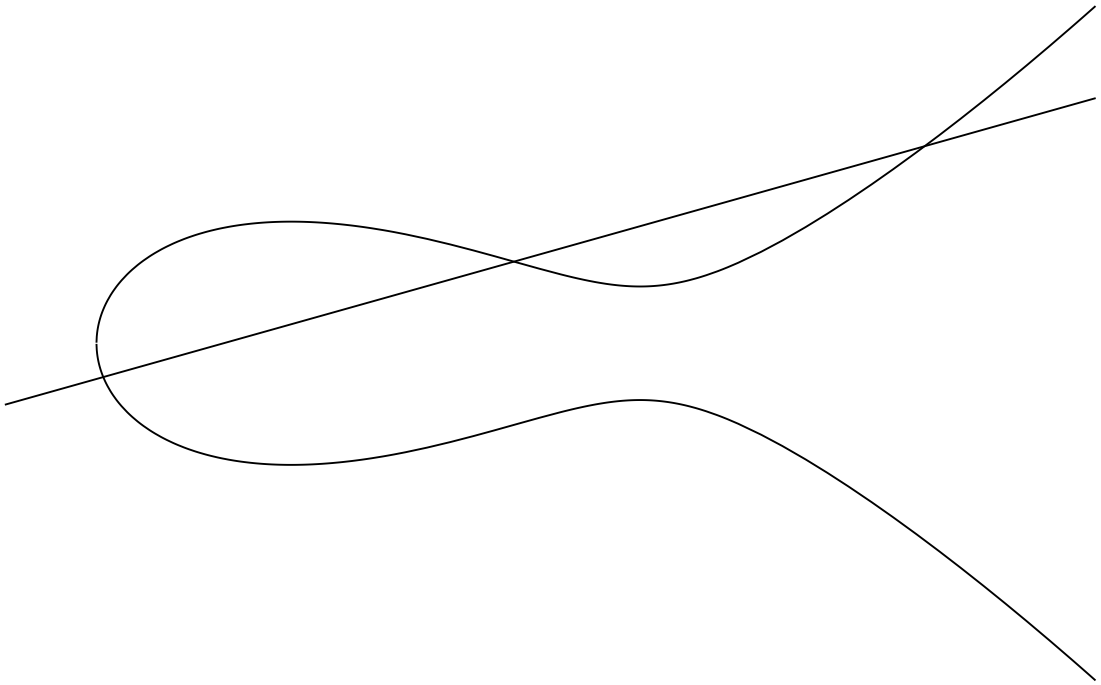
On Elliptic Curves of the Form $y^2 = x^3 + A(x - B)^2$

Monique van Beek



Institute for Mathematics and Computing Science

RuG

Master's thesis

On Elliptic Curves of the Form $y^2 = x^3 + A(x - B)^2$

Monique van Beek

Supervisor:
Jaap Top
2nd Reader:
Devrim Kaba
University of Groningen
Institute for Mathematics and Computing Science
P.O. Box 800
9700 AV Groningen
The Netherlands

July 2010

Abstract

In this thesis, theory is sought about the rank of elliptic curves of the form $E : y^2 = x^3 + A(x - B)^2$ with A and B integers. An isogenous curve $\overline{E}$ is defined. A pair of maps α and $\overline{\alpha}$ are given from $E \to \mathbb{Q}(\sqrt{A})^*/\mathbb{Q}(\sqrt{A})^{*3}$ and from $\overline{E} \to \mathbb{Q}(\sqrt{\overline{A}})^*/\mathbb{Q}(\sqrt{\overline{A}})^{*3}$, respectively. These maps are homomorphisms, and can be used to derive a formula for the rank of E. Some examples are given involving this rank formula. Finally, we attempt to discover the rank through suitable reductions of E modulo various primes.

