks in Diophantus' family of elliptic curves

*Author:*
Bart van Kootwijk

*Supervisor:*
prof. dr. Jan Vonk




27 August 2025

Universiteit Leiden
The Netherlands

# Acknowledgement

Very few would say that the process in which this thesis was written was a smooth one. Some might say it was a complete disaster. Many more would be saying this, were it not for the so many people who, for far longer than should have been necessary, kept gently pushing me to continue and finish it, while helping in whatever way they could. To start, I would like to thank, in alphabetical order, my closest friends and family

Amber, Dad, Daniël, David, Floor, `\footnote{...}`, Jelle, Lide, Lois, Meili, Mom, Pim, my little Sis', Steef, Stijn, and Tamar,

for their everlasting patience, and for them relentlessly but politely asking about "the S thing", even when I desperately wanted them not to. It was because of their voices of confidence[1] that I kept faith that I, at some yet to be determined point in time, would indeed finish writing this.

A special thanks to Daniël, Pim, and Lide and Floor, who so often generously offered me a place in their living rooms on days where I otherwise would not have been productive, or would have gone insane.

And last but definitely not least (quite the opposite actually) is my supervisor Jan. Although I was far from the perfect student, any time I asked for help he would always be there for me, with never-ending wisdom, kindness, and patience. From the bottom of my heart, Jan, thank you.

[1] Some others who shared this sentiment are the manager of my favorite climbing gym and my optician.

# Contents

# Introduction

In his Arithmetica[1], written in the third century AD, Diophantus of Alexandria tasked the reader with the following exercise:

> *"To divide a given number into two numbers and make their product a cube except [its] side."*

(see book IV$^G$, problem 24 in [CO23]). Calling the given number $m$, we are thus tasked with finding numbers $y$ and $m - y$ summing to $m$, such that their product equals $x^3 - x$ for some $x$. Implicit in the historical context of this exercise is that all of $y, m - y$ and $x$ must be strictly positive rational numbers. In modern terms, this exercise thus is equivalent to finding a rational point, with positive coordinates, on the curve given by the equation

$$D_m : y(m - y) = x^3 - x. \tag{1}$$

A modern reader will recognise eq. (1) as one defining an *elliptic curve*, a non-singular curve of genus 1 with a rational point. In fact, the exercise that Diophantus provided us appears to be the first recorded mention of an elliptic curve, although Diophantus certainly did not think of it in this manner. Nevertheless, his solution to the case for $m = 6$ still very much fits in the modern viewpoint.[2] Namely, his solution boils down to the following: he starts with the "illegal" solution $P = (x, y) = (-1, 0)$, takes the tangent line $L$ of $D_6$ at $P$, and then he finds the other intersection point of $L$ with $D_6$. In modern terms, this comes down to the calculation of

$$-2P = (26/27, 17/9),$$

which is non-trivial and satisfies the implicit constraints of the problem.

## The Mordell–Weil theorem

The rational solutions to Diophantus' equation, or the set of rational points on elliptic curves more generally, is described by the Mordell–Weil theorem. By definition, elliptic curves lie between genus 0 curves on one hand and curves of genus at least 2 on the other hand[3]. Genus 0 curves that contain a single rational point $P$ contain infinitely many, as these points are parametrised by lines with rational slopes through $P$. By Faltings's theorem, any curve of genus $g \geq 2$ has only a finite number of rational points. For elliptic curves, the situation is more variable, and has long remained mysterious, summarised best by Mordell in 1922 [Mor22].

> *"Mathematicians have been familiar with very few questions for so long a period with so little accomplished in the way of general results, as that of finding the rational [points on elliptic curves]."*

It was in this same paper that Mordell in part proved the theorem, now known as the Mordell–Weil theorem, which (at least partially) answered this question.

**Theorem** (Mordell–Weil)**.** *If $K$ is a number field and $E/K$ is an elliptic curve, then $E(K)$ is a finitely generated abelian group, i.e. there is an isomorphism*

$$E(K) \cong T \times \mathbb{Z}^r,$$

[1] This is the same work that contained the exercise "To divide a proposed square (number) into two squares" (book II, problem 8). It was in the margin next to this question where Pierre de Fermat wrote his famous *Last Theorem*, along with the mention that he had a proof that unfortunately did not fit in the margin.

[2] For a translation of his work into modern notation, see chapter 6 in [Bas97].

[3] In this context, by curve we mean a smooth, projective, and geometrically irreducible curve.

*with $T = E(K)_{\text{tors}}$ a finite group and $r \in \mathbb{N}$ an integer called the (algebraic)* rank *of $E(K)$.*

Mordell proved the $K = \mathbb{Q}$ case in his 1922 paper [Mor22], and the full version for arbitrary number fields was proved by Weil in 1929 [Wei29].[4]

The Mordell–Weil theorem allows us to decompose $E(K)$ as the product of two subgroups, the finite torsion subgroup and a (possibly infinite) free group. Much is known about the torsion part. Mazur's theorem (1976) tells us exactly which groups can occur as torsion groups for $K = \mathbb{Q}$. A later result by Merel in [Mer96] showed that for general number fields the torsion groups can be uniformly bounded in size.

**Theorem** (Merel)**.** *Let $d \in \mathbb{N}$. Then there exists a number $B(d) \in \mathbb{N}$ such that for every number field $K$ with $[K : \mathbb{Q}] = d$ and every elliptic curve $E/K$ we have*

$$|E(K)_{\text{tors}}| \leq B(d).$$

Later work by Parent in [Par99] gave an explicit value for $B(d)$. Meanwhile, Mazur's theorem has been extended to number fields of higher degree, and it is now known which torsion groups can occur for number fields of degree at most 4, see [Kam92] and [KM88] for quadratic fields, [DEvH$^+$21] for cubic fields, and [DN25] for the recent result on quartic fields. Moreover, there are effective algorithms to actually calculate the torsion groups, for example, see [Cre92].

## The minimalist conjecture

The free part of $E(K)$ has remained much more mysterious. For example, it is currently not even known whether the ranks of curves $E/\mathbb{Q}$ are bounded or not, and for a time they were generally believed to be unbounded. A recent heuristic however seems to indicate the opposite, as it predicts that there are (up to isomorphism) only a finite number of elliptic curves with rank higher than 21 [PPVW19].[5] Intuitively, this heuristic seems to tell us that generally, points on elliptic curves are rare, and there cannot be too many. There are a series of similar results and conjectures, all pointing in a similar direction.

- There is a folklore *minimalist conjecture*. One of the consequences to the BSD-conjecture is the *parity conjecture*, which states that[6]

  $$(-1)^{\operatorname{rank} E(K)} = w(E/K),$$

  where $w(E/K) \in \{\pm 1\}$ is the *(global) root number* of $E$ over $K$. The root number is an invariant of $E$ which can be determined solely by looking at the reduction of $E$ at its bad primes. The parity conjecture thus allows one to find the parity of $\operatorname{rank} E(K)$ directly by determining the root number. The minimalist conjecture then states that given this parity, the rank is expected to be minimal [BMSW07].

- Since the parity of the rank of an elliptic curve is suspected to have a 50% probability to be either odd or even, the minimalist conjecture implies that the average rank of all elliptic curves should be $1/2$. A recent result by Bhargava and Shankar in [BS15] shows that the average rank (when considering all elliptic curves ordered by height) is at most $7/6$.

- Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. For any $d \in \mathbb{Q}$ we can define the *quadratic twist* $E_d$ of $E$ by $d$ as the curve $E_d : dy^2 = x^3 + ax + b$, which is isomorphic to $E$ over $\mathbb{Q}(\sqrt{d})$. Goldfeld's conjecture states that the average rank of such quadratic twists is $\frac{1}{2}$, or more precisely that

  $$\lim_{D \to \infty} \frac{\sum_{|d|<D} \operatorname{rank} E_d}{\sum_{|d|<D} 1} = \frac{1}{2}$$

[4] In fact, Weil proved a more general version than the one stated above, as he proved the theorem for arbitrary abelian varieties, not just elliptic curves.

[5] Early researchers generally believed that they were bounded, but the consensus shifted in the 1960's due to a variety of reasons, one being the fact that it was shown that for functions fields $\mathbb{F}_p(T)$ the ranks are unbounded [TS67]. See [PPVW19, Section 3] for an overview.

[6] Although the full parity conjecture is currently not proven, there are several classes of curves for which the parity conjecture is known to hold, among which all curves of rank 0 or 1, and those for which the 2- and 3-primary parts of the Tate–Shafarevich group $Ш(E/K(E[2]))$ are finite [DD11].

when $d$ is taken over all square-free $d \in \mathbb{Z}$. In other words, Goldfeld's conjecture states that the minimalist conjecture holds when one restricts it to such a family of quadratic twists.[7]

## High ranks in the family of Diophantus

This brings us back to the family of Diophantus, whose members (in contradiction with this principle) seem to have many rational points. It can be quickly seen that each curve $D_m : y(m-y) = x^3 - x$ contains the points

$$(0,0),\ (1,0),\ (-1,0),\ (0,m),\ (1,m),\ (-1,m).$$

These points are not all independent (for example we have $-(1,0) = (1,m)$), but they do (generically) generate a rank 2 subgroup. In absence of other obvious rational points we thus might expect, according the above minimalist conjecture, that *most* curves in the family have rank either 2 or 3. Interestingly, when one calculates the ranks of the first thousand members of this family, one obtains the results given in table 1.

| **Rank** | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| **Occurrences** | 2 | 231 | 453 | 258 | 52 | 4 |

Table 1: Frequency of ranks for the curves $D_m$ with $1 \leq m \leq 1000$.

Surprisingly, and contrary to the expectations stated above, there is a high number of rank 4 curves, even outnumbering rank 2 curves in this range. This, of course, invites the question whether this behaviour is simply a statistical anomaly or if it persists as one computes a larger dataset. As we will see, on average the rank of $D_m$ indeed seems to lower as $m$ increases. In order to study this decay more closely, we will compare the behaviour found with the heuristic mentioned above from [PPVW19]. The conjecture states that an elliptic curve has probability

$$H^{(1-r)/24+o(1)}$$

of having rank at least $r$, where $H$ is the (naive) height of $H$ measuring the size of its coefficients, and $o(1)$ is a function that goes to zero as $H$ increases. Since a curve in Diophantus' family generically has rank at least 2, the conjecture as stated will definitely not hold for the family. Instead, it is natural conjecture that instead a curve has probability

$$H^{(1-(r-2))/24+o(1)}$$

of having rank at least $r$. The question at hand is now whether the family indeed follows these expectations, and if it does, what we can say about the yet mysterious $o(1)$ term. We will explore this subject in section 2.3.

The discussion so far focusses on the general behaviour of the family, which the majority of the members follow. A different approach is to instead focus on the outliers with exceptionally high rank. In this context, two main questions can be asked; which ranks occur in the family, and which ranks occur infinitely often. Both questions are difficult to answer, and generally progress is made only by explicitly finding curves of different ranks. For the first question, the best that we have managed is rank 8 (the first such curve being $D_{29689}$). In [BM02] a larger range is searched, where it was found that $D_{1531234}$ has rank at least 10.

Progress towards the second question can be made by constructing subfamilies that have higher generic rank $r$, meaning that all but finitely many members of this subfamily will have rank at least $r$. For the family of Diophantus, this was first done in [BM02], where a subfamily of generic rank 3 was constructed. To be precise, it was shown that for every $t \in \mathbb{Q}$, the curve

$$D_{108t^2-330t-180}$$

[7] Smith has announced a proof of Goldfeld's conjecture in [Smi17].

has rank at least 3, and an explicit expression for the additional generator is also given. It hence follows that the family of Diophantus contains an infinite number of curves of rank at least 3. This work was generalized in [Eik04], where it was shown that these quadratic subfamilies are far from rare. Namely, given any value $m_0 \in \mathbb{Q}$ and any point $R$ on $D_{m_0}$, there exists a quadratic polynomial $m(t)$ such $m(0) = m_0$, and such that $D_{m(t)}$ almost always has rank 3. By intersecting multiple of such quadratic families one can now obtain subfamilies of generic rank up to 5. Eikenberg indeed found a subfamily of generic rank 5, which was indexed by the points on the rank 2 elliptic curve

$$A : y^2 = x^3 - x^2 - 103307652308x + 12301315572924612.$$

By searching through a larger range of subfamilies we found that in fact a rank 2 indexing curve is far from the best that can be done, and we will obtain the following result (which is proposition 2.4.3).

**Proposition.** *There exists a (rational) map $m : B(\mathbb{Q}) \to \mathbb{Q}$, where $B$ is the rank 5 elliptic curve*

$$B : y^2 = x^3 - 831594956135615443677x + 42187336973175277338552097410 04$$

*such that for almost all $T \in B(\mathbb{Q})$ the curve $D_{m(T)}$ has at least rank 5.*

In summary, we will approach the subject in two distinct ways. On one hand, we consider the average behaviour of the family, where we are mainly concerned with the relative frequency with which curves of rank 4 and rank 5 occur compared to curves of lower rank. On the other hand, we will look into the construction of higher rank subfamilies.

In order to study these aspects, we need to calculate the rank of more curves in the Diophantus family. To understand how this can be done, we turn to the proof of the Mordell–Weil theorem. Namely, from the proof of the Mordell–Weil theorem one can extract an algorithm that computes the rank.

## Infinite descent

The proof of the Mordell–Weil theorem consists of two parts. First, one proves the weak Mordell–Weil theorem, which states that $E(K)/nE(K)$ is finite for some integer $n \geq 2$ (which we will show in theorem 1.2.8). This certainly must be the case if $E(K)$ is indeed finitely generated, but it is not yet a proof. For example, the group $\mathbb{Z}_p$ satisfies $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$, but it is not finitely generated (which follows from its uncountable cardinality). To exclude such cases the second part of the proof is needed, which roughly states that there are only finitely many "small" points (see section VIII.3 in [Sil09] for details).[8] In practice, determining $E(K)/nE(K)$ (a procedure known as an $n$-descent) is still the main tool used to determine the rank of $E(K)$. Given the decomposition $E(K) \cong T \times \mathbb{Z}^r$ provided by the Mordell–Weil theorem, it follows that

$$E(K)/nE(K) \cong (T/nT) \times (\mathbb{Z}/n\mathbb{Z})^r.$$

Assuming that we are able to determine $T$, this allows us to find the rank $r$ solely by considering the size of $E(K)/nE(K)$. It is unsurprising that the process of calculating $E(K)/nE(K)$ depends on $T$, more specifically on the $n$-torsion part $E(K)[n]$ of $T$. It is known that over an algebraic closure $\bar{K}$ of $K$ (or equivalently over $\mathbb{C}$) we have

$$E(\bar{K})[n] \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}),$$

and any subgroup of this may be $K$-rational. The traditional reference on the subject [Sil09] only explicitly shows how $E(K)/nE(K)$ can be found in the situation where $E(K)$ contains a point of order $n$. Unfortunately for us, this is not applicable for the family of Diophantus, as $D_m(\mathbb{Q})$ is torsion-free for almost all integers $m$, $m = 0$ being the sole exception.[9] Therefore, it is necessary to expand this theory and learn how to do a so called *irrational* $n$-descent. As often it is sufficient to only consider the $n = 2$ case, we will focus on this. We do this using a cohomological interpretation, avoiding ad hoc solutions as much as possible.

[8] This part of the proof is very like the proof Fermat gave for the $n = 4$ case of his Last Theorem. Here, Fermat used the technique of *infinite descent*. That is, he showed that given an integer solution $(x, y, z)$ of the equation $x^4 + y^4 = z^4$ there must be a smaller solution. This results in an impossible infinitely descending chain of solutions, yielding a contradiction and the name of the proof. Similarly, the proof of the Mordell–Weil theorem is also described as "doing a descent".

[9] We will prove this fact in section 2.2.1.

## Overview of this thesis

In chapter 1 we develop the method of irrational 2-descent through cohomology. In section 1.1 we consider the simpler case of fully rational $n$-torsion, as this simpler case allows us to demonstrate many of the relevant ideas. Then, in section 1.2 we develop the full theory needed to deal with curves without rational torsion. As a finishing touch we will apply this theory on Diophantus's curve $D_6$ and show how one can find not only one, but (provably) all points on this curve. In chapter 2 we turn to the family of Diophantus. In section 2.1 we discuss analytic ranks and their relevance in the computation of algebraic ranks. In section 2.2 we then proceed with some general properties of the family; we prove the lack of torsion and discuss the occurrences of higher ranks within the family. In section 2.3 we analyze the data that we obtained and compare it to existing heuristics. Finally, in section 2.4 we discuss the results by Eikenberg [Eik04] on subfamilies of higher generic rank.

# Notation

- For $m \in \mathbb{Q}$, $D_m$ denotes the elliptic curve given by

$$D_m : y(m - y) = x^3 - x.$$

- We use $K, L, M, ...$ to denote number fields, $k, \ell, m, ...$ for residue fields, and $\mathcal{K}, \mathcal{L}, \mathcal{M}, \ldots$ for complete fields.
- For a field $K$, we let $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$ denote the absolute Galois group of $K$, which if $K$ is perfect equals $\mathrm{Gal}(\bar{K}/K)$.
- For $K$ a field and $M$ a $G_K$-module, we write $H^n(K, M) := H^n(G_K, M)$.
- For an abelian group $A$ and an integer $n \in \mathbb{Z}_{\geq 2}$ we write $A[n]$ for the $n$-torsion subgroup $\{a \in A : n \cdot a = 0\}$.

# Chapter 1

# Cohomological 2-descent

The goal of this chapter is to discuss the method of 2-descent for elliptic curves over number fields that do not possess a rational 2-isogeny. Though less classical than the case of elliptic curves with a rational 2-isogeny, the method for irrational 2-torsion is described for instance in [Sil09, Exercise 10.9] or [Cas91, Chapter 15]. Our goal is to recast this method cohomologically, providing an alternative description compared to the above sources. We start initially with an elliptic curve $E$ defined over a number field $K$, and study for any $n \geq 2$ the injection

$$E(K)/nE(K) \hookrightarrow H^1(K, E[n])$$

obtained by passing to the long exact sequence in Galois cohomology associated to the short exact sequence of $G_K$-modules defined by the multiplication by $n$ map:

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{n} E \longrightarrow 0.$$

In section 1.1 the case in which $E$ has fully $K$-rational $n$-torsion is discussed. In spite of this case being covered extensively in the literature, its inclusion in this thesis allows us to introduce some notation and many relevant ideas needed for the irrational case. In section 1.2 we set $n = 2$ and discuss the case where $E[2]$ is irreducible. As an illustration, we discuss the rank computation for the Diophantus curve

$$D_6 : y(6 - y) = x^3 - x$$

revisiting the example discussed in the introduction. In the next chapter, this method will be applied to a large number of curves $D_m$ in Diophantus' family, using its implementation in `Magma`.

## 1.1 Rational 2-torsion

Even though this material is very well-known, we use it as an opportunity to introduce some key notions that we will use later in the irreducible case. This part of the discussion is based on [Sil09, Chapter X]. We also determine the Mordell–Weil group of the simplest member of the Diophantus family, namely

$$D_0 : -y^2 = x^3 - x.$$

Let $E$ be an elliptic curve over a number field $K$, and let $n \geq 2$. In this section we consider the case where $E[n] \subseteq E(K)$. We let $\mu_n \subseteq \bar{K}$ denote the group of $n$-th roots of unity. We will work under the assumption that $\mu_n \subseteq K$.[1] From the short exact sequence

$$1 \longrightarrow \mu_n \hookrightarrow \bar{K}^* \xrightarrow{(\cdot)^n} \bar{K}^* \longrightarrow 1$$

we then obtain the long exact sequence

$$1 \longrightarrow \mu_n \hookrightarrow K^* \xrightarrow{(\cdot)^n} K^* \longrightarrow H^1(K, \mu_n) \longrightarrow H^1(K, \bar{K}^*) \longrightarrow H^1(K, \bar{K}^*) \longrightarrow \dots.$$

[1] There is not much harm in making this assumption as we are mainly interested in $n = 2$ anyway, in which case every number field satisfies the condition.

By Hilbert's Theorem 90[2] we have $H^1(K, \bar{K}^*) = 0$, and so we obtain the following lemma.

**Lemma 1.1.1.** *If $K$ is a field containing all $n$-th roots of unity, then*

$$H^1(K, \mu_n) \cong K^*/(K^*)^n.$$

Now, from the assumption that $E[n] \subseteq E(K)$, it follows that $E[n]$ and $\mu_n \times \mu_n$ are isomorphic as $G_K$-modules, and as a direct consequence we obtain the isomorphisms

$$H^1(K, E[n]) \xrightarrow{\sim} H^1(K, \mu_n \times \mu_n) \xrightarrow{\sim} H^1(K, \mu_n) \times H^1(K, \mu_n) \xrightarrow{\sim} K^*/(K^*)^n \times K^*/(K^*)^n.$$

Together with the injection $E(K)/nE(K) \hookrightarrow H^1(K, E[n])$ (see appendix A.2) this gives an injection

$$\iota : E(K)/nE(K) \hookrightarrow K^*/(K^*)^n \times K^*/(K^*)^n \tag{1.1}$$

The ultimate goal is to find the image of $\iota$. For this, we have two tasks. The first is to use local conditions to find a finite subgroup of $K^*/(K^*)^n \times K^*/(K^*)^n$ in which the image is contained, which we do in section 1.1.1. Secondly, in section 1.1.2, we will find an explicit description of the morphism $\iota$ that we can use to determine its image.

### 1.1.1 Local conditions

We will shortly prove theorem 1.1.4, which gives a finite subgroup of $K^*/(K^*)^n \times K^*/(K^*)^n$ in which the image of $\iota$ lies. To this end, we need two technical results. We follow Milne [Mil06, Chapter 4].

**Proposition 1.1.2.** *Let $E/K$ be an elliptic curve with discriminant $\Delta$. Let $\gamma \in H^1(K, E[n])$ such that the image of $\gamma$ in $H^1(K_v, E)$ is trivial for every place $v$ of $K$[3]. Then, for every finite place $v$ of $K$ that does not divide $n\Delta$ (i.e. $v(n\Delta) = 0$), there exists a finite unramified extension $\mathcal{L}$ of $K_v$ such that $\gamma$ maps to 0 in $H^1(\mathcal{L}, E[n])$.*

*Proof.* See proposition A.3.7 in appendix A. □

**Lemma 1.1.3.** *Let $K$ be a number field, let $v$ be a (normalised) finite place of $K$, and let $\mathcal{L}$ be an unramified extension of $K_v$. If $x \in K$ lies in $(\mathcal{L}^*)^n$ for some $n \geq 2$, then $v(x) \equiv 0 \mod n$.*

*Proof.* Since $\mathcal{L}$ is obtained from $K$ by first taking a completion with respect to a non-archimedean valuation and then an unramified extension, it has the same value group as $K$. The fact that $x$ is in $(\mathcal{L}^*)^n$ then immediately implies that $v(x)$ is the $n$-fold of an integer, or equivalently $v(x) \equiv 0 \mod n$. □

**Theorem 1.1.4.** *Let $n \in \mathbb{Z}_{\geq 2}$, let $K$ be a number field containing $\mu_n$, let $E/K$ be an elliptic curve with rational $n$-torsion and let $\Delta$ be the discriminant of $E$. Let $T$ be the set of finite primes of $K$ that do not divide $n\Delta$. Then the images of $\iota_1$ and $\iota_2$ are contained in the finite subgroup of $K^*/(K^*)^n$ consisting of elements that have trivial $v$-adic valuation for all $v \in T$.*

*Proof.* We write

$$\iota_1, \iota_2 : E(K)/nE(K) \hookrightarrow K^*/(K^*)^n$$

for the components of $\iota$. Recall that these can be defined as composite maps

$$\iota_1, \iota_2 : E(K)/nE(K) \longrightarrow H^1(K, E[n]) \rightrightarrows H^1(K, \mu_n) \xrightarrow{i_K^{-1}} K^*/(K^*)^n, \tag{1.2}$$

[2] See for example [Šaf63] for (a translation of) Hilbert's original proof of the same theorem in a different form. For a simple direct proof of the fact that $H^1(K, \bar{K}^*) = 0$, see theorem 6.2.1 in [NSW13].

[3] In other words, $\gamma$ lies in $\mathrm{Sel}_n(E/K)$.

where the second maps are postcomposition with one of the projection maps. Let $P \in E(K)/nE(K)$, and let $\gamma$ be one of the images of $P$ in $H^1(K, \mu_n)$ under the above maps (that is $\gamma = i_K(\iota_1(P))$ or $\gamma = i_K(\iota_2(P))$). By commutativity and exactness of the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/nE(K) & \xrightarrow{(1)} & H^1(K, E[n]) & \longrightarrow & H^1(K, E)[n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_v E(K_v)/nE(K_v) & \longrightarrow & \prod_v H^1(K_v, E[n]) & \longrightarrow & \prod_v H^1(K_v, E)[n] & \longrightarrow & 0, \end{array}$$

it follows that $\gamma$ satisfies the conditions of proposition 1.1.2. Let $v \in T$. By proposition 1.1.2 we may choose a finite unramified extension $\mathcal{L}$ of $K_v$ such that $\gamma$ maps to zero in $H^1(\mathcal{L}, \mu_n)$. Now note that we have the commutative square

$$\begin{array}{ccc} H^1(K, \mu_n) & \xrightarrow{i_K^{-1}} & K^*/(K^*)^n \\ \downarrow & & \downarrow \\ H^1(\mathcal{L}, \mu_n) & \xrightarrow{i_{\mathcal{L}}^{-1}} & \mathcal{L}^*/(\mathcal{L}^*)^n \end{array}$$

where the horizontal maps are the isomorphisms given in lemma 1.1.1. Since, by construction of $\mathcal{L}$, we have that $\gamma$ maps to 0 under the left vertical map, it follows that $i_K^{-1}(\gamma)$ maps to zero under the right vertical map. By lemma 1.1.3 we conclude that $v(i_K^{-1}(\gamma)) \equiv 0 \mod n$. □

As a special case we have the following well known result.

**Corollary 1.1.5.** *Let $E/\mathbb{Q}$ be an elliptic curve with $E[2] \subset E(\mathbb{Q})$. Let $S$ be the set of primes that dividing $2\Delta$, and define the finite subgroup $A = \langle S, -1\rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Then (1.1) induces an injection*

$$\iota : E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow A \times A.$$

### 1.1.2 Explicit description of the Weil pairing

Our goal of this section is to find an explicit description of $\iota$, which can be used to determine its image. In order to do this, we will define the Weil pairing.

**Definition 1.1.6.** *The Weil pairing*

$$\langle \cdot, \cdot \rangle : E[n] \times E[n] \longrightarrow \mu_n$$

*is defined as follows: given a point $P \in E[n]$, let $f \in \bar{K}(E)$ with $\operatorname{div}(f) = n(P) - n(O)$. Choose a point $Q$ with $[n]Q = P$, and $g \in \bar{K}(E)$ with*

$$\operatorname{div}(g) = [n]^*(P) - [n]^*(O) = \sum_{R \in E[n]} (Q + R) - (R).$$

*Since $f \circ [n]$ and $g^n$ have the same divisor, their quotient is a scalar, and so by redefining $f$ we may assume that $f \circ [n] = g^n$. For any point $S \in E[n]$ we define*

$$\langle S, P \rangle := \frac{g(X + S)}{g(X)} \in \mu_n,$$

*where $X$ is any point where this expression is defined.*

To make sense of this last definition, note that

$$\left(\frac{g(X+S)}{g(X)}\right)^n = \frac{g(X+S)^n}{g(X)^n} = \frac{(f \circ [n])(X+S)}{(f \circ [n])(X)} = \frac{f([n]X + O)}{f([n]X)} = 1,$$

hence indeed $\frac{g(X+S)}{g(X)} \in \mu_n$. The Weil pairing is moreover independent of the choice of $X$ (and hence well-defined), nondegenerate, alternating and bilinear, see e.g. [Sil09, Prop III.8.1] for a proof.

Recall that in order to construct the two maps

$$\iota_1, \iota_2 : E(K)/nE(K) \longrightarrow K^*/(K^*)^n.$$

we used an isomorphism $\phi : E[n] \xrightarrow{\sim} \mu_n \times \mu_n$. As we are free to choose this isomorphism, we define it as follows. We pick two generators $T_1, T_2 \in E[n]$, and set $\zeta := \langle T_1, T_2 \rangle \in \mu_n$. Define[4]

$$\phi : aT_1 + bT_2 \longmapsto (\zeta^a, \zeta^b).$$

From here on we fix such $T_1, T_2, \zeta$. Such a choice of a particular $\zeta$ also allows us to regard $E[n]$ as a $\mu_n$-module; we define

$$\zeta^c * P := cP.^5$$

Now, given a point $P = \zeta^a * T_1 + \zeta^b * T_2$ it follows that

$$\langle P, T_2 \rangle = \langle \zeta^a T_1, T_2 \rangle = \langle aT_1, T_2 \rangle = \langle T_1, T_2 \rangle^a = \zeta^a,$$

and consequently that

$$\phi(P) = (\langle P, T_2 \rangle, \langle P, T_1 \rangle).$$

Consequently, given the decomposition of $\iota_1, \iota_2$ in eq. (1.2), it follows that we can decompose $\iota_1$ as

$$E(K)/nE(K) \longrightarrow H^1(K, E[n]) \longrightarrow H^1(K, \mu_n) \longrightarrow K^*/(K^*)^n$$

$$P \longmapsto (\sigma \mapsto \sigma Q - Q) \longmapsto (\sigma \mapsto \langle \sigma Q - Q, T_2 \rangle) \longmapsto \iota_1(P)$$

and $\iota_2$ similarly. For $n = 2$ and $E$ in Weierstrass form we can use this to find explicit formulas for $\iota_1$ and $\iota_2$.[6]

**Proposition 1.1.7.** *Let $x_1, x_2, x_3 \in K$ and consider the elliptic curve $E : y^2 = (x - x_1)(x - x_2)(x - x_3)$. For brevity we write*

$$T_1 = (x_1, 0), \quad T_2 = (x_2, 0), \quad \text{and} \quad T_3 := T_1 + T_2 = (x_3, 0).$$

*Then the maps $\iota_1$ and $\iota_2$ are given by*

$$\iota_1 : (x, y) \mapsto \begin{cases} 1 & \text{if } (x, y) = O, \\ (x_1 - x_2)(x_3 - x_2) & \text{if } (x, y) = T_2, \\ x - x_2 & \text{else,} \end{cases} \qquad \iota_2 : (x, y) \mapsto \begin{cases} 1 & \text{if } (x, y) = O, \\ (x_2 - x_1)(x_3 - x_1) & \text{if } (x, y) = T_1, \\ x - x_1 & \text{else.} \end{cases}$$

*Proof.* Note that $f = x - x_2$ has divisor exactly $2(T_2) - 2(O)$. Moreover, with the function $g \in \bar{K}(E)$ as in definition 1.1.6, for any affine point $P = (x, y) \in E(K)$ with $P \neq T_1, T_2$ we have

$$\langle \sigma Q - Q, T_2 \rangle = \frac{g(Q + (\sigma Q - Q))}{g(Q)} = \frac{g(\sigma Q)}{g(Q)} = \frac{\sigma g(Q)}{g(Q)} = \frac{\sigma \sqrt{f([2]Q)}}{\sqrt{f([2]Q)}} = \frac{\sigma \sqrt{f(P)}}{\sqrt{f(P)}} = \frac{\sigma \sqrt{x - x_2}}{\sqrt{x - x_2}}. \quad (1.3)$$

As the map $\sigma \mapsto \frac{\sigma \sqrt{x - x_2}}{\sqrt{x - x_2}}$ is clearly equal to the image of $x - x_2$ under the isomorphism $i_K$ from lemma 1.1.1 it follows that $\iota_1(P)$ must equal $x - x_2$. Similarly $\iota_2(P) = x - x_1$. Since we know that both $\iota_1$ and $\iota_2$ are group isomorphisms, the given formula follows. □

We will now demonstrate how theorem 1.1.4 and proposition 1.1.7 together can be used to determine the rank of an elliptic curve with rational torsion.

[4] Note that by non-degeneracy of the Weil pairing $\zeta$ is a primitive root of unity, and so this map is indeed an isomorphism.
[6] Using Miller's algorithm one can do the same for general values of $n$. See [Sil09, Chapter XI.8] for details.

### 1.1.3 Example: $D_0$

We completely solve Diophantus' exercise for $m = 0$, by finding all rational points on

$$D_0 : -y^2 = x^3 - x$$

By the coordinate transformation $(x, y) \mapsto (-x, y)$ we see that this curve is isomorphic to $E : y^2 = x^3 - x$, which has the rational 2-torsion points $(0, 0), (1, 0), (-1, 0)$ and discriminant $\Delta = 64$. It follows that $E(\mathbb{Q})/2E(\mathbb{Q})$ injects into $\{\pm 1, \pm 2\}^2$. We take $T_1 = (0, 0)$ and $T_2 = (1, 0)$.

The image of the torsion points is as follows:

- The point $O$ maps to $(1, 1)$.
- The point $T_1 = (0, 0)$ maps to $(-1, -1)$.
- The point $T_2 = (1, 0)$ maps to $(1, 2)$
- The point $T_3 = (-1, 0)$ maps to $(-1, -2)$.

For each remaining pair $(b_1, b_2) \in \{\pm 1, \pm 2\}^2$ we thus have to check whether it lies in the image of $\iota$, or equivalently whether there exist $P = (x, y) \in E(\mathbb{Q})$ and $z, w \in \mathbb{Q}$ with $b_1 z^2 = x - x_1$ and $b_2 w^2 = x - x_2$ (where $x_1 = 0$ and $x_2 = 1$). The system we have to solve is thus

$$\begin{cases} b_1 z^2 = x \\ b_2 w^2 = x - 1 \\ y^2 = x^3 - x. \end{cases}$$

A trivial but useful observation is that if a pair $(b_1, b_2)$ does lie in the image and a pair $(c_1, c_2)$ does not, then $(b_1 c_1, b_2 c_2)$ also does not. This drastically reduced the required work as we will see shortly.

- For $(b_1, b_2) = (2, 1)$ we get

$$\begin{cases} 2z^2 = x \\ w^2 = x - 1 \\ y^2 = x^3 - x. \end{cases}$$

  Let $v = \mathrm{ord}_2$. Note that since $x = 2z^2$, $v(x)$ must be odd.

  - If $v(x) < 0$, then

$$v(x - 1) \geq \min(v(x), v(-1)) = \min(v(x), 0)) = v(x),$$

    and since $v(x) \neq v(-1) = 0$ the above inequality is in fact an equality, and we find that $v(x - 1) = v(x)$. However, from the first two equations we see that $v(x)$ is odd and $v(x - 1)$ is even, which is a contradiction.
  - If $v(x) > 0$, then similarly we get

$$v(x - 1) \geq \min(v(x), v(-1)) = \min(v(x), 0)) = 0,$$

    and by the same argument $v(x + 1) = 0$. Hence

$$v(y^2) = v(x^3 - x) = v(x) + v(x - 1) + v(x + 1) = v(x)$$

    which shows that $v(x)$ is even, which is again a contradiction.

  We conclude there are no solutions and so $(b_1, b_2) = (2, 1)$ does not lie in the image of $\iota$. As a consequence, $(-2, -1), (2, 2)$ and $(-2, -2)$ also do not lie in the image.

- For $(b_1, b_2) = (-1, 1)$ we get

$$\begin{cases} -z^2 = x \\ w^2 = x - 1 \\ y^2 = x^3 - x. \end{cases}$$

  In particular, $x$ is negative and $x - 1$ is positive, which is a contradiction. Hence $(-1, 1)$ does not lie in the image, and neither do $(1, -1), (-1, 2)$ and $(1, -2)$.

- Note that the argument for $(b_1, b_2) = (-1, 1)$ holds whenever $b_1$ is negative and $b_2$ is positive. In particular we can also exclude $(-2, 1)$, and consequently also $(2, -1), (-2, 2)$ and $(2, -2)$.

In conclusion, of the sixteen points in $\{\pm 1, \pm 2\}^2$, four do lie in the image (namely the images of the torsion points), and the remaining twelve do not. We conclude that

$$\iota\left(E(\mathbb{Q})/2E(\mathbb{Q})\right) = \{(1,1), (-1,-1), (1,2), (-1,-2)\}.$$

Since this is already the image of the 2-torsion subgroup, it follows that $E(\mathbb{Q})$ has rank 0, and that the only rational points on $E$ are

$$E(\mathbb{Q}) = \{\mathcal{O}, (0,0), (1,0), (-1,0)\}$$

## 1.2 Irrational 2-torsion

For a generic member $E$ of the Diophantus family, the Galois module $E[2]$ is irreducible over $K$, and so the methods of section 1.1 do not apply. In this section, we give a cohomological interpretation of the method of 2-descent in the case where $E[2]$ is irreducible. We construct a short exact sequence

$$0 \longrightarrow E[2] \longrightarrow V \longrightarrow \mu_2 \longrightarrow 0$$

where $V = \mathrm{Ind}_L^K(\mu_2)$ is induced from the trivial representation of the cubic field $L$ obtained by adjoining the coordinates of a 2-torsion point. Using Shapiro's lemma, we extract an injection

$$E(K)/2E(K) \hookrightarrow \mathrm{Ker}\left(L^\times/(L^\times)^2 \xrightarrow{\mathrm{N}_{L/K}} K^\times/(K^\times)^2\right).$$

To describe this map explicitly, we investigate the isomorphism of Shapiro's lemma in §1.2.1. The method of 2-descent is described in §1.2.2 and illustrated on the Diophantus curve $D_6$ in §1.2.3. In chapter 2, an implementation of this method is used to obtain statistical rank data on the family $D_m$.

### 1.2.1 Shapiro's lemma

In this section we let $G$ be a group and $H \subseteq G$ a subgroup of finite index. Shapiro's lemma on induced modules provides, for every $H$-module $M$, a canonical isomorphism

$$H^1(G, \mathrm{Ind}_H^G(M)) \xrightarrow{\sim} H^1(H, M).$$

The main goal of this section is to explicitly describe the *inverse* of this isomorphism.

Let $\{g_i\}_{i\in I}$ be a set of coset representatives of $H$, i.e. $G = \coprod_{i\in I} g_i H$, where without loss of generality we assume $1 \in I$ and $g_1 = 1$. For $\sigma \in G$ and $i \in I$ we define $\sigma(i) \in I$ and the map $h_i : G \to H$ by

$$\sigma g_i = g_{\sigma(i)} h_i(\sigma).$$

That is, $\sigma g_i = g_j h$ for some $h \in H$. We define $\sigma(i) := j$ and $h_i(\sigma) := h$.

**Remark 1.2.1.** *Note that if $\sigma \in H$, then since $\sigma g_1 = \sigma = g_1 \sigma$ it follows that*

$$\sigma(1) = 1 \qquad \textit{and} \qquad h_1(\sigma) = \sigma.$$

Note that since the definition of $h_i$ depends on the choice of elements $g_i$ there is no reason for the $h_i$ to be homomorphisms. This indeed is not always the case.[7] We do however have the following property.

**Lemma 1.2.2.** *For any $\sigma, \tau \in G$, $i \in I$ we have*

$$\sigma(\tau(i)) = (\sigma\tau)(i) \qquad \textit{and} \qquad h_i(\sigma\tau) = h_{\tau(i)}(\sigma) h_i(\tau).$$

[7] A rare case in which this happens is for example when $G = H \times X$ and when one takes $I = \{1\} \times X$ and $g_i = (1, i)$ for all $i \in X$. In this case all the $h_i$ are equal to the projection map $H \times X \to H$.

*Proof.* This follows very quickly from the equalities

$$\begin{aligned} g_{(\sigma\tau)(i)}h_i(\sigma\tau) &= (\sigma\tau)g_i \\ &= \sigma(\tau g_i) \\ &= \sigma(g_{\tau(i)}h_i(\tau)) \\ &= (\sigma g_{\tau(i)})h_i(\tau) \\ &= g_{\sigma(\tau(i))}h_{\tau(i)}(\sigma)h_i(\tau). \end{aligned}$$

□

Using the maps $\{h_i\}_i$ we can now define our object of interest, namely induced modules.

**Definition 1.2.3.** *Let $M$ be a (left) $H$-module. The **induced $G$-module** of $M$ is the abelian group*

$$\mathrm{Ind}_H^G(M) := \bigoplus_{i\in I}[g_i]\cdot M,$$

*where the action of $G$ is defined by linearly extending the rule*

$$\sigma\cdot[g_i]m := [g_{\sigma(i)}](h_i(\sigma)m). \tag{1.4}$$

The module $\mathrm{Ind}_H^G$ can alternatively be defined as the tensor product $\mathbb{Z}G\otimes_{\mathbb{Z}H}M$ with the natural $G$-action. Note that eq. (1.4) indeed defines a group action, as for any $\sigma,\tau\in G$ and any $g_im$ we have

$$\begin{aligned} \sigma\cdot(\tau\cdot[g_i]m) &= \sigma\cdot[g_{\tau(i)}](h_i(\tau)m) \\ &= [g_{\sigma(\tau(i))}]h_{\tau(i)}(\sigma)h_i(\tau)m \\ &= [g_{(\sigma\tau)(i)}]h_i(\sigma\tau)m \\ &= (\sigma\tau)\cdot[g_i]m, \end{aligned}$$

where we used both statements of lemma 1.2.2 in the third equality. We are now able to formulate the main theorem of this section, which is *Shapiro's lemma*. It concerns a certain restriction map

$$S : H^1(G,\mathrm{Ind}_H^G(M)) \to H^1(H,M),$$

which is defined by taking a cocycle $\phi : G\to \mathrm{Ind}_H^G(M)$ of a class $[\phi]$, projecting to its 1-component $\phi_1 : G\to [g_1]M = M$ of $\phi$, and restricting it to $H$ to obtain a representative of $S([\phi])$.