Contents

Chapter 1

Introduction

Elliptic curves are fascinating entities. In this thesis, we shall choose a particular form of elliptic curves, and try to find out more about them. The chosen form consists of curves given by

$$E : y^2 = x^3 + A(x - B)^2$$

where A and B are integers. The form of elliptic curve studied in this thesis has received less attention than the form

$$C : y^2 = x(x^2 + ax + b).$$

This is unfair, although it is easy to see why this has occured. Curves of the form C contain an easy point of order 2, namely $(0, 0)$. Also, they can be studied without use of algebraic number theory. Although we need some knowledge of algebraic number theory to get some pleasing results about curves of the form E, the amount needed is not excessive.

We shall be especially interested in Γ, the group of rational points on this curve, and attempt to find out as much as possible about the rank of this group.

In chapter 2, there is a presentation of the information required to understand the rest of the thesis. In particular, section 2.3 is important, as it sketches the proof of the Mordell-Weil theorem, of which chapters 3 and 4 are a part. This proof is analogous to a proof found in [Tat92] and will follow very much the same lines. In chapter 5 a formula for the rank of Γ is derived. Chapter 6 contains a few examples to illustrate all we have found so far. We also attempt, using the computer program Magma [WB97], to construct a few curves with a high-rank Γ. In chapter 7 we then move on to investigating the rank of Γ armed with reduction maps.

Without further ado, let us now get stuck in, and get to work on our chosen kind of elliptic curves.

Chapter 2

Required Knowledge

The goal of this thesis is to study elliptic curves of the form

$$E : y^2 = x^3 + A(x - B)^2. \tag{2.1}$$

All of the information presented in this chapter is geared towards a better understanding of this specific form of elliptic curve. Although we may sometimes formulate definitions and theorems in a more general way, the reader should keep in mind that we shall only be applying them to curves of this form.

This chapter contains some basics, which can be skipped if the reader is already familiar with these concepts. Section 2.1 concerns the algebraic number theory that will be useful in our study of elliptic curves. Section 2.2 briefly states the most important definitions and concepts about elliptic curves themselves. Section 2.3 is concerned with the place that this thesis occupies in the literature. Many of the proofs in the thesis only make sense if this basic framework of the proof of the Mordell-Weil theorem is known. Section 2.4 deals with the points of order 3 on the curve E given in (2.1). These points will play an important part in this thesis, and therefore deserve a section to themselves.

2.1 A Bit of Algebraic Number Theory

An excellent source of information is [Ste08]. Some information specifically about quadratic number fields can be found in [Ros80]. Here we will go through some of the most important theory required in this thesis. The number fields we shall be working with will all be quadratic extensions of the field $\mathbb{Q}$, thus of the form $\mathbb{Q}(\sqrt{A})$ with A some squarefree integer.

Inside the number field $\mathbb{Q}(\sqrt{A})$ are many different number rings. There is, however, a unique number ring $O_{\mathbb{Q}(\sqrt{A})}$ called the *ring of integers* of $\mathbb{Q}(\sqrt{A})$. This ring of integers is the smallest Dedekind domain with field of fractions $\mathbb{Q}(\sqrt{A})$. This means that, although we may not have unique factorization in $O_{\mathbb{Q}(\sqrt{A})}$, we do have unique prime ideal factorization. We can even find out exactly what $O_{\mathbb{Q}(\sqrt{A})}$ is in each case:

$$O_{\mathbb{Q}(\sqrt{A})} = \begin{cases} \mathbb{Z}[\sqrt{A}] & \text{if } A \equiv 2, 3 \bmod 4; \\ \mathbb{Z}[\frac{1+\sqrt{A}}{2}] & \text{if } A \equiv 1 \bmod 4. \end{cases}$$

The Dirichlet unit theorem (see [Ste08]) tells us what to expect for the units of each of these rings of integers:

Theorem 1. *Let R be an order admitting r real and $2s$ complex embeddings, and write μ_R for the group of roots of unity in R. Then μ_R is finite, and R/μ_R is a free abelian group of rank $r + s - 1$.*

Thus any order $\mathbb{Z}[\sqrt{d}]$ with nonsquare $d < -1$ has just two units, namely $\{\pm 1\}$. Any such order with nonsquare $d > 1$ has units generated by -1 and some fundamental unit.

For any prime ideal $P \neq (0)$ in $O_{\mathbb{Q}(\sqrt{A})}$, we have that $P \cap \mathbb{Z} = p\mathbb{Z}$ for some prime number p. We say that P *lies over* p. Looking at this the other way around, any prime number p can exhibit one of three forms of behaviour:

1. The only prime ideal over p is (p).
2. The only prime ideal over p is $P \neq (p)$.
3. There are different prime ideals lying over p.

The Kummer-Dedekind theorem tells us exactly what happens to each prime number p (see [Ste08]). Summarizing the results for our specific number rings, whenever (p) is the only prime ideal over p, p is called *inert*. If $P \neq (p)$ is the only prime ideal lying over p, p is called *ramified* and we have $(p) = P^2$. If different prime ideals lie over p, p is called *split* and we have $(p) = P \cdot Q$ with $P \neq Q$.

These prime ideals need not necessarily be principal, and this will prove to be a crucial fact in this thesis.

A very useful entity is the class group of a number ring R. If R is a ring, let $\mathcal{P}(R)$ denote the principal fractional ideals and $\mathcal{I}(R)$ the invertible ideals. In a Dedekind ring, all ideals are invertible. This leads us to the following definition.

Definition 1. *The class group of a Dedekind ring R is defined as $Cl(R) = \mathcal{I}(R)/\mathcal{P}(R)$.*

An extremely important result about this group is that every ideal class of $Cl(R)$ contains an integral ideal of norm not exceeding the Minkowski constant

$$M_R = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^2} \cdot |\Delta(R)|^{\frac{1}{2}} .$$

Here, n is the degree of the number field, Δ is the discriminant, and s is the number of pairs of complex embeddings. Thus every prime ideal of norm greater than M_R can be written as a fractional principal ideal multiplied by some integral ideal of norm at most M_R.

Armed with this knowledge, we should be ready to tackle anything that may crop up.

2.2 Basics

In general, elliptic curves are curves given by equations of the form we call the Weierstrass normal form:

$$F : y^2 = f(x) = x^3 + ax^2 + bx + c \tag{2.2}$$

such that the (complex) roots of $f(x)$ are distinct. This means that the discriminant cannot be zero. The discriminant is given by

$$\Delta = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

In the cases we shall be studying, the elliptic curves will be of the form

$$E : y^2 = x^3 + A(x - B)^2$$

so the discriminant becomes

$$\Delta = A^2B^3(-4A - 27B).$$

There are many different kinds of solutions to (2.2) we might consider. Perhaps we would like to know all the complex solutions, or all the real solutions. In this thesis, we will be interested in finding all the rational solutions (x, y). There is some very useful theory concerning these solutions to be found in the literature. One first comment to make is that any rational solution (x, y) of the equation (2.2) will be of the form

$$(x, y) = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$$

where $m, n, e \in \mathbb{Z}$, $e > 0$, and $\gcd(m, e) = \gcd(n, e) = 1$. The proof of this statement can be found in [Tat92].

Highly important is the fact that the set of rational solutions of (2.2), together with the 'point at infinity' $\mathcal{O}$, form a commutative group. The group law is given by:

Group Law. *To add two points P and Q on the curve E, take the third intersection point of E with the straight line through P and Q. Call this third intersection point $P * Q$. Join $P * Q$ to $\mathcal{O}$, and take the third intersection point of this line with E to be $P + Q$. Thus by definition, $P + Q = \mathcal{O} * (P * Q)$.*

Bezout's theorem ensures that this third point of intersection always exists. The group of rational points so formed will henceforth be referred to as Γ. The most important property of this group for our purposes is that it is finitely generated. The next section gives further information concerning this fact.