**Theorem 1.2.4.** *With $G, H$ and $M$ as before, the restriction map*

$$S : H^1(G,\mathrm{Ind}_H^G(M)) \longrightarrow H^1(H,M)$$

*is an isomorphism, and its inverse is given by the map*

$$T : H^1(H,M) \longrightarrow H^1(G,\mathrm{Ind}_H^G(M))$$

*that sends a cohomology class $[\psi]$ with representative $\psi : H\to M$ to the cohomology class of the map*

$$\begin{aligned} G &\longrightarrow \mathrm{Ind}_H^G(M) \\ \sigma &\longmapsto \sum_{i\in I}[g_i]\psi(h_{\sigma^{-1}(i)}(\sigma)) \end{aligned}$$

We will give a direct proof in appendix B.

### 1.2.2 Back to elliptic curves

The main goal of this section is to prove theorem 1.2.6 and theorem 1.2.7, which together give us the tools necessary to perform the irrational 2-descent.

Let $E$ be an elliptic curve that has no non-trivial $K$-rational 2-torsion points. Without loss of generality, we write

$$E : y^2 = f(x) = (x - \alpha)(x - \beta)(x - \gamma),$$

where $\alpha, \beta, \gamma$ all generate a cubic extension of $K$ (these extensions need not be the same however). Let $L := K(\alpha)$, and denote

$$G := G_K \qquad \text{and} \qquad H := G_L \subseteq G_K.$$

Note that as we have no reason to assume that $L$ is Galois over $K$, $H$ may not be normal in $G$. We now view $\mu_2$ as a trivial $H$-module, and we define

$$W := \mathrm{Ind}_H^G(\mu_2).$$

Note that $G/H$ has size 3, and the three classes correspond to the different possible images of $\alpha$ under the automorphisms in $G_K$. Hence, $W$ has a $\mu_2$-basis given by $([\alpha \mapsto \alpha], [\alpha \mapsto \beta], [\alpha \mapsto \gamma])$, and the action of $G$ is given by

$$\sigma[\alpha \mapsto x] = [\alpha \mapsto \sigma(x)].$$

It follows that $W$ as a $G$-module is thus isomorphic to

$$V := \bigoplus_{i=1,2,3} \mu_2 T_i$$

equipped with the obvious action that extends the action on $E[2]$. It is this $G$-module that we will use in the descent. Note that there is a short exact sequence[8]

$$0 \longrightarrow E[2] \xrightarrow{a} V \xrightarrow{b} \mu_2 \longrightarrow 0, \tag{1.5}$$

with maps $a$ and $b$ defined by

$$a(P) = \sum_{i=1}^{3} \langle P, T_i \rangle * T_i, \qquad \text{and} \qquad b\left(\sum_{i=1}^{3} \lambda_i T_i\right) = \prod_{i=1}^{3} \lambda_i.$$

As usual, we get a long exact sequence

$$0 \longrightarrow H^0(K, E[2]) \longrightarrow H^0(K, V) \longrightarrow H^0(K, \mu_2)$$
$$\longrightarrow H^1(K, E[2]) \longrightarrow H^1(K, V) \longrightarrow H^1(K, \mu_2) \longrightarrow \dots.$$

**Lemma 1.2.5.** *The map $H^1(K, E[2]) \longrightarrow H^1(K, V)$ is injective.*

*Proof.* Note that since $E[2]$ is irreducible, we have $H^0(K, E[2]) = 0$. Hence the map $H^0(K, V) \to H^0(K, \mu_2)$ is injective. Since both $H^0(K, V)$ and $H^0(K, \mu_2)$ have size 2 (the former is given by $\{0, T_1 + T_2 + T_3\}$), it is thus also surjective. The map $H^0(K, \mu_2) \to H^1(K, E[2])$ is hence 0, so since the kernel of $H^1(K, E[2]) \to H^1(K, V)$ is the image of $H^0(K, \mu_2) \to H^1(K, E[2])$, the former is injective. □

[8] The fact that this sequence is exact is a short (finite) computation, most of which can be directly deduced from the fact that $\langle \cdot, \cdot \rangle$ is non-degenerate.

We hence obtain the following diagram.

$$\begin{array}{ccccc} E(K)/2E(K) & \hookrightarrow & H^1(K,E[2]) & \hookrightarrow & H^1(K,V) \twoheadrightarrow H^1(K,\mu_2) \\ & \searrow^{\iota} & & & \downarrow \wr \qquad \downarrow \wr \\ & & & & H^1(L,\mu_2) \\ & & & & \downarrow \wr \\ & & & & L^*/(L^*)^2 \dashrightarrow K^*/(K^*)^2 \end{array} \tag{1.6}$$

The map $H^1(K,V) \longrightarrow H^1(L,\mu_2)$ is the restriction map described in theorem 1.2.4, and the other two vertical maps are the isomorphisms from lemma 1.1.1. As counterpart of the descriptions of $\iota_1$ and $\iota_2$ given in section 1.1.2 for the case of rational 2-torsion, for completely irrational 2-torsion we obtain the following result.

**Theorem 1.2.6.** *The diagonal map $\iota : E(K)/2E(K) \longrightarrow L^*/(L^*)^2$ in the diagram above is given by*

$$O \longmapsto 1 \qquad \text{and} \qquad (x,y) \longmapsto x - \alpha.$$

*Proof.* Starting with a point $P = (x,y) \in E(K)/2E(K)$, its image in $H^1(K,E[2])$ is the class of the cocycle $\sigma \mapsto (\sigma Q - Q)$, where $nQ = P$. Its image in $H^1(K,V)$ is given by

$$\sigma \longmapsto \sum_{i=1}^{3} \langle \sigma Q - Q, T_i \rangle * T_i$$

which, under the isomorphism provided by Shapiro's lemma, gets mapped to

$$\tau \longmapsto \langle \tau Q - Q, T_1 \rangle.$$

By the same reasoning as in section 1.1.2, this last term equals $\frac{\tau\sqrt{x-\alpha}}{\sqrt{x-\alpha}}$, which is also the image of the class $[x-\alpha]$ under the isomorphism $i_K : L^*/(L^*)^2 \to H^1(L,\mu_2)$ provided by Kummer theory. □

The second result of this section considers the composite map $L^*/(L^*)^2 \longrightarrow K^*/(K^*)^2$ shown in eq. (1.6). When asking ourselves what this map is, an obvious candidate is the norm map $N_{L/K}$, first and foremost since it is hard to come up with a homomorphism $L^*/(L^*)^2 \longrightarrow K^*/(K^*)^2$ in the first place. As a sanity check, we can quickly check whether $N_{L/K}$ makes the above diagram commute when it is restricted to the image of $\iota$. Of course, by exactness of the top row in eq. (1.6), the image of any $P \in E(K)/2E(K)$ in $K^*/(K^*)^2$ must be trivial. Moreover, it can be easily seen that any number $\iota(P) \in L^*/(L^*)^2$ in the image of $\iota$ has $K$-norm that is (up to a square) also trivial. Namely, as argued at the start of the section, the cosets of $G/H$ correspond to the different images of $\alpha$, which may be $\alpha$, $\beta$ and $\gamma$. Hence, using the Weierstrass equation $E : y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ we find that

$$N_{L/K}(\iota(P)) = N_{L/K}(x-\alpha) = (x-\alpha)(x-\beta)(x-\gamma) = y^2,$$

which indeed is trivial in $K^*/(K^*)^2$. This reinforces the idea that the composite map indeed is $N_{L/K}$, and indeed we are able to prove the following theorem.

**Theorem 1.2.7.** *The composite map $L^*/(L^*)^2 \longrightarrow K^*/(K^*)^2$ is the norm map $N_{L/K}$.*

*Proof.* Since the inverse of the Kummer maps

$$\iota_K : K^*/(K^*)^2 \longrightarrow H^1(K,\mu_2) \qquad \text{and} \qquad \iota_L : L^*/(L^*)^2 \longrightarrow H^1(L,\mu_2)$$

is difficult to work with, the easiest way to prove the theorem is by showing that the following diagram is commutative:

$$\begin{array}{ccc} H^1(K,V) & \longrightarrow & H^1(K,\mu_2) \\ \wr\uparrow & & \\ H^1(L,\mu_2) & & \wr\uparrow \\ \wr\uparrow & & \\ L^*/(L^*)^2 & \xrightarrow{N_{L/K}} & K^*/(K^*)^2 \end{array}$$

For $i = 1, 2, 3$ we let $g_i \in G_K$ and $h_i : G_K \to G_L$ as in section 1.2.1. Starting with an $x \in L^*/(L^*)^2$ we see that along the top path $x$ gets mapped via

$$\begin{array}{ccccccc} x & \longmapsto & \left(\sigma \mapsto \frac{\sigma\sqrt{x}}{\sqrt{x}}\right) & \longmapsto & \left(\sigma \mapsto \sum_{i=1}^3 \left(\frac{h_{\sigma^{-1}(i)}(\sigma)\sqrt{x}}{\sqrt{x}}\right) * T_i\right) & \longmapsto & \left(\sigma \mapsto \prod_{i=1}^3 \frac{h_i(\sigma)\sqrt{x}}{\sqrt{x}}\right) \\ \cap & & \cap & & \cap & & \cap \\ L^*/(L^*)^2 & & H^1(L,\mu_2) & & H^1(K,V) & & H^1(K,\mu_2). \end{array}$$

Using that $N_{L/K}(x) = g_1(x)g_2(x)g_3(x)$, it follows that along the bottom path $x$ gets mapped via

$$\begin{array}{ccccc} x & \longmapsto & N_{L/K}(x) = \prod_{i=1}^3 g_i(x) & \longmapsto & \left(\sigma \mapsto \prod_{i=1}^3 \frac{\sigma\sqrt{g_i x}}{\sqrt{g_i x}}\right) \\ \cap & & \cap & & \cap \\ L^*/(L^*)^2 & & K^*/(K^*)^2 & & H^1(K,V). \end{array}$$

It thus remains to show that for all $\sigma \in G_K$ we have

$$\prod_{i=1}^3 \frac{h_i(\sigma)\sqrt{x}}{\sqrt{x}} \stackrel{?}{=} \prod_{i=1}^3 \frac{\sigma\sqrt{g_i x}}{\sqrt{g_i x}}. \tag{1.7}$$

Note that since $h_i(\sigma)$ fixes $L$, we have that

$$\left(\frac{h_i(\sigma)\sqrt{x}}{\sqrt{x}}\right)^2 = \frac{h_i(\sigma)x}{x} = 1,$$

and so $\frac{h_i(\sigma)\sqrt{x}}{\sqrt{x}} = \pm 1$. This in turn implies that any element of $G_K$ acts trivially on this fraction, which allows us to rewrite the left hand side of eq. (1.7) as

$$\prod_{i=1}^3 \frac{h_i(\sigma)\sqrt{x}}{\sqrt{x}} = \prod_{i=1}^3 g_{\sigma(i)} \frac{h_i(\sigma)\sqrt{x}}{\sqrt{x}} = \prod_{i=1}^3 \frac{g_{\sigma(i)} h_i(\sigma)\sqrt{x}}{g_{\sigma(i)}\sqrt{x}} = \prod_{i=1}^3 \frac{\sigma g_i \sqrt{x}}{g_{\sigma(i)}\sqrt{x}},$$

where we used that by definition $h_i(\sigma) = g_{\sigma(i)}^{-1} \sigma g_i$ (see the start of section 1.2.1). Using this, we find that eq. (1.7) is equivalent with

$$\prod_{i=1}^3 \frac{\sigma g_i \sqrt{x}}{g_{\sigma(i)}\sqrt{x}} \stackrel{?}{=} \prod_{i=1}^3 \frac{\sigma\sqrt{g_i x}}{\sqrt{g_i x}}$$

which by simply rearranging we see is equivalent to

$$\prod_{i=1}^3 \frac{\sigma g_i \sqrt{x}}{\sigma\sqrt{g_i x}} \stackrel{?}{=} \prod_{i=1}^3 \frac{g_{\sigma(i)}\sqrt{x}}{\sqrt{g_i x}}. \tag{1.8}$$

Now since each fraction $\frac{g_i\sqrt{x}}{\sqrt{g_i x}}$ squares to 1, $\sigma$ acts trivially and so the left hand side equals $\prod_{i=1}^3 \frac{g_i\sqrt{x}}{\sqrt{g_i x}}$. Moreover, since $\sigma$ only permutes the indices 1, 2 and 3, the right hand side of eq. (1.8) also equals $\prod_{i=1}^3 \frac{g_i\sqrt{x}}{\sqrt{g_i x}}$. This proves that eq. (1.7) holds, and hence we are done. □

The final result of this section concerns the following analogue of theorem 1.1.4.

**Theorem 1.2.8.** *Let $E/K$ be an elliptic curve with $K$-irrational $n$-torsion, define $L$ as before and let $\Delta$ be the discriminant of $E$. Let $T$ be the set of finite primes of $L$ that do not divide $n\Delta$. Then the image of $\iota : E(K)/nE(K) \longrightarrow L^*/(L^*)^n$ is contained in the finite subgroup of $L^*/(L^*)^n$ consisting of elements that have trivial $v$-adic valuation mod $n$ for all $v \in T$.*

*Proof.* Let $P \in E(K)/nE(K)$, let $\gamma$ be the image of $P$ in $H^1(K, E[2])$, and let $v \in T$. Our goal is to show that $v(\iota(P)) \equiv 0 \mod n$. By proposition A.3.7 we may choose a finite unramified extension $\mathcal{M}$ of $L_v$ such that $\gamma$ maps to zero in $H^1(\mathcal{M}, E[n])$. Now note that we have the commutative diagram

$$\begin{array}{ccccc} H^1(K, E[n]), & \longrightarrow & H^1(L, \mu_n) & \xrightarrow{i_L^{-1}} & L^*/(L^*)^n \\ \downarrow & & \downarrow & & \downarrow \\ H^1(\mathcal{M}, E[n]) & \longrightarrow & H^1(\mathcal{M}, \mu_n) & \xrightarrow{i_{\mathcal{M}}^{-1}} & \mathcal{M}^*/(\mathcal{M}^*)^n. \end{array}$$

Here the horizontal arrows on the left both send a cocycle $\sigma$ to the composition $\mathrm{pr}_1 \circ \sigma$ of $\sigma$ with the projection on the first coordinate. Since $\gamma$ maps to zero in $H^1(\mathcal{M}, E[n])$, it maps to zero in $\mathcal{M}^*/(\mathcal{M}^*)^n$, and so by commutativity $\iota(P)$ does as well. By lemma 1.1.3 this gives us the required result. □

In the following section we will show how theorem 1.2.6, theorem 1.2.7, and theorem 1.2.8 together can be used to perform a descent on the Diophantus curve $D_6$.

### 1.2.3 Example: Diophantus' exercise $D_6$

Recall that $D_6/\mathbb{Q}$ is the elliptic curve given by the Weierstrass equation

$$D_6 : y(6 - y) = x^3 - x.$$

By a simple coordinate transformation it follows that $D_6$ is isomorphic to

$$E : y^2 = x^3 - 16x + 16 \cdot 36,$$

and it is the rank of this curve that we will calculate. Recall that we already know a rank 2 subgroup generated by $(4, 4 \cdot 6)$ and $(-4, 4 \cdot 6)$. Since a brute-force search does not yield any other points, it is reasonable to suspect that the rank is indeed 2, and so we will try to prove this. We will use Sage to do the routine calculations that are necessary. Let $\alpha$ be a zero of $x^3 - 16x + 16 \cdot 36$. We have the following data.

- The conductor of $E$ equals $2^2 \cdot 37 \cdot 59$.
- The unit group of $\mathcal{O}_L$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, generated by $u = (\alpha/4)^2 - 5$ and $-1$.
- The class group of $L$ has order 2 and is generated by the fractional ideal $\mathfrak{c}_3 = (3, \alpha/4 + 1)$.
- The ideal (2) is inert in $\mathcal{O}_L$, and (37) and (59) factor as

$$(37) = (37, \alpha/4 + 5)^2 \cdot (37, \alpha/4 - 10) = \mathfrak{p}_{37}^2 \mathfrak{q}_{37},$$
$$(59) = (59, \alpha/4 + 16)^2 \cdot (59, \alpha/4 + 27) = \mathfrak{p}_{59}^2 \mathfrak{q}_{59}.$$

It turns out all of these ideals are actually principal, as we have

$$\mathfrak{p}_{37} = (\alpha^2/16 - \alpha/2 + 2) = (g_{37}), \qquad \mathfrak{q}_{37} = (\alpha^2/16 - 3\alpha/4 + 4) = (h_{37}),$$
$$\mathfrak{p}_{57} = (\alpha^2/16 + \alpha/4 - 4) = (g_{59}), \qquad \mathfrak{p}_{57} = (\alpha^2/16 + 3\alpha/4 + 1) = (h_{59}).$$

From now on, we call the primes $2, \mathfrak{p}_{37}, \mathfrak{q}_{37}, \mathfrak{p}_{59}, \mathfrak{q}_{59}, \mathfrak{c}_3$ the *bad primes*, and we call the others good.

Let $x \in L^*$ be a lift of a point $\iota(P) \in L^*/(L^*)^2$ in the image of $\iota$. We will now change $x$ by squares to make it as simple as possible.

Let $\mathfrak{q}$ be a prime ideal that is not $\mathfrak{c}_3$ for which $v_\mathfrak{q}$ is non-zero. If $\mathfrak{q}$ is principal (say equal to $(z)$), we can multiply $x$ by an appropriate even power of $z$ to make $v_\mathfrak{q}(x)$ equal to 0 or 1, without changing any other valuation. If $\mathfrak{q}$ is not principal, then $\mathfrak{q}\mathfrak{c}_3^{-1}$ *is* principle (say $(z)$), so we can again change $x$ by an even

power of $z$ to make $v_{\mathfrak{q}}(x)$ equal to 0 or 1, while only changing the valuation of $\mathfrak{c}_3$. After performing this procedure for every prime for which $x$ had a non-zero valuation, the valuation at every good prime that is not $\mathfrak{c}_3$ is identically zero, since those started out as even. We can thus assume that $x$ is an element of $L^*$ which has valuation 0 or 1 at all the bad primes, 0 at all good primes, and which moreover has squared norm. We calculate that

$$\mathfrak{c}_3^2 = (\alpha/4 + 1) =: (c_3).$$

Taking all this toghether, it follows that $x$ must lie in the subgroup of $L^*/(L^*)^2$ generated by

$$-1, \quad u, \quad 2, \quad g_{37}h_{37}, \quad g_{59}h_{59}, \quad \text{and} \quad c_3.$$

Starting with the points $\alpha + 4$ and $\alpha - 4$ that are trivially in the image (as we know the points $(4, 4 \cdot 6)$ and $(-4, 4 \cdot 6)$). We calculate the valuations of these numbers at all relevant primes. Our findings are that both $4 + \alpha$ and $4 - \alpha$ have valuation 2 at the prime (2), and valuation 0 at all of $\mathfrak{p}_{37}, \mathfrak{q}_{37}, \mathfrak{p}_{59}, \mathfrak{q}_{59}, \mathfrak{c}_3$. Using this and some bruteforce computations, we find the factorisations

$$\alpha - 4 = 1/u \cdot (-\alpha/4 - 2)^2 \cdot 2^2 \qquad \text{and} \qquad \alpha + 4 = c_3 \cdot 2^2.$$

In particular, $u$ and $c_3$ (and $uc_3$) are in the image. It thus remains to find out whether any of the remaining 15 values given by

$$-1, \quad 2, \quad g_{37}h_{37}, \quad \text{and} \quad g_{59}h_{59}$$

and their (non-empty) products are in the image. Let $\gamma$ be such a product. This means that we want to find out whether there is a point $P = (x, y)$ on $E$ such that $x - \alpha$ can be written as $\gamma \cdot w^2$ for some $w \in L$. Writing $w = f + g\alpha + h\alpha^2$, this means that we need to solve a system of equations of the form

$$\begin{cases} y^2 & = x^3 - 16x + 16 \cdot 36 \\ x & = \text{homogeneous degree 2 polynomial in } f, g, h, \\ -1 & = \text{homogeneous degree 2 polynomial in } f, g, h, \\ 0 & = \text{homogeneous degree 2 polynomial in } f, g, h. \end{cases}$$

It should be noted that this is the hard part; there exists no known algorithm which decides whether a given variety over $\mathbb{Q}$ has a rational point.[9] As an example, we show how to proceed for $\gamma = g_{37}h_{37}$. In this case, the last equation is given by

$$(13/16)f^2 - 14fg + 66g^2 + 132fh - 1160gh + 5088h^2 = 0, \tag{1.9}$$

which defines a (projective) conic. This conic is isomorphic to the conic given by

$$(13/16)a^2 + (74/13)b^2 - 296c^2 = 0. \tag{1.10}$$

We will show that eq. (1.10) has no solutions. Given such a solution, by clearing denominators we may assume that $a, b$, and $c$ are coprime integers. Since 74 and 296 are divisible by 37, it follows that $a$ must be divisible by 37 as well. In particular, we can divide by 37 and reduce modulo 37 to obtain

$$(2/13)b^2 - 8c^2 \equiv 0 \mod 37. \tag{1.11}$$

Since $8/(2/13) \equiv 15 \mod 37$ is not a square modulo 37, it follows that both $b$ and $c$ must be divisible by 37, which contradicts the coprimality of $a, b$ and $c$. Hence eq. (1.11) has no solutions, and so neither has eq. (1.9). Hence $\gamma = g_{37}h_{37}$ indeed does not lie in the image of $\iota$.

In a similar manner, it is possible to exclude all remaining values. This allows us to conclude that the rank of $E$ (and hence also of $D_6$) is indeed equal to 2.

To finalize, it should be noted that we have not yet proven that $D_6(\mathbb{Q})$ is indeed generated by the two points $(4, 24), (-4, 24)$, just that these points generate a subgroup of finite index in $D_6(\mathbb{Q})$. Since only multiples of integer points can be integer points (assuming an integer model), the search for actual generators of $D_6(\mathbb{Q})$ is in this case a finite computation, which indeed shows that $D_6(\mathbb{Q})$ is generated by $(4, 24)$ and $(-4, 24)$.

[9] The corresponding problem of for $\mathbb{Z}$ is known as Hilbert's tenth problem, and by the MRDP theorem is known to be undecidable [MPD93].

# Chapter 2

# The family of Diophantus

In this chapter, we return to Diophantus's family of elliptic curves given by the equations

$$D_m : y(m - y) = x^3 - x,$$

where $m \in \mathbb{N}$ is an integer. As mentioned in the introduction, it is notable that (at least for low values of $m$) many curves in this family have high rank, and we see more curves of rank 4 than curves of rank 2. One of the main goals of this chapter is to investigate these ranks further? This family was studied by Brown–Ezra [BM02], where it was proven that there are infinitely many values $m$ for which $D_m$ has rank at least 3. Later investigations in [Eik04] generalised this approach and showed the same for curves of rank at least 5.

We start in section 2.1 with a discussion on analytic ranks, and their relevance in the computation of algebraic ranks. In section 2.2 we discuss torsion and the generic rank of the family. In section 2.3 we investigate our data to see how it compares with expected heuristics. Lastly, in section 2.4, we briefly discuss the result of Eikenberg considering infinite subfamilies of high generic rank.

## 2.1 Notes on computation

In chapter 1 we discussed how one can use the method of 2-descent to calculate the rank of an elliptic curve. Since mathematicians rarely have the time to perform these descents by hand, computers are used in practice. We will briefly discuss some of the available implementations. First, however, we highlight a different method of calculating ranks, based on the BSD-conjecture.

### 2.1.1 The Birch–Swinnerton-Dyer conjecture

The Birch and Swinnerton-Dyer conjecture, or BSD for short, concerns the $L$-function of an elliptic curve[1]. Let $E/\mathbb{Q}$ be an elliptic curve, and assume we have some minimal integral Weierstrass model for $E$. For every prime $p$ we can look at the reduction $\tilde{E}$ of $E$ modulo $p$ and count the number of points $N_p$ in $\tilde{E}(\mathbb{F}_p)$ and set $a_p = p + 1 - N_p$. [2] The local $L$-function $L_p(E, s)$ at a prime $p$ in the complex variable $s$ is then defined as [3]

$$L_p(E,s) := \begin{cases} 1 - a_p p^{-s} + p^{1-2s} & \text{if } E \text{ has good reduction at } p, \\ 1 - p^{-s} & \text{if } E \text{ has split multiplicative reduction at } p, \\ 1 + p^{-s} & \text{if } E \text{ has nonsplit multiplicative reduction at } p, \\ 1 & \text{if } E \text{ has additive reduction at } p, \end{cases}$$

[1] The conjecture can be stated over any number field, but we will restrict to $\mathbb{Q}$.

[2] Hasse's theorem (see [Sil09, Theorem V.1.1]) tells us that $|N_p - (p + 1)| \leq 2\sqrt{p}$. The value $a_p$ hence measures the deviation from the expected value $p + 1$. In practice, the values $a_p$ are computable in time a time that is polynomial in $\log(p)$, see [Coh93, 7.4.12] and the references therein.

[3] The expressions for these factors look fairly mysterious, and can be thought of as a result instead of as a definition. Namely, the $L$-function can also be defined in terms of the more primitive zeta function $\zeta(E, s)$, from which the given expressions can be derived. We refer to [Mil06, Chapter IV.10] for details.

and the $L$-function $L(E, s)$ of $E$ is defined by

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

As a consequence of Hasse's theorem this function converges on the half plane $\{s \in \mathbb{C} : \text{Re } s > 3/2\}$ and is analytic on this domain. Moreover, it can be shown that $L(E, s)$ has an analytic continuation to the entirety of $\mathbb{C}$, and that it satisfies a functional equation. To be precise, we let $N_E$ be the conductor of $E$, we let $\Gamma(s) = \int_0^\infty t^{s-1}e^{-t}\, dt$ denote the gamma function, and we define

$$\Lambda(E, s) = N_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E, S). \tag{2.1}$$

With the help of the modularity theorem, one can prove the following result.

**Theorem 2.1.1.** *$\Lambda(E, s)$ has an analytic continuation to all of $\mathbb{C}$, and for all $s \in \mathbb{C}$ satisfies*

$$\Lambda(E, s) = w(E/\mathbb{Q})\Lambda(E, 2 - s), \tag{2.2}$$

*where $w(E/\mathbb{Q}) \in \{\pm 1\}$ denotes the root number of $E$.*

The generalisation of this theorem to abelian varieties over arbitrary number fields is known as the Hasse–Weil conjecture, and is as of yet unproven.

Theorem 2.1.1 tells us moreover that $L(E, s)$ can similarly be extended to an entire function, and the BSD-conjecture is concerned with its behaviour around $s = 1$.

**Definition 2.1.2.** *The analytic rank* $\text{rank}_{\text{an}}(E/\mathbb{Q})$ *of $E$ is the order of vanishing of $L(E, s)$ in $s = 1$.*

**Conjecture 2.1.3** (Birch and Swinnerton-Dyer)**.** *For every elliptic curve $E/\mathbb{Q}$ we have*[4]

$$\text{rank}_{\text{an}}(E/\mathbb{Q}) = \text{rank}(E/\mathbb{Q}).$$

A more refined version of the conjecture also specifies the leading coefficient of the Laurent series around 1 in terms of invariants of the curve, such as the order of the torsion subgroup and the size of the Tate–Shafarevich group $Ш(E/\mathbb{Q})$.

Although few seem to doubt the validity of conjecture 2.1.3, a proof to date has remained elusive. There are, however, several partial results, from among which we highlight the following, which is due to the combined work of Kolyvagin [Kol89], and Gross and Zagier [GZ85].[5]

**Theorem 2.1.4.** *Conjecture 2.1.3 holds for all elliptic curves of analytic rank 0 or 1.*

In principle, the BSD-conjecture gives us a new way to calculate the rank of an elliptic curve, sidestepping the problem (which we illustrated in section 1.2.3) of having to decide whether certain varieties contain rational points or not. Indeed, if we return to the curve $D_0$ that we discussed in section 1.1.3, `Sage` can calculate for us that

$$L(D_0, 1) \approx 0.65551,$$

and so by theorem 2.1.4 it follows that $D_0$ has rank 0 (and consequently only a finite number of rational points). Although this is a nice application, we will now discuss why analytical rank calculations are often not preferable to regular (honest) 2-descents.

(i) As of the current state of the art, analytical rank methods can not prove that a certain elliptic curve has a given rank, unless that rank is either 0 or 1. Recall that this thesis concerns the family of Diophantus, none of whose members (with a finite number of exceptions) actually satisfy this requirement. This drawback of obtaining only conjectural results is however not one we are too concerned with; many of the 2-descents that we performed were under the assumption that the generalised Riemann hypothesis holds, which also gives only conjectural results.

[4] Outside of academic circles conjecture 2.1.3 is mostly known because of its status as one of the seven Millennium Problems, a set of open conjectures upon which the Clay Mathematics Institute put a bounty of 1 million US dollars in 2000. Unfortunately, these bounties do not seem to increase with inflation, so those whishing to claim one should do so sooner than later.

[5] The results of Kolyvagin, Gross and Zagier only concerned modular curves, which by the modularity theorem (proven in [BCDT01]) we now know all elliptic curves over $\mathbb{Q}$ are.

(ii) In order to prove that the analytical rank of an elliptic curve $E$ equals a number $r$, one needs to show that $L(E,1), L'(E,1), \ldots, L^{(r-1)}(E,1)$ are zero, and that $L^{(r)}(E,1)$ is non-zero. This last part is doable, there are explicit bounds on the tail-end of the $L$-series, such as those in [GJP+09, Section 2.2], which can be used to provably determine that $L^{(r)}(E,1)$ is indeed non-zero. The first task is unfortunately not so simple, as computers sadly lack the capability to perform an infinite number of operations in a finite amount of time. `Pari/GP` solves this issue by working under the assumption that any value found less than some parameter $\epsilon$ is probably zero, and then returns a number that is *probably* the analytic rank (c.f. the `ellanalyticrank` function in [gro25]). It is not surprising such solutions are necessary, since, according to the `Sage` source code,

*It is an open problem to prove that any particular elliptic curve has analytic rank $\geq 4$.*

A useful result in this direction is the Gross-–Zagier theorem [GZ85, Theorem 7.3], which links the value of $L'(E,1)$ to the height of a certain Heegner point.[6] This allows one to use a calculation which shows that up to a certain finite precision $L'(E,1) \approx 0$ to conclude that in fact $L'(E,1) = 0$. Similarly, using the Manin–Drinfeld theorem [Dri73] the value of $L(E,1)$ can be bounded (c.f. [RS17, Proposition 17.2.10]), which similarly allows finite precision calculations to yield a proof of whether $L(E,1)$ is 0. Lastly, recall that the root number $w(E/\mathbb{Q}) \in \{\pm 1\}$ (seen in eq. (2.2)) can be effectively calculated, and if it equals $-1$, then this directly implies that $L(E,1) = 0$. Notably, none of the three results mentioned allow one to prove that a particular elliptic curve has a specific analytic rank higher than 3.

(iii) It turns out that calculating analytic ranks is in fact very slow, at least compared to calculations of the algebraic rank by 2-descent, and this difference increases for curves of larger conductor. In table 2.1 we show for a select number of values of $m$ the time it takes `Sage` to calculate both of the two ranks. While for small values of $m$ the analytic rank can be found faster than the real rank, as $m$ increases this ceases to be the case, and for value of $m$ above 1000 the descents tend to outperform analytic rank computations by about a factor 1000.

| $m$ | 1 | 10 | 100 | 1000 |
|---|---|---|---|---|
| $t_{\text{an}}$ | $1.5 \cdot 10^{-3}$ | $1.2 \cdot 10^{-2}$ | $1.8 \cdot 10^{0}$ | $2.2 \cdot 10^{2}$ |
| $t_{\text{alg}}$ | $1.4 \cdot 10^{-2}$ | $7.0 \cdot 10^{-2}$ | $7.4 \cdot 10^{-2}$ | $2.2 \cdot 10^{-1}$ |
| $t_{\text{an}}/t_{\text{alg}}$ | $1.0 \cdot 10^{-1}$ | $1.7 \cdot 10^{-1}$ | $2.5 \cdot 10^{1}$ | $1.0 \cdot 10^{3}$ |

Table 2.1: Computation times in seconds for selected values of $m$ for the curves $D_m$ of both the analytic rank and the real rank, using `Sage`. This was a small test with small sample sizes, so the displayed numbers should be taken with a grain of salt, but the pattern should be clear. While for small values of $m$ the analytic rank can be found faster than the algebraic rank, as $m$ increases this pattern inverts, and algebraic ranks becomes significantly easier to compute.

To finish this section, we will make the following loosely related remark. Intuitively one would expect that the computation of the analytic rank becomes more difficult as the analytic rank gets higher. Interestingly, the implementation in `Pari/GP` does not reflect this. In fig. 2.1 we show the time it takes`Pari/GP` (when called by `Sage`) to calculate the analytic rank of $D_m$ for $1 \leq m \leq 400$. We will not go into a thorough statistical analysis, but at least visually there seems to be no correlation between the analytic rank and the computation time. Instead, the only relevant contributing factor seems to be the conductor.

### 2.1.2 Our calculations

For our research, we attempted to calculate the rank of the curves $D_m$ for $m = 1, \ldots, 468183$. For this task, we considered using the software packages `Magma` [BCP97] and `Sage` [The20]. Limited testing showed that `Magma` performed the calculations ever so slightly faster, although due to the closed source nature of `Magma` it is to us unclear why. Nevertheless, we decided to stick with `Magma`. Within `Magma` we used the recommended `SetClassGroupBounds("GRH")` command to make it so that all class group computations assume the generalised Riemann hypothesis (GRH). Ordinarily, in order to determine the class group

[6] This Heegner point is a constructible point on $E(\mathbb{Q})$ which has infinite order exactly when $\text{rank}_{\text{an}}(E,\mathbb{Q}) = 1$. It is thanks to Heegner points that we know theorem 2.1.4 holds, and the theory of Heegner points currently is our only source of constructable points. Since the Heegner point is a torsion point in all curves with analytic rank higher than 1, it unfortunately seems to be no help in proving the full BSD-conjecture.

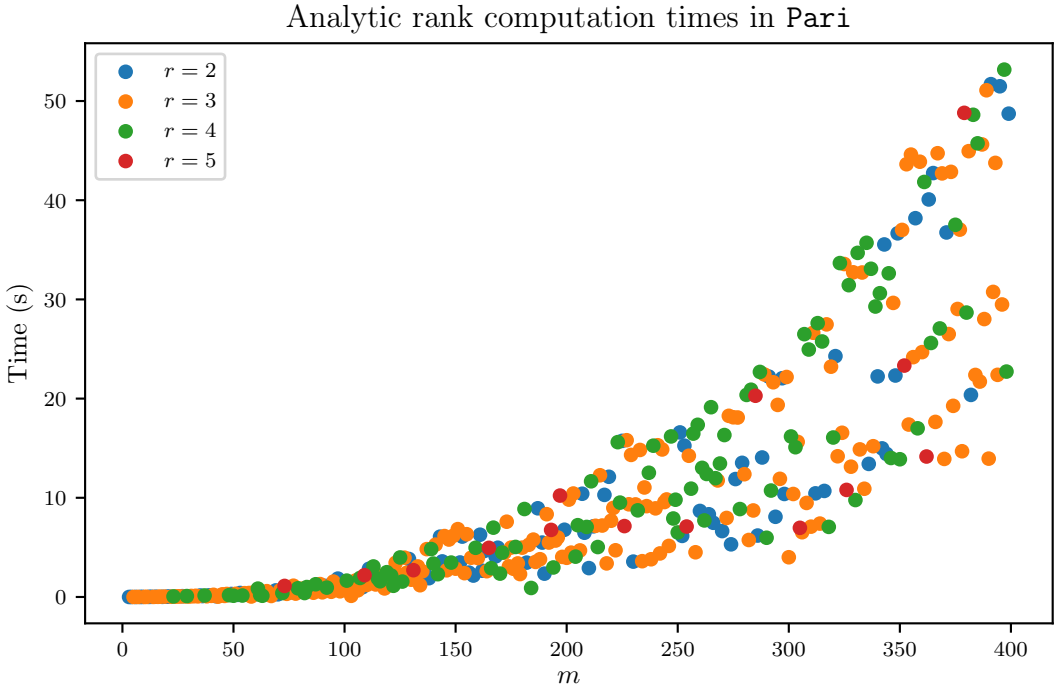



Figure 2.1: For the values $m \in \{1, 400\}$ we determined how long it took `Pari` to calculate the analytic rank of $D_m$. While our initial expectation was that it would probably be faster to calculate the rank of curves with lower (analytic) rank, the experiment does not confirm that, and the time spent in fact seems independent of the rank. Notable are the three bands of data points; these correspond to the residues of $m$ mod 4. For *most* curves, the conductor $N_m$ of $D_m$ satisfies $N_m = \Delta_m/2^k$, where $k = 0, 1, 2$ if $m$ mod 4 is odd, 0 and 2 respectively. As a consequence, for e.g. odd values of $m$ the conductor is relatively large and so a larger computation time is needed.

of a field $K$ (which we saw was needed to perform a 2-descent), one needs to consider all prime ideals with norm below the Minkowski bound. It has been shown in [Bac90] that, assuming GRH, Minkowski's bound (which is $O(\sqrt{\Delta_K})$ for a fixed degree of $K$) can be replaced by a much stronger bound that is $O(\log^2(\Delta_K))$, and so assuming GRH greatly speeds up these calculations. Within `Magma` we used the `MordellWeilShaInformation` command, which uses all available `Magma` machinery (such as 4-descents). For these calculations it is recommended to use the `RankOnly` option as this halts the function as soon as the rank has been determined. As a result of our computations, we obtained for each curve $D_m$ in the domain a lower and upper bound for the rank. In a small number of cases ($< 500$) these bounds did not agree, and for simplicity, we decided to assume the lower one.

## 2.2 Provable results

In this section we briefly consider two results about the Diophantus family, namely the lack of torsion for integral values of $m$ and the generic rank of the family, which was proven in [Eik04] to be equal to 2.

### 2.2.1 Torsion

Since our calculations show that (except for $m = 0$) none of the curves $D_m$ have non-trivial torsion, it is natural to conjecture that indeed holds for all $m > 0$. Indeed, this follows from the following two well known results, which are corollary VIII.7.2 and proposition VII.3.1 in [Sil09] respectively.

**Theorem 2.2.1** (Lutz-Nagell)**.** *Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass model $E : y^2 = x^3+Ax+B$, with $A, B \in \mathbb{Z}$. Let $P = (x, y) \in E(\mathbb{Q})$ be a torsion point. Then*

*(i)* $x, y \in \mathbb{Z}$, *and*
*(ii)* $2P = O$, *or* $y^2$ *divides* $4A^3 + 27B^2$.

**Proposition 2.2.2.** *Let $K$ be a number field, $\mathfrak{p}$ a finite prime of $K$, $K_\mathfrak{p}$ the completion of $K$ at $\mathfrak{p}$, $k$ the residue field of $K_\mathfrak{p}$, $E/K$ an elliptic curve with some fixed minimal integral model, and $m \geq 1$ an integer coprime to* $\mathrm{char}(k)$. *Let $\tilde{E}/k$ be the reduction of $E$ to $k$. If $\tilde{E}$ is nonsingular, then the natural reduction map $E(K)[m] \to \tilde{E}(k)$ is injective.*

Using these results we are able to prove the following proposition.

**Proposition 2.2.3.** *For all $m \in \mathbb{Z}_{\geq 1}$, $D_m$ as trivial torsion.*

*Proof.* To apply theorem 2.2.1 we instead look at the curve

$$D'_m : y^2 = x^3 - 16x + 16m^2,$$

which through a simple coordinate transformation

$$\begin{aligned} D_m &\longrightarrow D'_m \\ (x, y) &\longmapsto (-4x, 8y + 4m) \end{aligned}$$

can be seen to be isomorphic to $D_m$. Because of part (ii) of theorem 2.2.1, our proof naturally splits into two parts.

(i) We first show that no $D'_m$ has a nontrivial 2-torsion point. Such torsion points must have $y = 0$ and hence correspond to rational solutions of the equation $x^3 - 16x + 16m^2 = 0$. This last equation defines an elliptic curve, and `Sage` tells us that it has rank 0 and that the rational torsion points are exactly the 2-torsion points given by $m = 0$ and $x = 0, 4, -4$. Therefore, unless $m = 0$, $D'_m$ (and hence $D_m$) has no rational 2-torsion points.