The study of maps between elliptic curves is just as important as the study of the curves themselves. A very important kind of map between elliptic curves is called an *isogeny*, which respects the zero point $\mathcal{O}$.

Definition 2. *Let E_1 and E_2 be elliptic curves. An* isogeny *between E_1 and E_2 is a morphism*

$$\phi : E_1 \to E_2$$

satisfying $\phi(\mathcal{O}) = \mathcal{O}$. E_1 and E_2 are isogenous *if there is an isogeny ϕ between them with $\phi(E_1) \neq \{\mathcal{O}\}$.*

Such an isogeny of elliptic curves is always a homomorphism.

One of the easiest isogenies we can imagine is the multiplication by m map, denoted by $[m]$. We shall be using one particular such map, namely [3], together with a pair of dual isogenies Φ, Ψ. What this means is that we shall have

$$\Phi : E \to \overline{E}$$
$$\Psi : \overline{E} \to E$$

with

$$\Psi \circ \Phi = [3].$$

Let us give a pair of such dual isogenies precisely for the curves of the form E in (2.1). From [Top91], we find that the curves E and $\overline{E}$ are given by

$$E : y^2 = x^3 + A(x - B)^2$$
$$\overline{E} : \eta^2 = \xi^3 + \overline{A}(\xi - \overline{B})^2$$

such that $\overline{A} = -27A$ and $\overline{B} = 4A + 27B$. The first isogeny Φ is given by

$$\Phi : E \to \overline{E}$$
$$\Phi(x, y) = (\xi, \eta)$$

$$\xi = \frac{9}{x^2}\left(2y^2 + 2AB^2 - x^3 - \frac{2}{3}Ax^2\right)$$
$$\eta = \frac{27y}{x^3}\left(-4ABx + 8AB^2 - x^3\right).$$

The dual then becomes:

$$\Psi : \overline{E} \to \overline{\overline{E}}$$
$$\Psi(\xi, \eta) = (x, y)$$

$$x = \frac{9}{\xi^2}\left(2\eta^2 + 2\bar{A}\bar{B}^2 - \xi^3 - \frac{2}{3}\bar{A}\xi^2\right)$$
$$y = \frac{27\eta}{\xi^3}\left(-4\bar{A}\bar{B}\xi + 8\bar{A}\bar{B}^2 - \xi^3\right).$$

We see that if we take E and successively apply Φ and then Ψ, we end up in the curve $\overline{\overline{E}}$ given by the equation

$$\overline{\overline{E}} : y^2 = x^3 + 3^6A(x - 3^6B)^2.$$

By replacing y by 3^9y and x by 3^6x, and then dividing the equation by 3^{18}, we obtain the equation for E. Thus the group $\overline{\overline{\Gamma}}$ of rational points on $\overline{\overline{E}}$ is isomorphic to the group Γ of rational points on E.

These maps constitute an important tool in better understanding curves of the form we want to study.

2.3 The Mordell-Weil Theorem

Γ can be seen as a collection of points, some of which have finite order and some of which have infinite order. We want to show that Γ is finitely generated, a result that is known as the Mordell-Weil theorem. However, following [Tat92], we want to do it in just one specific form and thus obtain a simpler proof than can be found in [Sil86]. See also [Kna92] for details of the Mordell-Weil theorem.

Following [Tat92], we see that the proof of this theorem follows from four lemmas. Before stating these lemmas, we need to define a tool used in them. Let $P = (x, y)$ be a rational point on E. The *height* of P is defined as being the height of the x-coordinate of P:

$$\begin{aligned} H(P) = H(x) &= H\left(\frac{m}{e^2}\right) \\ &= \max\{|m|, |e^2|\}. \end{aligned}$$

The function h is then defined as

$$\begin{aligned} h(P) &= \log(H(P)) \\ h(\mathcal{O}) &= 0. \end{aligned}$$

The function h plays an important role in the following lemmas.