(ii) Now assume that $(x, y)$ is a torsion point on $D'_m$ whose order is more than 2. We calculate the discriminant of $D'_m$ to be

$$\Delta_m = 4 \cdot (-16)^3 + 27 \cdot 16^2 \cdot d^4 = -2^{14} + 3^3 \cdot 2^8 \cdot m^4.$$

Since $\Delta_m \equiv 2 \mod 3$ for all $m$, $D'_m$ has good reduction mod 3. Reducing $D'_m$ modulo 3 then yields the two possible curves

$$y^2 = x^3 - x \qquad \text{if } m \equiv 0 \mod 3 \qquad \text{and} \qquad y^2 = x^3 - x + 1 \qquad \text{if } m \equiv 1, 2 \mod 3.$$

which have torsion subgroups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/7\mathbb{Z}$. By proposition 2.2.2 it follows that $D'_m$ can only have 2-, 3- or 7-torsion. Similarly, since we have

$$\Delta_m \equiv -(-1)^7 + 27(-1)^4 \cdot 1 \equiv 28 \not\equiv 0 \mod 5,$$

we have good reduction modulo 5. Reducing mod 5 gives the torsion subgroups $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/8\mathbb{Z}$, which shows that there are no torsion points of order 3 or 7, which together with the previous part proves that $D'_m$ (and hence $D_m$) has no non-trivial torsion.

□

Instead of solely looking at integral $m$, it is natural to also consider rational $m$. The above proof showing that for integral $m$ there is no rational 2-torsion also directly shows the same for all rational $m$. The second part of the proof, which shows that there are no higher order torsion points, does not work for all rational $m$, and also does not easily generalize. Instead, we can try the same approach as we used to find 2-torsion points to find $p$-torsion points for $p = 3, 5, 7$. [7] That is, we write an equation in $x$ and $m$ whose solutions correspond to $p$-torsion points on $D'_m$ with first coordinate equal to $x$, and try to find all rational solutions to these equations. The resulting equations (which are in fact all polynomial) are known as *division polynomials*, and we refer to [Was08, Section 3.2] for more information. In our case, the resulting polynomials are

$$3x^4 - 96x^2 + 192m^2x - 256,$$

for 3-torsion points,

[7] Recall that by Mazur's theorem any curve that has non-trivial torsion has a torsion point of order 2,3,5 or 7.

$$5x^{12} - 992x^{10} + 6080m^2x^9 - 26880x^8 - 61440m^2x^7 + \left(-61440m^4 + 1228800\right)x^6 - 2850816m^2x^5 + \left(7864320m^4 - 8192000\right)x^4 + \left(-6553600m^6 + 5242880m^2\right)x^3 + \left(-15728640m^4 + 52428800\right)x^2 + \left(41943040m^6 - 104857600m^2\right)x - 16777216m^8 + 33554432m^4 + 16777216$$

for 5-torsion points, and

$$7x^{24} - 4928x^{22} + 63104m^2x^{21} - 756224x^{20} + 28672m^2x^{19} + \left(-10981376m^4 + 81313792\right)x^{18} - 379158528m^2x^{17} + \left(2342387712m^4 - 2308898816\right)x^{16} + \left(-3398434816m^6 + 2084569088m^2\right)x^{15} + \left(-40328232960m^4 + 86260056064\right)x^{14} + \left(139754209280m^6 - 169701539840m^2\right)x^{13} + \left(-60834185216m^8 + 311921999872m^4 - 1877638905856\right)x^{12} + \left(-2730257022976m^6 + 10203231682560m^2\right)x^{11} + \left(3453690576896m^8 - 20011863244800m^4 + 11319386308608\right)x^{10} + \left(-1631013830656m^{10} + 62534723829760m^6 - 114276194844672m^2\right)x^9 + \left(-118605521879040m^8 + 223321119522816m^4 + 67315022430208\right)x^8 + \left(119571889520640m^{10} - 352874513039360m^6 + 231172319739904m^2\right)x^7 + \left(-47141561040896m^{12} + 615726511554560m^8 - 817761773158400m^4 - 1014024598716416\right)x^6 + \left(-992858999881728m^{10} + 723478651076608m^6 + 3936801383251968m^2\right)x^5 + \left(815837627809792m^{12} + 1693247906775040m^8 - 9235897673318400m^4 + 1431564139364352\right)x^4 + \left(-215504279044096m^{14} - 3571213767016448m^{10} + 10467350696427520m^6 - 1847179534663680m^2\right)x^3 + \left(2339760743907328m^{12} - 6649846324789248m^8 + 4063794976260096m^4 - 3448068464705536\right)x^2 + \left(-985162418487296m^{14} + 4433230883192832m^{10} - 7881299347898368m^6 + 6896136929411072m^2\right)x + 281474976710656m^{16} - 1688849860263936m^{12} + 3659174697238528m^8 - 2814749767106560m^4 - 281474976710656$$

for 7-torsion points. All three equations define (the affine part of) irreducible curves. It should be clear that determining whether these curve have rational points is no easy task, and so we will not try to perform it here. In principle, if one can show that the above curves are smooth and have high genus, Falting's theorem implies that there are at most a finite number of solutions, although this would be non-constructive and does not immediately give a bound on the number of such points.

### 2.2.2 Generic points

It is clear that every curve $D_m$ contains the six points

$$(1,0),\ (0,0),\ (-1,0),\ (1,m),\ (0,m),\ \text{and}\ (-1,m). \tag{2.3}$$

A natural point of view to study a family of elliptic curves as the one at hand is one where we view the family as a single curve

$$D : y(t-y) = x^3 - x$$

over the function field $\mathbb{Q}(t)$. For any value $m \in \mathbb{Q}$ of $t$ we obtain the so-called specialisation maps

$$\sigma_m : D(\mathbb{Q}(t)) \longrightarrow D_m(\mathbb{Q})$$

by substituting $m$ for $t$. These maps are homomorphisms whenever $D_m$ is non-singular. We now have the following result by Silverman (c.f. in [Sil13, theorem III.11.4]).

**Proposition 2.2.4.** *$\sigma_m$ is injective for all but finitely many $m$.*

As a direct consequence we have that for all but finitely many $m$, $D_m(\mathbb{Q})$ contains a subgroup isomorphic to $D(\mathbb{Q}(t))$. This is a good reason to study $D$ more closely.

The six points in eq. (2.3) also define six points on $D(\mathbb{Q}(t))$ (when $m$ is replaced by $t$). By considering the intersection of $D$ with the lines $x = 1, x = 0, x = -1$, and $y = 0$, and using that for each such line the points in the intersection (counted with multiplicity) sum to zero, we find the relations

$$(1,0) + (1,t) = O, \qquad (0,0) + (0,t) = O, \qquad (-1,0) + (-1,t) = O, \qquad (1,0) + (0,0) + (-1,0) = O$$

As there are no obvious relations between the points $(0,0)$ and $(1,0)$, it is reasonable to expect them to be independent. Since any relation between the points of $D$ holds at every specialisation, it is sufficient

to show this suspected independence for any value of $t$. As we've already seen the independence holds in $D_6$, it directly follows that they are independent in $D$ as well.

As the above argument shows that the generic rank must be at least 2, a now compelling question is whether it is possible to give an upper bound on this generic rank. This is indeed possible, as was proven in [Eik04].

**Theorem 2.2.5.** *$D/\mathbb{Q}(t)$ has rank 2.*

*Proof.* The full proof of this is beyond the scope of this thesis. We instead give a brief overview of its structure.

The proof is based on the concept of an elliptic surface $S$, which (omitting some details) is a surface $S$ together with a projective curve $C$ and a morphism $S \to C$ (all defined over some number field $k$), such that almost all fibers are elliptic curves. In our example, the surface consists of the points $(x, y, m)$ that satisfy $y(m - y) = x^3 - x$, and the map sends such a point to its value of $m$.

For an elliptic surface $S$ the Néron-Severi group $NS(S)$ is defined as the quotient $\mathrm{Pic}(S)/\mathrm{Pic}^0(S)$ of the Picard group $\mathrm{Pic}(S)$ by the connected component of the identity $\mathrm{Pic}^0(S)$. The latter consists of those divisors that are algebraically equivalent to the identity. Importantly, $\mathrm{NS}(S)$ is a finitely generated abelian group equipped with a bilinear form. Moreover, within $\mathrm{NS}(S)$ it is possible to define a sublattice $T$ such that there is a (natural) isomorphism

$$D(k(C)) \xrightarrow{\sim} \mathrm{NS}(S)/T.$$

Importantly, the rank of $T$ can be extracted from knowledge about the singular (reducible) fibers. To be precise, each fiber decomposes as a union of a finite number of curves. The possible configurations of these curves (i.e. their number together with the types of singularities and multiplicities occurring) have been independently classified by both Kodaira [Kod63] and Néron [Né64]. In [OS91], for each of the possible configurations the corresponding contribution to $T$ has been calculated. Moreover, it can be shown (see e.g. [SS19, Chapter 6]) that for families $E/\mathbb{Q}(m)$ indexed by $\mathbb{P}^1$ (such as the family of Diophantus), the generic rank is at most 8, and the reducible fibers may reduce this further down. In the case of $D$, there are four trivial contributions corresponding to the four $\overline{\mathbb{Q}}$-roots of the discriminant $2^6 - 3^3 \cdot m^4$, and a contribution of rank 6 corresponding to $m = \infty$. Consequently, the rank is indeed brought down from 8 to 2.

□

## 2.3 Analysing the dataset

As part of our research, we have calculated the rank of the curves $D_m$ for $m = 1, \ldots, 4112804$. In this section we consider two expectations.

- First, we expect the parity of the ranks to behave randomly, with odd and even ranks occurring with a probability of 50%.
- Secondly, given the parity of the rank, we generally expect the rank to be the minimal value allowed by the parity and the generic rank, i.e. rank 2 if even and rank 3 if odd.

The first point will be swiftly dealt with in section 2.3.1. The second point will take more work, since (as noted in the introduction), the ranks do need not seem to be minimal, with curves of rank 4 being more prevalent than those of rank 2 for small $m$. We will study this behaviour as $m$ increases, and compare it to quantitative expectations derived from more general existing heuristics.

We introduce the notations

$$P(\phi(m) \mid m \leq M) := \frac{\#\{m : 0 < m \leq M \text{ and } \phi(m)\}}{M}$$

and

$$P(\phi(m) \mid m = M) := \frac{\#\{m : M - B < m \leq M \text{ and } \phi(m)\}}{B},$$

where $\phi$ is some boolean statement (usually concerning $\operatorname{rank} D_m$), and $B$ is some appropriate bound, often 1000 or 10 000 depending on the expected variance.

### 2.3.1 Rank parity

While the rank of an elliptic curve has remained mysterious, the parity of the rank seems much more well behaved. That is, in general, the parity is expected to be "random", with odd and even ranks occurring with 50% probability. It is natural to conjecture that this behaviour also holds in the family of Diophantus. We will not perform a rigorous statistical analysis to test this hypothesis, and instead we will simply show three figures that hopefully make it at least seem plausible to the reader.

In fig. 2.2 we show how $P(\operatorname{rank} D_m \text{ is even} \mid m \leq M)$ (as a function of $M$) changes within our subset. As expected, it quickly tends to $\frac{1}{2}$. In fig. 2.3 we show the local equivalent of fig. 2.2 and graph $P(\operatorname{rank} D_m \text{ is even} \mid m = M)$. A priori, there is no particular reason why this graph would show something interesting, and luckily for us, it indeed does not. A perhaps more enlightening representation of the same data is shown in fig. 2.4. Here, we divided our dataset into buckets of 100 consecutive data points, and within each bucket we calculated the number of even ranks, fig. 2.4 shows the distribution of the numbers found. We expect these numbers to follow a binomial distribution with an average of 50 and a variance of $100 \cdot \frac{1}{2} \cdot (1 - \frac{1}{2}) = 25$. The figure indeed shows that our found data closely matches the appropriate approximating Gaussian. Quantitively, our data has an average of 49.96 and a variance of 24.50, which are both very close to the expected values.

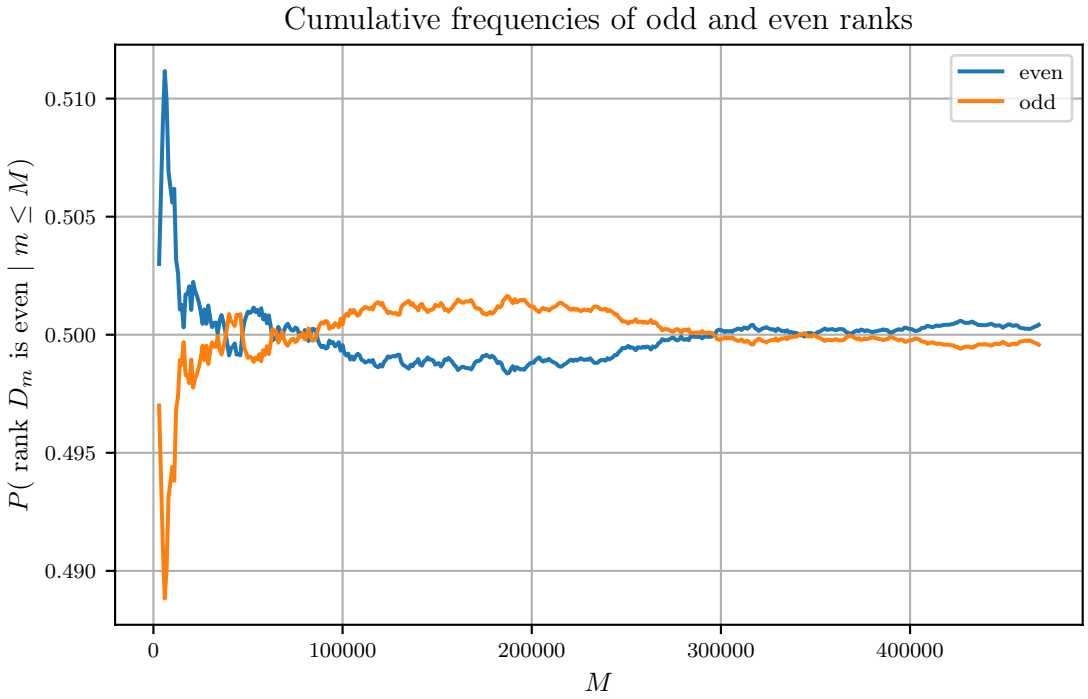



Figure 2.2: This figures shows the graphs for $P(D_m \text{ is odd/even} \mid m \leq M)$ within our dataset. As expected, both graphs (which by definition sum to 1) seem to tend to $\frac{1}{2}$.

### 2.3.2 Rank occurrences and the PPVW conjecture

Recall from section 2.2.2 the fact that the family of Diophantus has two independent generic points, and that by proposition 2.2.4 this means that all but finitely many curves in the family will have rank at least 2. Recall that the informal minimalist conjecture states that elliptic curves generally have the minimal rank allowed by the parity of their rank. A natural application of the conjecture to the family of Diophantus would be the following.

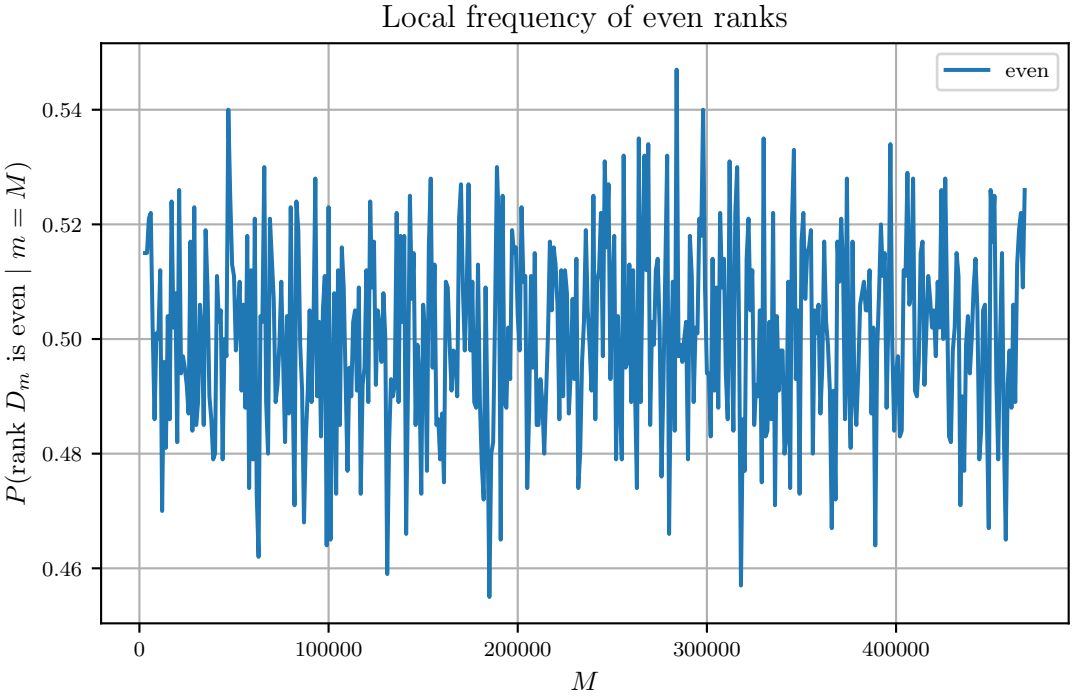



Figure 2.3: Local behaviour of rank parity

**Conjecture 2.3.1.** *In the family of Diophantus, 50% of curves have rank 2, and 50% have rank 3.*

These percentages should be understood as referring to the asymptotic density with respect to some natural orderings on the curves.

In fig. 2.5 we show the frequency with which the different ranks occur in our dataset. Two observations can immediately be made. Most notably, the curves with rank 4 outnumber the curves with rank 2, and a significant portion of curves have rank higher than 4. Secondly, the frequencies with which curves of high rank occur decreases as $N$ increases. This decrease is more clearly visible in fig. 2.6. Nevertheless, given our data it seems unlikely that we will be able to give a meaningful answer to the question of whether conjecture 2.3.1 holds. This is of course not unexpected as conjecture 2.3.1 lacks a quantitative statement which we can directly test. Instead, we turn to the recent paper [PPVW19], which does give an exact quantitive expectation for the distribution of the ranks of elliptic curves. To state it, we first introduce the (naive) height of an elliptic curve.

**Definition 2.3.2.** *For a short Weierstrass model $E : y^2 = x^3 + Ax + B$ of an elliptic curve, we define its height as*

$$\operatorname{ht} E = \max\{4|A|^3, 27B^2\}.$$

Every elliptic curve has an integral short Weierstrass model. We let $\mathcal{E}$ denote a set containing one minimal short Weierstrass model for every isomorphism class, and we let $\mathcal{E}_{\leq H}$ denote the subset of those models with height at most $H$. In particular one can show that[8]

$$T(H) := \#\mathcal{E}_{\leq H} = (\kappa + o(1))H^{5/6},$$

where $\kappa = 2^{4/3}3^{-3/2}\zeta(10)^{-1}$ and where $o(1)$ is a function that goes to zero when $H$ goes to infinity.

We now arrive at the conjecture stated in [PPVW19], to which we will refer as the PPVW conjecture.

[8] See for example lemma 4.3 in [Bru92].

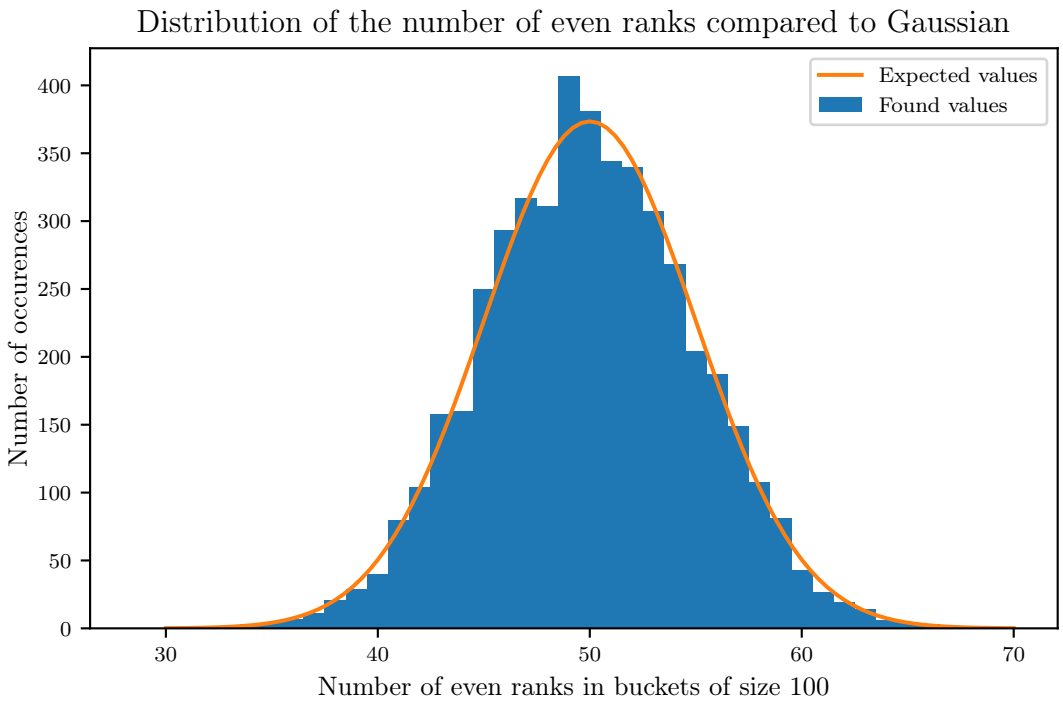



Figure 2.4: The parity of the rank an elliptic curve is expected to be odd and even with equal probability. To test this, we divided our dataset in buckets of size 100, and within each bucket we counted the number of even ranks. In blue we show the distribution of the found values. In orange we show the expected values when modelled as a binomial distribution, which for clarity we approximated by the Gaussian shown.

**Conjecture 2.3.3** ([PPVW19])**.** *For $1 \leq r \leq 20$ we have*

$$N_r(H) := \#\{E \in \mathcal{E}_{\leq H} : \operatorname{rank} E \geq r\} = H^{(21-r)/24+o(1)}.$$

*In particular, a positive proportion of curves have rank 1. Similarly, there is only a finite number of elliptic curves with rank $\geq 21$.*

In particular, a curve of height $H$ has probability

$$P^{\geq r}(H) = \frac{N_r'(H)}{T'(H)} = \frac{((21-r)/24 + o(1)) \cdot H^{(-3-r)/24+o(1)}}{(\kappa + o(1)) \cdot 5/6 \cdot H^{-1/6}} \propto H^{(1-r)/24+o(1)}.$$

of having rank at least $r$.

It should be noted that conjecture 2.3.3 is about the family of all elliptic curves, which has generic rank 0. Clearly, our family will not follow this heuristic due to the fact that the generic rank is 2, and, for example, there is only a finite number of curves with rank 0 or 1. Instead, it seems natural to conjecture the following.

**Conjecture 2.3.4.** *For $3 \leq r \leq 22$ the probability $P^{\geq r}(H)$ that a curve $D_m$ of height $H$ from the family of Diophantus has rank at least $r$ is*

$$P^{\geq r}(H) \propto H^{(1-(r-2))/24+o(1)} = H^{(3-r)/24+o(1)}.$$

*In particular, the probability that $D_m$ has rank at least $r$ is proportional to*

$$m^{(3-r)/6}.$$

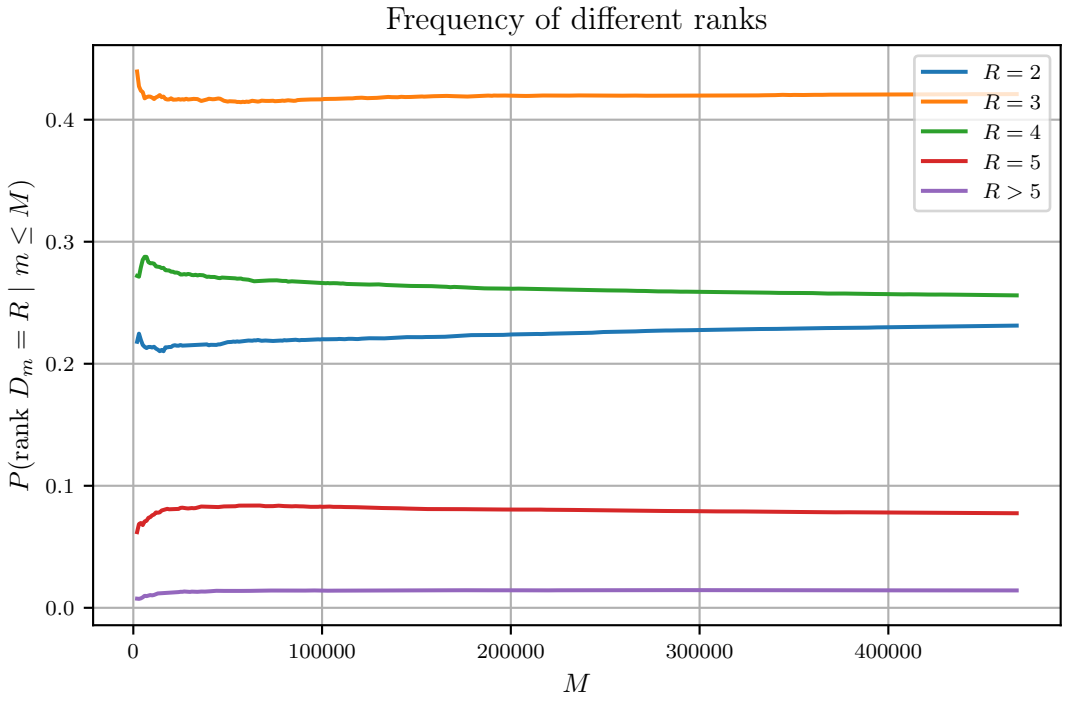



Figure 2.5: While we expect to see mostly curves of rank 2 and 3, we instead see a large number of rank 4 curves.

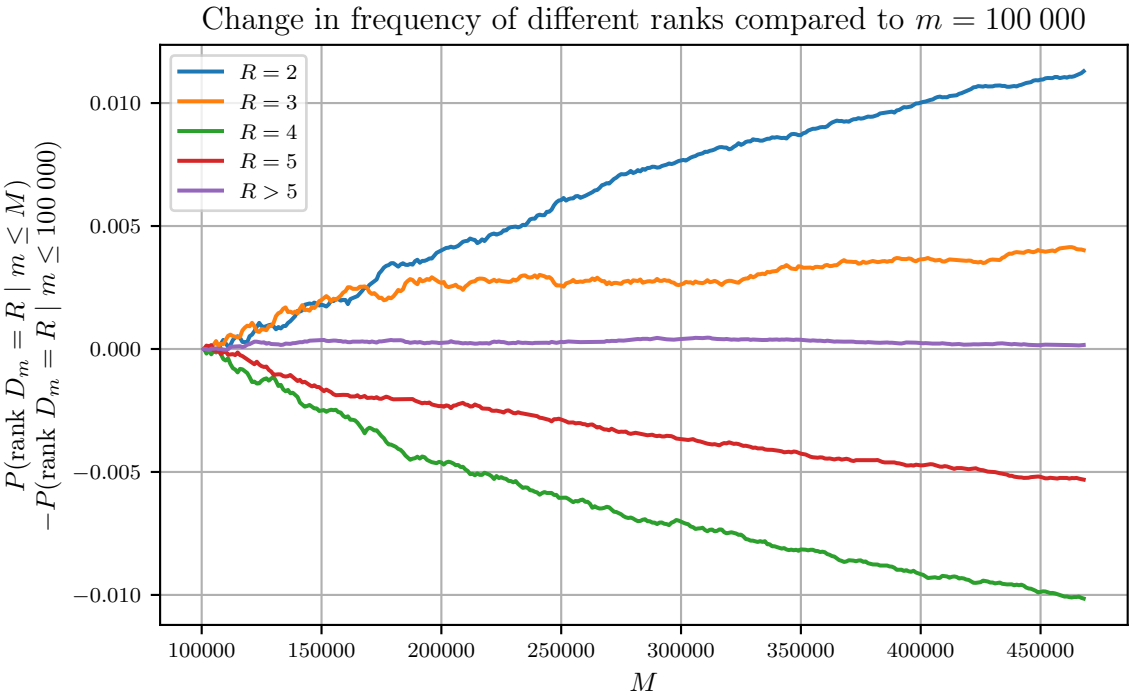



Figure 2.6: This figure shows the change in frequency with which different ranks occur compared to $m = 100\,000$. As expected, the low ranks 2 and 3 increase, and the high ranks 4 and 5 decrease. Ranks higher than 5 also see a small increase, which can probably be explained by a small sample size.

It should be noted that heights behave differently for odd and even $m$, since we assume *minimal* integral models. This means that for $m$ even or odd we have to use the models

$$y^2 = x^3 - x + \left(\frac{m}{2}\right)^2 \qquad \text{and} \qquad y^2 = x^3 - 16x + 16m^2 \tag{2.4}$$

for $m$ even and odd respectively, which (approximate) corresponding heights

$$27 \cdot \left(\frac{m}{2}\right)^4 \qquad \text{and} \qquad 27 \cdot 16^2 \cdot m^4. \tag{2.5}$$

In particular, we would expect $D_m$ to have a slightly larger chance to have large rank if $m$ is even than if it were odd. Indeed, this is what we see; see fig. 2.7.

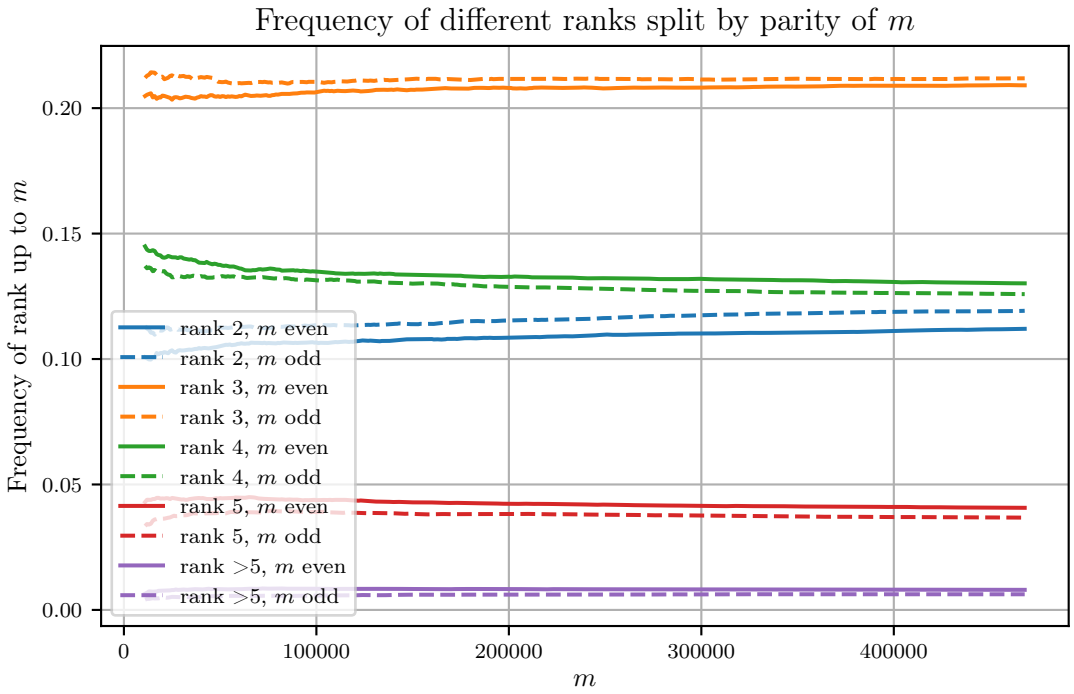



Figure 2.7: This figure shows the frequency with which different ranks occur, where we make a distinction between odd (dashed lines) and even (filled lines) values of $m$. The figure shows that for odd $m$ the low ranks 2 and 3 occur more often than for even $m$, which is line with eq. (2.4).

### 2.3.3 Verifying the conjecture

In order to test conjecture 2.3.4, will now assume that it holds, and that the $o(1)$ term is constant in our domain. To make this more precise, we will write

$$P_{\pm}^{\geq r}(H)$$

for the probability that a curve $D_m$ of height $H$, such that the sign of $m$ matches the subscript, has rank at least $r$. We now suppose that there are correlations of the form

$$P_{\pm}^{\geq r}(H) = c_{\pm}^{\geq r} H^{d_{\pm}^{\geq r}}. \tag{2.6}$$

The best fitting values for $r = 4, 5, 6$ within our dataset are found in table 2.2. These values were found by performing a linear regression on $\log(P_{\pm}^{\geq r}(H))$ and $\log(H)$. The corresponding correlation coefficients can be found in table 2.3. We make the following observations.

- For $r = 4$ and $r = 5$, the values found are similar between the odd and even values of $m$, which is a good consistency check. Conjecture 2.3.4 only depends on the height of a curve, so it should not matter whether we consider odd or even values of $m$.
- For $r = 6$, we find a positive exponent for odd $m$, which makes very little sense. This is probably best explained by a low sample size.
- For $r = 4$, the correlation coefficients that we obtained are very large, and fig. 2.8 indeed shows a convincing linear behaviour.
- None of the exponents found are even remotely close to the expected value $(3-r)/24$. To show this even better, in fig. 2.9 we show the same data as in fig. 2.8, but with the inclusion of a line that shows how the probability should decay were it to follow conjecture 2.3.4 without the $o(1)$ term.

As a simple way to test the formulas we obtained, we calculated the ranks of an additional set of curves further in the family; the results are shown in table 2.4. In table 2.5 we show how the corresponding values of $P_{\pm}^{\geq r}$, and in addition the values predicted by eq. (2.6) (using the values in table 2.2). The conclusion we can draw from this data is probably at best a weak one. Most of the values (bar a few outliers) are reasonably close to the number we expect, and so our way of modelling the ranks seems to hold up. However, a thorough verification likely requires much more data including higher values of $m$.

In conclusion, by assuming conjecture 2.3.4 holds with a (locally) constant $o(1)$ term, we obtain relations of the form eq. (2.6). The data that we generated indeed seems to fit these relations, and we obtain a decently performing predictive model of the ranks. Now, a tempting next question is whether the relations that we found hold up as $m$ increases further. Recall that we actually do not expect this to be the case, as the $o(1)$ term should go to 0. Attempts at verifying the decay of the $o(1)$ term using just the data that we collected yielded no convincing results. In order to verify whether this is indeed the case, more data is thus needed, preferably over multiple orders of magnitude.

One way to interpret the seemingly too small exponents is that there are more higher ranked than we should ordinarily expect. In the next section, we will argue that this is at least partially true. Namely, it turns out that it is fairly easy to manually construct curves of rank 4 or 5.

| | $r = 4$ | $r = 5$ | $r = 6$ |
|---|---|---|---|
| $d_{+}^{\geq r}$ | -0.0084 | -0.014 | -0.014 |
| $d_{-}^{\geq r}$ | -0.0081 | -0.011 | +0.0055 |
| $(3-r)/24$ | -0.042 | -0.083 | -0.125 |
| $c_{+}^{\geq r}$ | 0.54 | 0.20 | 0.033 |
| $c_{-}^{\geq r}$ | 0.53 | 0.16 | 0.0091 |

Table 2.2: Experimentally found values for the constants $d_{\pm}^{\geq r}$ and $c_{\pm}^{\geq r}$.

| | $r = 4$ | $r = 5$ | $r = 6$ |
|---|---|---|---|
| $m$ even | -0.85 | -0.72 | -0.34 |
| $m$ odd | -0.83 | -0.52 | +0.16 |

Table 2.3: Correlation coefficients of the calculations of $d_{\pm}^{\geq r}$ and $c_{\pm}^{\geq r}$.

## 2.4 Subfamilies of high generic rank

It is still an open question whether the rank of a rational elliptic curve is bounded or not. The two ways one can go about improving the situation are either finding a theoretical bound from above, or finding elliptic curves with high rank to push the bound from below. Throughout the 20th century various mathematicians have worked on this second option by searching for elliptic curves with ranks higher than

| | $r = 2$ | $r = 3$ | $r = 4$ | $r = 5$ | $r \geq 6$ |
|---|---|---|---|---|---|
| $m \in \{700\,000, \ldots, 701\,000\}$ | 267 | 415 | 224 | 81 | 13 |
| $m \in \{800\,000, \ldots, 801\,000\}$ | 245 | 416 | 256 | 67 | 16 |
| $m \in \{900\,000, \ldots, 901\,000\}$ | 246 | 425 | 258 | 60 | 11 |

Table 2.4: Distribution of ranks for high values of $m$.

| | | $r \geq 4$ | | $r \geq 5$ | |
|---|---|---|---|---|---|
| | | Predicted | Actual | Predicted | Actual |
| $m$ even | $m \approx 7 \cdot 10^6$ | 0.342 | 0.300 | 0.092 | 0.078 |
| | $m \approx 8 \cdot 10^6$ | 0.341 | 0.336 | 0.092 | 0.094 |
| | $m \approx 9 \cdot 10^6$ | 0.339 | 0.322 | 0.091 | 0.070 |
| $m$ odd | $m \approx 7 \cdot 10^6$ | 0.326 | 0.336 | 0.084 | 0.110 |
| | $m \approx 8 \cdot 10^6$ | 0.324 | 0.342 | 0.084 | 0.072 |
| | $m \approx 9 \cdot 10^6$ | 0.323 | 0.336 | 0.083 | 0.072 |

Table 2.5: Expected and actual probabilities of high ranks for high values of $m$.

| | | $r \geq 4$ | $r \geq 5$ |
|---|---|---|---|
| $m$ even | $m \approx 7 \cdot 10^6$ | 0.025 | 0.16 |
| | $m \approx 8 \cdot 10^6$ | 0.43 | 0.37 |
| | $m \approx 9 \cdot 10^6$ | 0.22 | 0.059 |
| $m$ odd | $m \approx 7 \cdot 10^6$ | 0.29 | 0.017 |
| | $m \approx 8 \cdot 10^6$ | 0.19 | 0.20 |
| | $m \approx 9 \cdot 10^6$ | 0.26 | 0.20 |

Table 2.6: The one-sided $p$-values observed data shown in table 2.5.

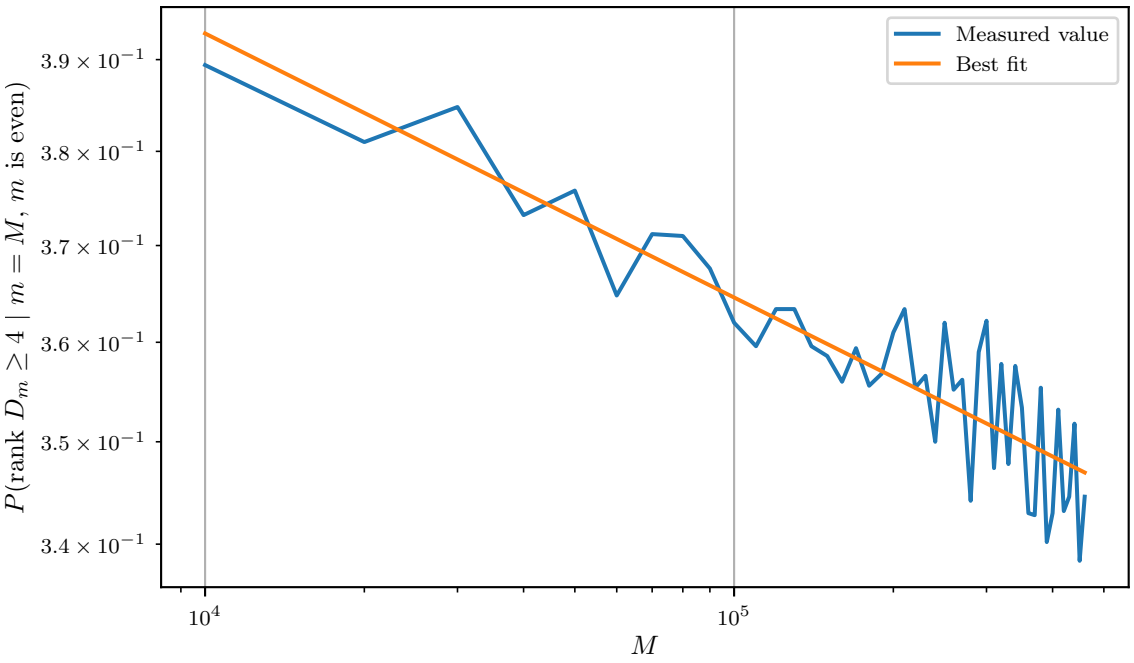



Figure 2.8: The probability that a curve has rank at least 4 seems to neatly exponential decay.