Lemma 1. *For every real number M, the set*

$$\{P \in \Gamma \mid h(P) \leq M\}$$

is finite.

This lemma is proved in [Tat92], exactly as it is stated here.

Lemma 2. *Let P_0 be a fixed rational point on E. There is a constant κ_0, depending on P_0 and on A, B so that*

$$h(P + P_0) \leq 3h(P) + \kappa_0$$

for all $P \in \Gamma$.

Proof. This is a slight variation of the lemma proved in [Tat92]. There it was proved that there is a constant κ_0 such that $h(P + P_0) \leq 2h(P) + \kappa_0$. This lemma is weaker, and follows directly from this result. □

Lemma 3. *There is a constant κ, depending on A, B, so that*

$$h(3P) \geq 9h(P) - \kappa$$

for all $P \in \Gamma$.

This is another variation of a lemma found in [Tat92]. However, it is necessary to modify the proof to obtain the result desired here. Because this is quite a lengthy business, the proof has been moved to appendix B on page 55.

Lemma 4. *The index* $(\Gamma : 3\Gamma)$ *is finite.*

Lemma 4 will be proved during the course of this thesis. We shall set out the steps of the proof here, but the real body of the proof is completed in other chapters.

Lemma 4 states that the subgroup 3Γ has finite index inside Γ. To prove this, we shall be using the pair of dual isogenies given at the end of the previous section. Recall that $\Psi \circ \Phi$ is the multiplication by 3 map on the elliptic curve E.

The proof further requires a map α, which is defined as follows:

$$\alpha : \Gamma \to \mathbb{Q}(\sqrt{A})^*/\mathbb{Q}(\sqrt{A})^{*3}$$

$$\alpha(P) = \begin{cases} 1 \cdot \mathbb{Q}(\sqrt{A})^{*3} & \text{if } P = \mathcal{O}; \\ (y + (x - B)\sqrt{A}) \cdot \mathbb{Q}(\sqrt{A})^{*3} & \text{otherwise.} \end{cases}$$

This map will be proved to be a homomorphism in chapter 3. It will then be shown to have a finite image in chapter 4. We can easily see that $\ker(\alpha) = \text{im}(\Psi(\overline{\Gamma}))$, and this will be proved in chapter 5. We will see in that chapter that it then follows that $(\Gamma : 3\Gamma)$ is indeed finite.

It is quite easy to prove the Mordell-Weil theorem from these lemmas, and this is what we shall finish this section with.

Theorem 2. *The group of rational points* Γ *on the elliptic curve* $E : y^2 = x^3 + A(x - B)^2$ *is a finitely generated group.*

Proof. Once again, this proof is a slight modification of a proof found in [Tat92]. First, we choose a representative for each coset of 3Γ in Γ. By lemma 4, we know there are only finitely many such cosets, say n. The representatives are

$$Q_1, \ldots, Q_n.$$

Any $P \in \Gamma$ is of course a member of one of the cosets described. For any P, there exists some index i_1, depending on P, such that

$$P - Q_{i_1} \in 3\Gamma.$$

Thus we can write

$$P - Q_{i_1} = 3P_1$$

for some $P_1 \in \Gamma$. Do the same with P_1 as we just did with P. Continuing in this manner, we obtain a list of equations

$$\begin{aligned} P - Q_{i_1} &= 3P_1 \\ P_1 - Q_{i_2} &= 3P_2 \\ P_2 - Q_{i_3} &= 3P_3 \\ &\vdots \\ P_{m-1} - Q_{i_m} &= 3P_m. \end{aligned}$$