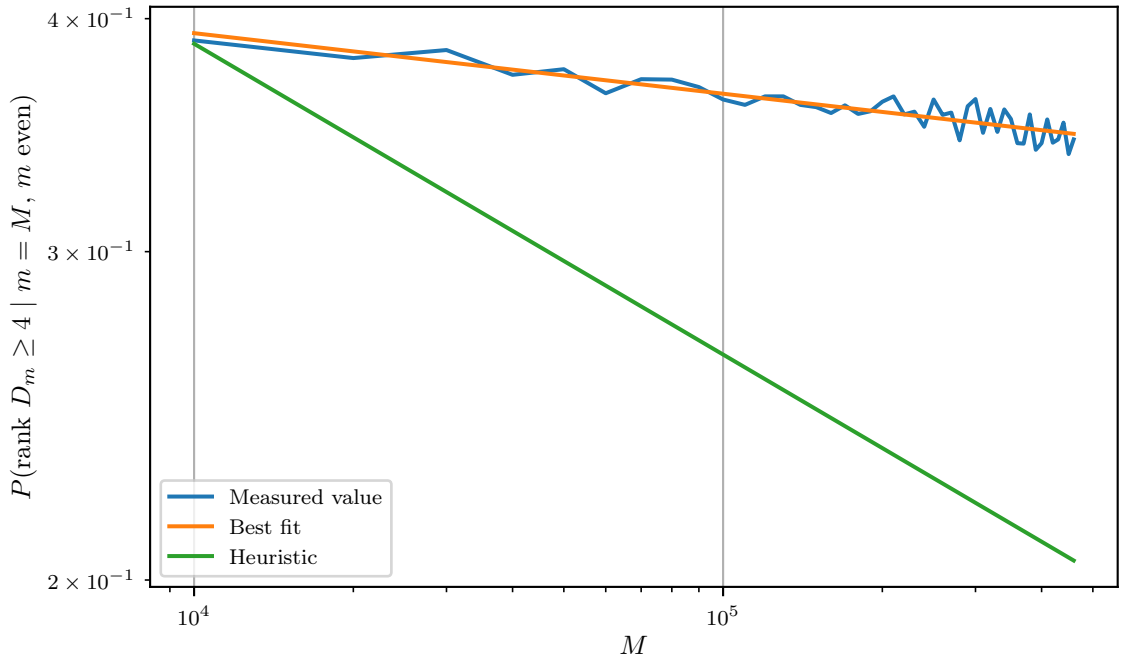



Figure 2.9: Here we show the same data as in fig. 2.8, but in addition we show the decay predicted by conjecture 2.3.4 if we exclude the $o(1)$ term.

those known before. This so-called rank record has been pushed to rank 29 by Elkies and Klagsbrun in 2024 [EK24] with the elliptic curve

$$\begin{aligned} y^2 + xy = x^3 &- 27\,006\,183\,241\,630\,922\,218\,434\,652\,145\,297\,453\,784\,768\,054\,621\,836\,357\,954\,737\,385x \\ &+ 55\,258\,058\,551\,342\,376\,475\,736\,699\,591\,118\,191\,821\,521\,067\,032\ldots \\ &\ldots 535\,079\,608\,372\,404\,779\,149\,413\,277\,716\,173\,425\,636\,721\,497 \end{aligned}$$

which provably has rank *at least* 29.[9] In [Duj24] one can find an overview of the history of this record, along with equations of the once leading curves and their sets of generators. Various records in between (e.g. [Nag92] and [Nag93]) have used a similar strategy: start with a family of elliptic curves with high generic rank, and cleverly choose specifications with high rank. With these efforts as inspiration in the back of our minds, we will use this last section to highlight (and slightly expand) earlier work by Eikenberg in [Eik04] regarding subfamilies of the Diophantus family of higher generic rank.

In line with [Eik04] we work with the family of elliptic curves given by

$$E_m : y^2 = x^3 - x + m^2,$$

and we note that we have an isomorphism

$$\begin{aligned} D_m &\longrightarrow E_{m/2} \\ (x, y) &\longmapsto (-x, y - m/2). \end{aligned}$$

Eikenberg then proves the following result, which is in [Eik04, Theorem 3.4.1].

**Proposition 2.4.1.** *Let $m_0 \in \mathbb{Q}$ be nonzero, and let $R \in E_{m_0}(\mathbb{Q})$ with $y(R) \neq m_0$ and $x(R) \neq 0$. Then there exist $M, X, Y \in \mathbb{Q}[t]$ such that*

- *$M, X, Y$ are quadratic, linear and quadratic respectively,*
- *$M(0) = m_0$ and $(X(0), Y(0)) = R$, and*
- *for each $t \in \mathbb{Q}$ we have $(X(t), Y(t)) \in E_{M(t)}(\mathbb{Q})$.*

*Moreover, there are exactly six choices for $(M, X, Y)$.*

Eikenberg moreover provides explicit formulae for (all six choices of) $M, X$ and $Y$.

This proposition allows us to lift a given point $R \in E_m(\mathbb{Q})$ to all the curves in the subfamily $\{E_{M(t)} : t \in \mathbb{Q}\}$. Generically, this point will then be independent of the generic points (i.e. those generated by $(0, m)$ and $(1, m)$), and so $\{E_{M(t)} : t \in \mathbb{Q}\}$ hence has a generic rank of 3. A natural question is then whether it is possible to lift several points simultaneously. To do this, one would fix a value of $m_0$, take several points $R_1, \ldots, R_n$ on $E_{m_0}$, and choose for each $i \in \{1, \ldots, n\}$ a lift $(M_i, X_i, Y_i)$ of the point $R_i$. The question then is whether the intersection of the images of all $M_i$ is nonempty. For $n = 2$ the answer is simple; the intersection can be found by equating two quadratic polynomials, which defines a conic. Since both quadratics satisfy $M_i(0) = m_0$, we have a rational point on this conic, and so by a standard result we have infinitely many rational points which are indexed by $\mathbb{P}^1(\mathbb{Q})$. Consequently, we obtain an infinite family of curves with generic rank 4.

For $n = 3$, the situation becomes more difficult but is still manageable. We now have three quadratic polynomials $M_1, M_2, M_3$, and the intersection of their images can be thought of as the intersection of the two quadratic surfaces $M_1(t_1) = M_2(t_2)$ and $M_1(t_1) = M_3(t_3)$ in $\mathbb{Q}^3$ (with coordinates $t_1, t_2, t_3$). Generally such an intersection is an elliptic curve, which we will call $A$. In section 2.4.1 we show how one can obtain an explicit (quartic) model for $A$. If $A(\mathbb{Q})$ has positive rank, then this yields an infinite subfamily of curves within the family of Diophantus consisting of curves that generally have rank 5. In [Eik04], indeed the following result is achieved.

**Proposition 2.4.2.** *There exists a (rational) map $m_A : A(\mathbb{Q}) \to \mathbb{Q}$, where $A$ is the elliptic curve given by*

$$A : y^2 = x^3 - x^2 - 103307652308x + 12301315572924612,$$

[9] In yet unpublished work it is (allegedly) shown that the rank is exactly 29, conditionally on GRH.

*such that for almost all $T \in A(\mathbb{Q})$ the curve $D_{m_A(T)}$ has at least rank 5.*[10]

This curve was found by starting out with the rank 5 curve $E_{113}$ and lifting the three independent points $(-23,-25),(-19,-77)$, and $(-11,107)$. As it turns out, finding such a subfamily of generic rank 5 indexed by a rank 2 elliptic curve is not particularly hard.[11] By a brute force search we were even able to find such a subfamily indexed by an elliptic curve of rank 5.

**Proposition 2.4.3.** *There exists a (rational) map $m : B(\mathbb{Q}) \to \mathbb{Q}$, where $B$ is the rank 5 elliptic curve given by*

$$B : y^2 = x^3 - 831594956135615443677x + 421873369731752773385520974 1004$$

*with conductor*

$$2^5 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 41 \cdot 53 \cdot 229^2 \cdot 1297 \cdot 1559$$

*such that for almost all $T \in B(\mathbb{Q})$ the curve $D_{m(T)}$ has at least rank 5.*

However, it turns out (perhaps unsurprisingly) that the Diophantus curves corresponding to the points on $B(\mathbb{Q})$ have extremely large coefficients and are therefore difficult to handle. For example, the smallest value of $m$ corresponding to one of the points on $B$ is $m = 31850580760/1260037009$, with the additional independent points

$$(-306884/35497, 1504509862/1260037009),$$
$$(1414529/141988, 405439253819/10080296072),$$
$$(-241572/35497, 22909564130/1260037009).$$

The conductor of this curve factors as

$$2^5 \cdot 7^2 \cdot 11^2 \cdot 193 \cdot 461^2 \cdot 4049425972295243 \cdot 888837286159506556027446 1.$$

It is easy to confirm that this curve indeed has rank *at least* 5, simply by calculating the determinant of the height matrix of the points that the algorithm gives us. However, actually determining the exact rank proves very difficult because of the large constants involved, and, for example `Sage` gives up rather quickly. Unfortunately, this is a theme among the curves we construct this way, and we were unable to determine the rank of any curve constructed by the above algorithm.

### 2.4.1 An equation for the indexing curve

In [Eik04, Section 3.5] it is shown how a quartic equation for the elliptic curve in proposition 2.4.2 is derived. In this section, we show that this approach works in general, and we provide the resulting equation for the general case (c.f. eq. (2.10)).

Let $m_0 \in \mathbb{Q}$, and let

$$R_1 = (x_1, y_1), \quad R_2 = (x_2, y_2), \quad R_3 = (x_3, y_3),$$

be points on $E_{m_0} : y^2 = x^3 - x + m_0^2$. Let $M_1(t_1), M_2(t_2), M_3(t_3)$ be the quadratic polynomials from proposition 2.4.1 corresponding to $R_1, R_2$ and $R_3$ respectively, and write

$$M_i = a_i t_i^2 + b_i t_i + m_0.$$

Recall that $M_1(0) = M_2(0) = M_3(0) = m_0$. The intersection $M_1(t_1) = M_2(t_2)$ defines a conic that has the point $(0,0)$, so we can parametrize all its rational points by considering lines through $(0,0)$. We set $t_2 = wt_1$ and obtain

$$a_1 t_1^2 + b_1 t_1 = a_2 w^2 t_1^2 + b_2 w t_1,$$

[10] It should be noted that this "almost all" in practice can be thought of as an "always"; examples where it fails are extremely hard to find, if they exist at all.

[11] It should be noted that `Sage` is not always able to actually compute the rank of these indexing curves. Curiously, in our tests `Sage` could only determine these ranks if they were nonzero. Suposedly, this is because the presence of a rational point reduces the ammount of work that needs to be done to complete the 2-descent.

which has the non-trivial solution

$$t_1(w) = \frac{b_2 w - b_1}{a_1 - a_2 w^2} \qquad \text{and} \qquad t_2(w) = \frac{b_2 w - b_1}{a_1 - a_2 w^2} \cdot w. \tag{2.7}$$

The intersection thus consists of the points in the image of

$$\begin{aligned} M_{1,2}(w) = M_1(t_1(w)) = M_2(t_2(w)) &= a_1 \left( \frac{b_2 w - b_1}{a_1 - a_2 w^2} \right)^2 + b_1 \cdot \frac{b_2 w - b_1}{a_1 - a_2 w^2} + m_0 \\ &= \frac{m_0 a_2^2 w^4 - b_1 a_2 b_2 w^3 + (a_1 a_2^2 - 2a_1 a_2 m_0 + b_1^2 a_2) w^2 + (a_1 b_1 b_2 - 2a_1 b_1 a_2) w + a_1^2 m_0}{(a_1 - a_2 w^2)^2}. \end{aligned} \tag{2.8}$$

We now want to solve $M_{1,2}(w) = M_3(t_3)$. To clear the denominator in eq. (2.8) we set

$$t_3 = \frac{v}{(a_1 - a_2 w^2)} - \lambda \tag{2.9}$$

for a currently unknown $\lambda$, and we first calculate

$$\begin{aligned} M_3(t_3) \cdot (a_1 - a_2 w^2)^2 &= \left( a_3 \left( \frac{v}{a_1 - a_2 w^2} - \lambda \right)^2 + b_3 (\frac{v}{a_1 - a_2 w^2} - \lambda) + m_0 \right) \cdot (a_1 - a_2 w^2)^2 \\ &= a_3 v^2 + \left( -2a_3 (a_1 - a_2 w^2) \lambda + b_3 (a_1 - a_2 w^2) \right) v + a_3 \lambda^2 (a_1 - a_2 w^2)^2 \\ &\qquad - b_3 \lambda (a_1 - a_2 w^2)^2 + m_0 (a_1 - a_2 w^2)^2. \end{aligned}$$

Taking

$$\lambda = \frac{b_3 (a_1 - a_2 w^2)}{2a_3 (a_1 - a_2 w^2)} = \frac{b_3}{2a_3}$$

kills the $v$-term, and $M_{1,2}(w) = M_3(t_3)$ then gives us

$$\begin{aligned} A : a_3 v^2 = {} & m_0 a_2^2 w^4 - b_1 a_2 b_2 w^3 + (a_1 a_2^2 - 2a_1 a_2 m_0 + b_1^2 a_2) w^2 + (a_1 b_1 b_2 - 2a_1 b_1 a_2) w + a_1^2 m_0 \\ & - \left( \frac{b_3^2}{4a_3} (a_1 - a_2 w^2)^2 - \frac{b_3^2}{2a_3} (a_1 - a_2 w^2)^2 + m_0 (a_1 - a_2 w^2)^2 \right) \end{aligned} \tag{2.10}$$

This (generally) defines a genus 1 curve [Cas91, Chapter 8]. From the point $t_1 = t_2 = t_3 = 0$ we obtain a point on $A$ turning it into an elliptic curve, and this point can then (if one wishes) further be used to find a Weierstrass model of the curve. Finally, using eq. (2.7) and eq. (2.9) a point $(v, w)$ on $A$ can be turned into a value of $m$ such that $D_m$ (at least generically) has rank 5.

# Appendix A

# Galois cohomology and Selmer groups

In this thesis we study the theory of descent through (Galois) cohomology. In (co)homology a series of algebraic objects is in a functorial way assigned to an object of interest. This concept is for example used frequently in algebraic topology to study topological spaces. In this thesis we will only consider Galois-cohomology, that is, the cohomology theory of $G_K$-modules. We will moreover only define the zeroth and first cohomology groups, as those are sufficient for our goals. A full overview can be found in [Ser79] or [Sil09].

## A.1 Galois cohomology

In what follows we will use the following notation. Let $K$ be a field, we let $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$ denote the absolute Galois group of $K$, which if $K$ is perfect equals $\mathrm{Gal}(\bar{K}/K)$. We will always assume that we have chosen some fixed algebraic closure $\bar{K}$. In the following we will deal with $G_K$-modules, which in line with [Mil06] we will always write as a left action. In order to define Galois cohomology we need some elementary definitions.

**Definition A.1.1.** *Let $K$ be a perfect field. The **Krull topology** on $G_K$ is the the topology with basis around 1 given by $\{N \subseteq G_K : N$ normal and finite index$\}$. By Galois theory such $N$ equal the set of automorphisms that leave some finite field extension $L/K$ fixed.*

**Definition A.1.2.** *A (discrete) $G_K$-module is an abelian group $M$ with a group action of $G_K$ which is continuous with respect to the topology on $G_K$ and the discrete topology on $M$. Equivalently, for $m \in M$, $\mathrm{Stab}(m)$ will be of finite index.*

**Definition A.1.3.** *Let $M$ be a $G_K$-module. The 0-th cohomology group of $M$ is*

$$H^0(K, M) = \{m \in M : \sigma m = m \text{ for all } \sigma \in G_K\}.$$

*We moreover define (assuming $M$ has the discrete topology)*

$$C^1(K, M) = \{\text{Continuous maps } G_K \to M\},$$

*the **group of continuous 1-cocycles from $G_K$ to $M$** as*

$$Z^1(K, M) := \{\zeta \in C^1(K, M) : (\forall \sigma, \tau \in G_K)(\zeta(\sigma\tau) = \zeta(\sigma) + \sigma\zeta(\tau))\},$$

*the **group of 1-coboundaries from $G_K$ to $M$** as*

$$B^1(K, M) := \{\zeta \in C^1(K, M) : (\exists m \in M)(\forall \sigma \in G_K)(\zeta(\sigma) = \sigma m - m)\},$$

*and finally the 1-st cohomology group of $M$ as*

$$H^1(K, M) := \frac{Z^1(K, M)}{B^1(K, M)}.$$

Of course there does exist a more elegant definition of these cohomology groups, in which these groups (along with the higher cohomology groups) arise naturally as the cohomology groups of certain chain complexes. For this thesis however the explicit definitions above are sufficient. In any case, we have the following results.

**Remark A.1.4.** *If $M$ has the trivial $G_K$ action, then*

$$H^0(K, M) = M \qquad \text{and} \qquad H^1(K, M) = \{\text{continuous homomorphisms } G_K \to M\}.$$

**Theorem A.1.5.** *Let*

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

*be a short exact sequence of $G_K$-modules. Then there is an induced long exact sequence of cohomology groups*

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^0(K,L) & \longrightarrow & H^0(K,M) & \longrightarrow & H^0(K,N) \\ & & & \swarrow^{\delta} & & & \\ & & H^1(K,L) & \longrightarrow & H^1(K,M) & \longrightarrow & H^1(K,N) \\ & & & \swarrow & & & \\ & & \dots & & & & \end{array}$$

*The horizontal maps are simply those induced by $f$ and $g$. The map $\delta$ is defined as follows: Given an $n \in H^0(K, N)$, $\delta(n)$ is the function that on input $\sigma \in G_K$ takes an inverse $m \in M$ of $n$ under the surjection $g$, notes that $\sigma(m) - m$ is in the kernel of $g$ and thus in the image of the injection $f$, and then outputs $f^{-1}(\sigma(m) - m)$.*

This theorem is a special instance of theorem 1.3.1 in [Wei94].

## A.2 The Selmer group

Let $K$ be a number field, $E/K$ an elliptic curve and $O \in E(K)$ its neutral element. In this section we will define the Selmer group $\mathrm{Sel}_n(E/K)$ and the Tate–Shafarevich group $Ш(E/K)$.

From the short exact sequence

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{n} E \longrightarrow 0$$

we use theorem A.1.5 to obtain the long exact cohomology sequence

$$0 \longrightarrow E(K)[n] \longrightarrow E(K) \xrightarrow{n} E(K) \longrightarrow H^1(K, E[n]) \longrightarrow H^1(K, E) \xrightarrow{n} H^1(K, E) \longrightarrow \dots,$$

from which we can extract the short exact sequence

$$0 \longrightarrow E(K)/nE(K) \longrightarrow H^1(K, E[n]) \longrightarrow H^1(K, E)[n] \longrightarrow 0.$$

Repeating the same process for every place $v$ of $K$, we get a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/nE(K) & \xrightarrow{(1)} & H^1(K, E[n]) & \longrightarrow & H^1(K,E)[n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_v E(K_v)/nE(K_v) & \longrightarrow & \prod_v H^1(K_v, E[n]) & \longrightarrow & \prod_v H^1(K_v,E)[n] & \longrightarrow & 0, \end{array}$$

Here in line with theorem A.1.5 the map (1) is explicitly given by $P \mapsto (\sigma \mapsto \sigma Q - Q)$, where $Q \in E(\bar{K})$ is chosen such that $[n]Q = P$. With this diagram in mind we are ready to define the Selmer group.

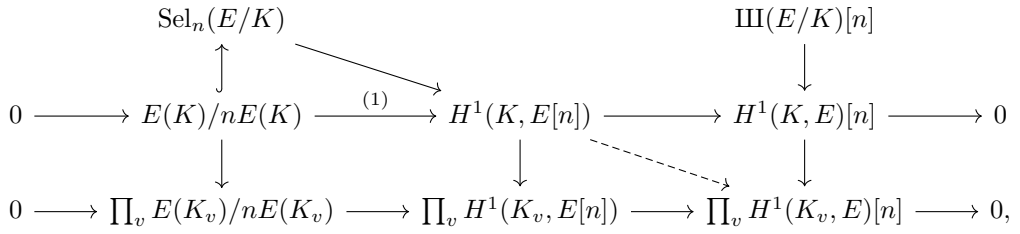
**Definition A.2.1.** *With $K, E$ and $n$ as above, we define the Selmer group $\mathrm{Sel}_n(E/K)$ as the kernel of the natural map*

$$H^1(K, E[n]) \longrightarrow \prod_v H^1(K_v, E)[n].$$

*We similarly define the Tate–Shafarevich group $Ш(E/K)$ as the kernel of the map*

$$H^1(K, E) \longrightarrow \prod_v H^1(K_v, E).$$

Note that by exactness of the top row the image of $E(K)/nE(K)$ lies within the kernel of the map $H^1(K, E[n]) \to H^1(K, E)$, and hence also in the Selmer group. It follows that we can extend our diagram to:




where both rows, the diagonal and the right column are exact.

**Remark A.2.2.** *From the above diagram we can obtain a short exact sequence*

$$0 \longrightarrow E(K)/nE(K) \longrightarrow \mathrm{Sel}_n(E/K) \longrightarrow Ш(E/K)[n] \longrightarrow 0.$$

*This shows that in some ways* Ш$(E/K)[n]$ *measures how much* $E(K)/nE(K)$ *(the group we are ultimately interested in) differs from* Sel$_n(E/K)$ *(the group we are more easily able to compute).*

## A.3 Local field theory

The main goal of this section is to prove proposition A.3.7, which is used to provide local conditions on elements of the Selmer group for both rational and irrational torsion. We start with some classical results on local field theory. The following two lemmas are theorems II.(4.6) and II.(4.8) in [NS13] respectively.

**Lemma A.3.1** (Hensel)**.** *Let $\mathcal{K}$ be a complete field with respect to a non-archimedean valuation, and let $A$ the valuation ring of $K$ with maximal ideal $\mathfrak{m}$. If $f \in A[X]$ factors as $\bar{f} = \bar{g}\bar{h}$ over $k = A/\mathfrak{m}$, then there are $g, h \in A[x]$ with reductions $\bar{g}, \bar{h}$ modulo $\mathfrak{m}$ such that $f = gh$, $\deg g = \deg \bar{g}$ and $\deg h = \deg \bar{h}$.*

**Lemma A.3.2.** *Let $\mathcal{K}$ be a complete non-archimedean field with valuation $v$, and let $\mathcal{L}/\mathcal{K}$ be a finite extensions. Then there exists exactly one extension of $v$ to a valuation on $\mathcal{L}$.*

**Definition A.3.3.** *Let $\mathcal{K}$ be a complete non-archimedean field with valuation $v$, let $\mathcal{L}/\mathcal{K}$ be a finite extension and let $v_{\mathcal{L}}$ be the unique extension of $v$ to $\mathcal{L}$. We say that the extension $\mathcal{K} \subseteq \mathcal{L}$ is* ***unramified*** *if the image of $v_{\mathcal{L}}$ equals the image of $v$.*

**Definition A.3.4.** *Let $\mathcal{K}$ be a complete non-archimedean field with separable closure $\mathcal{K}^{\mathrm{sep}}$. The* ***maximal unramified extension*** *$\mathcal{K}^{\mathrm{unr}}$ of $\mathcal{K}$ within $\mathcal{K}^{\mathrm{sep}}$ is defined as the union of all finite unramified subextensions $\mathcal{K} \subseteq \mathcal{L} \subseteq \mathcal{K}^{\mathrm{sep}}$.*

It should be noted that this definition makes sense as the composite of unramified field extensions is again unramified, see corollary II.(7.3) in [NS13].

We now have the following lemma. Here, for a field extension $K \subseteq L$ we write $\mathbb{T}_{L/K}$ for the category whose objects are subextensions $K \subseteq K' \subseteq L$ and the morphisms are inclusions.

**Lemma A.3.5.** *Let $\mathcal{K}$ be a complete non-archimedean field and let $\mathcal{K}^{\mathrm{sep}}$ be a separable closure of $\mathcal{K}$. Let $k$ be the residue field of $\mathcal{K}$ and let $k^{\mathrm{alg}}$ be an algebraic completion of $k$. Then there is an equivalence of categories*

$$\begin{aligned} \mathbb{T}_{\mathcal{K}^{\mathrm{unr}}/\mathcal{K}} &\xrightarrow{\sim} \mathbb{T}_{k^{\mathrm{sep}}/k}, \\ \mathcal{L} &\mapsto \ell, \end{aligned}$$

*which sends a field $\mathcal{L}$ to (a field isomorphic to) its residue field.*

*Proof.* See [Ste21, Theorem 4.2]. □

With this background in mind, we are now able to prove the following results on elliptic curves. These can also be found in section 4.3 in [Mil06].

**Lemma A.3.6.** *Let $\mathcal{K}$ be a finite extension of $\mathbb{Q}_p$, let $E$ be an elliptic curve over $\mathcal{K}$ with good reduction, and let $n \in \mathbb{Z}$ not divisible by $p$. Then for every $P \in E(\mathcal{K})$ there exists a finite unramified extension $\mathcal{L}$ of $\mathcal{K}$ such that $P \in nE(\mathcal{L})$.*

*Proof.* Let $k$ be the residue field of $\mathcal{K}$. Find an extension $\ell$ of $k$ such that $\bar{P} \in \bar{E}(k)$ is in $n\bar{E}(\ell)$. The $\mathcal{L} \supseteq \mathcal{K}$ corresponding to $\ell$ under the equivalence of categories given in lemma A.3.5 does the job: the equation $Q = nP$ (here $n$ and $P$ are fixed) can be solved over the residue field $\ell$, and so by Hensel's lemma (lemma A.3.1) it can also be solved over $\mathcal{L}$ itself. □

Having done all the preliminaries, we are now able to prove the following proposition.

**Proposition A.3.7.** *Let $E/K$ be an elliptic curve with discriminant $\Delta$. For every $\gamma \in \mathrm{Sel}_n(E/K)$ and every finite place $v$ of $K$ that does not divide $n\Delta$ (i.e. $v(n\Delta) = 0$) there exists a finite unramified extension $\mathcal{L}$ of $K_v$ such that $\gamma$ maps to 0 in $H^1(\mathcal{L}, E[n])$.*

*Proof.* Let $\gamma_v$ denote the image of $\gamma$ in $H^1(K_v, E[n])$. Recall that we have a short exact sequence

$$0 \longrightarrow E(K_v)/nE(K_v) \longrightarrow H^1(K_v, E[n]) \longrightarrow H^1(K_v, E)[n] \longrightarrow 0.$$

Since $\gamma$ lies in $\mathrm{Sel}_n(E/K)$, by definition it follows that $\gamma_v$ maps to 0 under the map $H^1(K_v, E[n]) \to H^1(K_v, E)[n]$. By exactness, $\gamma_v$ is thus the image of some $\bar{P} \in E(K_v)/nE(K_v)$ with lift $P \in E(K_v)$. Now by lemma A.3.6 there is an unramified extension $\mathcal{L} \supseteq K_v$ such that $P$ is in $nE(\mathcal{L})$. Then by commutativity of the diagram

$$\begin{array}{ccc} \bar{P} \in E(K_v)/nE(K_v) & \longrightarrow & H^1(K_v, E[n]) \ni \gamma_v \\ \downarrow & & \downarrow \\ 0 \in E(\mathcal{L})/nE(\mathcal{L}) & \longrightarrow & H^1(\mathcal{L}, E[n]) \ni 0 \end{array}$$

it follows that $\gamma_v$ maps to 0 in $H^1(\mathcal{L}, E[n])$, and so $\gamma$ does as well. □

# Appendix B

# Shapiro's lemma

The purpose of this appendix is to discuss Shapiro's lemma, and to make the isomorphism that it provides explicit in both directions, on degree one cohomology. Let $G$ be a group, and $M$ a left module of a finite-index subgroup $H$ of $G$. Shapiro's lemma states that, for any $n \geq 1$, the restriction-projection map (discussed below)

$$\text{res} \ : \ H^n(G, \text{Ind}_H^G(M)) \longrightarrow H^n(H, M),$$

is an isomorphism. The main purpose of this appendix is to make the inverse isomorphism explicit for the case $n = 1$, which we need for the cohomological treatment of irreducible 2-descent in section 1.2.2.

Let $\{g_i\}_{i \in I}$ be a full set of coset representatives of $H$, i.e. $|I| = [G : H]$ and $G = \sum_{i \in I} g_i H$, where without loss of generality we assume that $1 \in I$ and $g_1 = 1$. Consider a cohomology class $[\phi] \in H^1(G, \text{Ind}_H^G(M))$, represented by a cocycle

$$\phi : G \longrightarrow \text{Ind}_H^G(M) = \bigoplus_{i \in I} [g_i] \cdot M$$

Composition of the cocycle $\phi$ with the natural projection map to the first factor $i = 1$ gives us a map from $G$ to $M$ whose restriction to $H$ is denoted by $\phi_H : H \to M$. It may be verified directly that $\phi_H$ is a 1-cocycle, and that $\phi_H$ is a coboundary if $\phi$ is a coboundary. Passing to the associated cohomology classes, the association $[\phi] \mapsto [\phi_H]$ defines the restriction map res mentioned above.

To explicate the inverse isomorphism provided by Shapiro's lemma, we need some more notation. For $\sigma \in G$ and an index $i \in I$ we define the index $\sigma(i) \in I$ and the map $h_i : G \to H$ by

$$\sigma g_i = g_{\sigma(i)} h_i(\sigma).$$

That is, $\sigma g_i$ lies in some coset $g_j H$ and is thus of the form $g_j h$ for some $h \in H$. We define $\sigma(i) = j$ and $h_i(\sigma) = h$. We then have the following explicit version of Shapiro's lemma in degree one cohomology:

**Theorem B.0.1.** *With $G, H$ and $M$ as before, the restriction map*

$$\text{res} : H^1(G, \text{Ind}_H^G(M)) \longrightarrow H^1(H, M)$$

*is an isomorphism, and its inverse is given by the map $T$ that sends a cohomology class $[\psi]$ with representative $\psi : H \to M$ to the cohomology class of the map*

$$\sigma \longmapsto \sum_{i \in I} [g_i] \cdot \psi(h_{\sigma^{-1}(i)}(\sigma)) = \sum_{i \in I} [g_{\sigma(i)}] \cdot \psi(h_i(\sigma)).$$

*Proof.* There are a few things to check. First of all, we of course need to show that res and $T$ are well defined, in the sense that they are independent of the chosen representatives. Secondly, we need to show that they both indeed map into $Z^1(H, M)$ and $Z^1(G, \text{Ind}_H^G(M))$ respectively, such that their images indeed define cohomology classes. Lastly, we of course need to show that they are inverse to each other.

- First note that when we restrict a map $\phi : G \to \mathrm{Ind}_H^G(M)$ of the form

$$\sigma \mapsto \sigma \left( \sum_{i \in I} [g_i] m_i \right) - \sum_{i \in I} [g_i] m_i$$

to $H$, then by remark 1.2.1 the 1-component of this restriction is simply

$$\sigma \mapsto (h_1(\sigma) m_1 - m_1) = \sigma m_1 - m_1,$$

which is indeed a 1-coboundary. res is thus representative independent. Moreover, given a map $\psi : H \to M$ of the form $\sigma \mapsto \sigma m - m$, we find that

$$\begin{aligned} \sum_{i \in I} [g_i] \psi(h_{\sigma^{-1}(i)}(\sigma)) &= \sum_{i \in I} [g_i](h_{\sigma^{-1}(i)}(\sigma) \cdot m - m) = \sum_{i \in I} [g_{\sigma(i)}](h_i(\sigma) \cdot m - m) \\ &= \sigma \cdot \left( \sum_{i \in I} [g_i] m \right) - \sum_{i \in I} [g_i] m. \end{aligned}$$

As this is indeed a 1-coboundary, we conclude that $T$ is also representative independent.

- Let $\phi : G \to \mathrm{Ind}_H^G(M)$ be a 1-cocycle. Then restricted to $H$, the cocycle condition $\phi(\sigma\tau) = \phi(\sigma) + \sigma\phi(\tau))$ tells us that for any $\sigma, \tau \in H$ we have

$$\begin{aligned} \phi(\sigma\tau) &= \sum_{i \in I} [g_i] \phi_i(\sigma) + \sigma \sum_{i \in I} [g_i] \phi_i(\tau) \\ &= \sum_{i \in I} [g_i] \phi_i(\sigma) + \sum_{i \in I} [g_{\sigma(i)}] h_i(\sigma) \phi_i(\tau) \\ &= \sum_{i \in I} [g_i] \phi_i(\sigma) + \sum_{i \in I} [g_i] h_{\sigma^{-1}(i)}(\sigma) \phi_{\sigma^{-1}(i)}(\tau), \end{aligned}$$

and so the 1-component of this restriction is as expected equal to

$$\phi_1(\sigma) + h_{\sigma^{-1}(1)}(\sigma) \phi_{\sigma^{-1}(1)}(\tau) = \phi_1(\sigma) + \sigma\phi_1(\tau),$$

where we again used remark 1.2.1. In other words, if we restrict the $G$ action on $\mathrm{Ind}_H^G(M)$ to $H$, then it does not mix the different components/acts diagonally, and so the cocycle condition of $\phi$ directly implies the restriction of the 1-component has the same property. [1] Thus res indeed sends cocycles to cocycles. Moreover, given a cocycle $\psi : H \to M$ and elements $\sigma, \tau \in G$, we find that

$$\begin{aligned} T(\psi)(\sigma\tau) &= \sum_{i \in I} [g_i] \psi(h_{(\sigma\tau)^{-1}(i)}(\sigma\tau)) \\ &= \sum_{i \in I} [g_i] \psi(h_{\tau((\sigma\tau)^{-1}(i)}(\sigma) h_{(\sigma\tau)^{-1}(i)}(\tau)) \\ &= \sum_{i \in I} [g_i] \psi(h_{\sigma^{-1}(i))}(\sigma) h_{(\sigma\tau)^{-1}(i)}(\tau)) \\ &= \sum_{i \in I} [g_i] \psi(h_{\sigma^{-1}(i))}(\sigma)) + h_{\sigma^{-1}(i)}(\sigma) \psi(h_{(\sigma\tau)^{-1}(i)}(\tau)) \\ &= \sum_{i \in I} [g_i] \psi(h_{\sigma^{-1}(i))}(\sigma)) + \sum_{i \in I} [g_{\sigma(i)}] h_i(\sigma) \psi(h_{\tau^{-1}(i)}(\tau)) \\ &= T(\psi)(\sigma) + \sigma T(\psi)(\tau) \end{aligned}$$

which gives the required result for $T$ as well.

- To complete the proof, we must show that $T$ is indeed the inverse of res. Since res is an isomorphism, it is sufficient to show a single direction. If $\psi : G \to \mathrm{Ind}_H^G(M))$ is a 1-cocycle, then we have

$$(\mathrm{res} \circ T)(\psi) = (\sigma \mapsto T(\psi)_1(\sigma))|_H = \big(\sigma \mapsto \psi(h_{\sigma^{-1}(1)}(\sigma))\big)\big|_H = \psi,$$

which completes the proof.

□

[1] Note that restriction to $H$ here is necessary, the components of cocycles need not be cocycles.

# Bibliography


[Bac90] E. Bach. Explicit bounds for primality testing and related problems. *Mathematics of computation*, 55(191):355–380, 1990.

[Bas97] I. G. Bashmakova. *Diophantus and Diophantine Equations*. The Mathematical Association of America, 1997.

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3-adic exercises. *Journal of the American Mathematical Society*, 14(4):843–939, 2001.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BM02] E. Brown and B. T. Myers. Elliptic curves from Mordell to Diophantus and back. *The American mathematical monthly*, 109(7):639–, 2002.

[BMSW07] B. Bektemirov, B. C. Mazur, W. Stein, and M. Watkins. Average ranks of elliptic curves: Tension between data and conjecture. *Bulletin of the American Mathematical Society*, 44, 2007.

[Bru92] A. Brumer. The average rank of elliptic curves 1. *Inventiones mathematicae*, 109(3):445–472, 1992.

[BS15] M. Bhargava and A. Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Annals of mathematics*, 181(2):587–621, 2015.

[Cas91] J. W. S. Cassels. *Lectures on elliptic curves*. London Mathematical Society student texts; 24. Cambridge University Press, Cambridge, 1991.

[CO23] J. Christianidis and J. Oaks. *The Arithmetica of Diophantus : a complete translation and commentary*. Scientific Writings from the Ancient and Medieval World. Routledge, Abingdon, Oxon, England, first edition, 2023.

[Coh93] H. Cohen. *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics, 138. Springer Berlin Heidelberg, Berlin, Heidelberg, 1993.

[Cre92] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge [etc, 1992.

[DD11] T. Dokchitser and V. Dokchitser. Root numbers and parity of ranks of elliptic curves. *Journal für die reine und angewandte Mathematik*, 2011(658):39–64, 2011.

[DEvH+21] M. Derickx, A. Etropolski, M. van Hoeij, J. S. Morrow, and D. Zureick-Brown. Sporadic cubic torsion. *Algebra & Number Theory*, 15(7):1837–1864, 2021.

[DN25] M. Derickx and F. Najman. Classification of torsion of elliptic curves over quartic fields, 2025.

[Dri73] V. G. Drinfel'd. Two theorems on modular curves. *Functional analysis and its applications*, 7(2):155–156, 1973.

[Duj24] A. Dujella. History of elliptic curves rank records. `https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html`, 2024. Online; accessed 10 August 2025.

[Eik04] E. V. Eikenberg. *Rational points on some families of elliptic curves*. University of Maryland, College Park, 2004.

[EK24] N. D. Elkies and Z. Klagsbrun. The first rank 29 elliptic curve. `https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html`, 2024. Accessed: 2024-08-30.

[GJP+09] G. Grigorov, A. Jorza, S. Patrikis, W. A. Stein, and C. Tarniţă. Computational verification of the Birch and Swinnerton–Dyer conjecture for individual elliptic curves. *Mathematics of computation*, 78(268):2397–2425, 2009.

[gro25] The PARI group. `Pari/GP` documentation. `https://pari.math.u-bordeaux.fr/dochtml/html/`, 2025. Online; accessed 10 August 2025.

[GZ85] B. Gross and D. Zagier. Heegner points and derivatives of $L$-series. *Invent. math.*, 84:225–320, 1985.

[Kam92] S. Kamienny. Torsion points on elliptic curves and $q$-coefficients of modular forms. *Inventiones mathematicae*, 109(2):221–229, 1992.

[KM88] M. A. Kenku and F. Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya mathematical journal*, 109:125–149, 1988.

[Kod63] K. Kodaira. On compact analytic surfaces: Ii. *Annals of mathematics*, 77(3):563–626, 1963.

[Kol89] V. A. Kolyvagin. Finiteness of $E(\mathbb{Q})$ and Ш$(E, \mathbb{Q})$ for a subclass of Weil curves. *Mathematics of the USSR. Izvestiya*, 32:523–, 1989.

[Mer96] L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Inventiones mathematicae*, 124(1-3):437–449, 1996.

[Mil06] J. S. Milne. *Elliptic curves*. World Scientific, 2006.

[Mor22] L.J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Camb. Phil. Soc.*, 22:179–192, 1922.

[MPD93] Y. V. Matiyasevich, H. Putnam, and M. Davis. *Hilbert's tenth problem*. Foundations of computing. MIT Press, Cambridge, Mass, 1993.

[Né64] A. Néron. Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. *Publications mathématiques. Institut des hautes études scientifiques*, 21(1):5–125, 1964.

[Nag92] K.-I. Nagao. Examples of elliptic curves over $\mathbb{Q}$ with rank $\geq 17$. *Proc. Japan Acad. Ser. A Math. Sci.*, 68(9):287–289, 1992.

[Nag93] K.-I. Nagao. An example of elliptic curve over $\mathbb{Q}$ with rank $\geq 20$. *Proc. Japan Acad. Ser. A Math. Sci*, 69(8):291–293, 1993.

[NS13] J. Neukirch and N. Schappacher. *Algebraic number theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften*. Springer, 1999 edition, 2013.

[NSW13] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*, volume 323. Springer Science & Business Media, 2013.

[OS91] K. Oguiso and T. Shioda. The Mordell-Weil lattice of a rational elliptic surface. *Comment. Math. Univ. St. Pauli*, 40, 1991.

[Par99] P. Parent. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *Journal für die reine und angewandte Mathematik*, 1999(506):85–116, 1999.

[PPVW19] J. Park, B. Poonen, J. Voight, and M. M. Wood. A heuristic for boundedness of ranks of elliptic curves. *Journal of the European Mathematical Society : JEMS*, 21(9):2859–2903, 2019.

[RS17] K. A. Ribet and W. A. Stein. Lectures on modular forms and hecke operators. `https://wstein.org/books/ribet-stein/main.pdf`, 2017. Online; accessed 22 July 2025.

[Šaf63] I. R. Šafarevič. Algebraic number fields. *Amer. Math. Soc. Trans*, 31:25–39, 1963.

[Ser79] J.-P. Serre. *Galois cohomology*. Springer, 1979.

[Sil09] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.

[Sil13] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer, New York, NY, 1 edition, 2013.

[Smi17] A. Smith. $2^\infty$-selmer groups, $2^\infty$-class groups, and Goldfeld's conjecture, 2017.

[SS19] M. Schütt and T. Shioda. *Mordell-Weil Lattices*, volume 70 of *A Series of Modern Surveys in Mathematics*. Springer Nature, Singapore, 1st edition, 2019.

[Ste21] P. Stevenhagen. Voortgezette getaltheory. `https://pub.math.leidenuniv.nl/~stevenhagenp/VG.pdf`, 2021. Online; accessed 10 August 2025.

[The20] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.2)*, 2020. `https://www.sagemath.org`.

[TS67] J. T. Tate and I. R. Shafaravic. The rank elliptic curves. *Akad. Nauk SSSR*, 175(4):770–773, 1967.

[Was08] L. C. Washington. *Elliptic curves: number theory and cryptography*. CRC press, 2008.

[Wei29] A. Weil. L'arithmétique sur les courbes algébriques. *Acta mathematica*, 52:281–315, 1929.

[Wei94] C. A. Weibel. *An introduction to homological algebra*. Cambridge university press, 1994.