Substituting the second equation in this list into the first gives

$$P = Q_{i_1} + 3Q_{i_2} + 9P_2.$$

Continuing substituting in this manner gives us

$$P = Q_{i_1} + 3Q_{i_2} + 9Q_{i_3} + \ldots + 3^{m-1}Q_{i_m} + 3^m P_m.$$

So P is in the subgroup of Γ generated by the Q_i's and P_m. Using lemma 2,

$$h(P - Q_i) \leq 3h(P) + \kappa_i.$$

We do this for all Q_i. Because of lemma 4, we know there are a finite number of the Q_i. This means that we can take the maximum of all the κ_i. Let

$$\kappa' = \max\{\kappa_i\}.$$

Then we have for all $P \in \Gamma$ and all i

$$h(P - Q_i) \leq 3h(P) + \kappa'. \tag{2.3}$$

From lemma 3, we have

$$9h(P_j) - \kappa \leq h(3P_j) \tag{2.4}$$

for some κ. Combining equations (2.3) and (2.4) we get

$$\begin{aligned} 9h(P_j) &\leq h(3P_j) + \kappa \\ &= h(P_{j-1} - Q_{i_j}) + \kappa \\ &\leq 3h(P_{j-1}) + \kappa' + \kappa. \end{aligned}$$

This can be rewritten as

$$\begin{aligned} h(P_j) &\leq \frac{1}{3}h(P_{j-1}) + \frac{\kappa' + \kappa}{9} \\ &= \frac{4}{9}h(P_{j-1}) - \frac{1}{9}\left(h(P_{j-1}) - (\kappa' + \kappa)\right). \end{aligned}$$

If we know that $h(P_{j-1}) \geq \kappa' + \kappa$ then

$$h(P_j) \leq \frac{4}{9}h(P_{j-1}).$$

So in the sequence of points $P, P_1, P_2, \ldots$ as long as the point P_j satisfies the condition $h(P_j) \leq \frac{4}{9}h(P_{j-1})$, then the next point in the sequence has much smaller height, namely $h(P_{j+1}) \leq \frac{4}{9}h(P_j)$. If you start with a number and keep multiplying it by $\frac{4}{9}$, then it approaches zero. This means that eventually we will get m such that $h(P_m) \leq \kappa' + \kappa$. Thus every element can be written in the form

$$P = a_1Q_1 + a_2Q_2 + \ldots + a_nQ_n + 3^m R$$

for $a_i \in \mathbb{Z}$ and $R \in \Gamma$ satisfying $h(R) \leq \kappa' + \kappa$. Thus

$$\{Q_1, \ldots, Q_n\} \cup \{R \in \Gamma \mid h(R) \leq \kappa' + \kappa\}$$

generates Γ. Lemmas 1 and 4 show these sets to be finite. Thus Γ is finitely generated, which is what we wanted to prove.

□

2.4 The Points of Order Dividing 3

The points of order dividing 3 will play an important part in several chapters to come. It is therefore a good idea to expand on this subject here. Let E be an elliptic curve of the form

$$E : y^2 = x^3 + A(x - B)^2.$$

If we allow complex points, we can find that there are exactly eight points of order 3 (see [Tat92]). These points are characterized by the following theorem.

Theorem 3. *A point $P = (x, y) \neq \mathcal{O}$ on E has order 3 if and only if x is a zero of the polynomial*

$$\gamma(x) = 3x^4 + 4Ax^3 - 12ABx^2 + 12AB^2x.$$

These eight points, together with the point $\mathcal{O}$, form an abelian group of nine points. The only such group in existence is a product of two cyclic groups of order 3.

Now we want to know how many of these points can be rational. We see that there are either 1, 3 or 9 rational points of order dividing 3 in Γ. It is easy to make curves containing either 1 or 3 rational points of order 3. An example of the first is $y^2 = x^3 + 2(x - 1)^2$, the only torsion point of which is $\mathcal{O}$. An example of the second is $y^2 = x^3 + (x - 1)^2$, where we have the torsion group equal to $\{\mathcal{O}, (0, \pm 1)\}$. The only remaining question is whether all 9 points can be rational. This turns out not to be the case, a result that follows from a theorem by Möbius, which is proved in [Top07].

Theorem 4. *$y = \sqrt{x^3 + ax^2 + bx + c}$ contains exactly one point of inflection if $x^3 + ax^2 + bx + c$ has only simple zeroes.*

In order to make use of this theorem, we need to analyse carefully the points of order 3 using the group law. Let $P \neq \mathcal{O}$ be some point of order 3 on the curve E. Take the tangent at P, call it L, and let the third point of intersection on this line be Q. Thus $P + P = 2P = -Q$. Now add P to $2P$. Take the straight line through P and $-Q$. Because P has order 3, the third point of intersection on this line must be $\mathcal{O}$. But this means that the line through P and $-Q$ is vertical. Thus $Q = P$, and we see that the line L has a triple point of intersection at P. This means precisely that P must be a point of inflection: see figure 2.1. Möbius' theorem then gives the result we wanted. Our curve consists of two pieces, namely

$$y = \sqrt{x^3 + ax^2 + bx + c}$$
$$y = -\sqrt{x^3 + ax^2 + bx + c}.$$

On each piece, there is precisely one point of inflection, so on E there are at most two real points of order 3. Of course, rational points must be real, so there can be at most two rational points of order 3. Thus there are at most three rational points of order dividing 3.

It is now time to analyse more closely precisely when Γ can contain these real points of order 3. The x-coordinate of such a point must be a zero of $\gamma(x) = x(3x^3 + 4Ax^2 - 12ABx + 12AB^2)$.

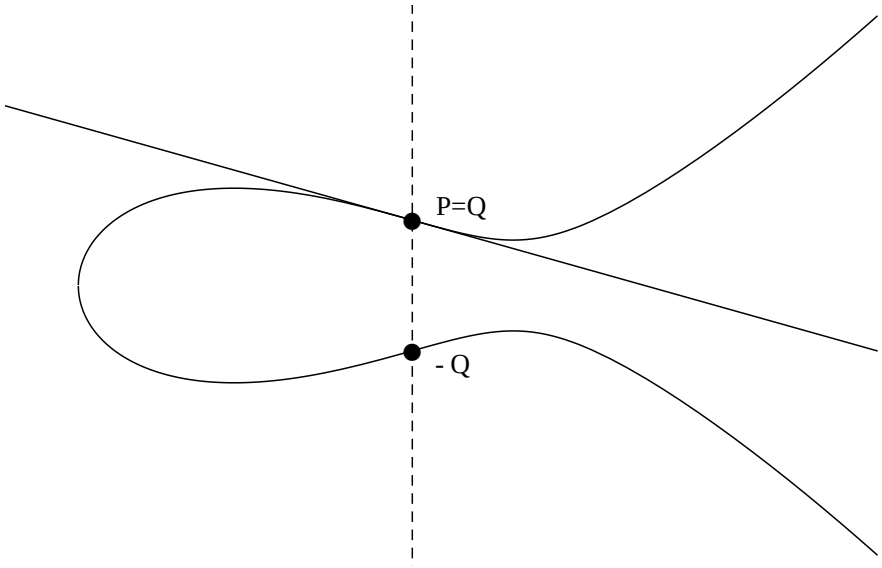


Figure 2.1: The Tangent at a Point of Order 3

The most obvious solution to the equation $\gamma(x) = 0$ is of course $x = 0$. This means that the point $(0, y)$ must be a point on E, so

$$y^2 = 0^3 + A(0 - B)^2 = AB^2$$

This will yield a rational result for y if and only if A is a perfect square, so $A = a^2$ for some $a \in \mathbb{Z}$. Whenever A is of this form, we always have two points of order 3 on Γ.

Now assume that there is some point of order 3 on the curve that has $x \neq 0$. In this case, we must have instead

$$3x^3 + 4Ax^2 - 12ABx + 12AB^2 = 0 \tag{2.5}$$

Multiplying the equation for E by 3, we obtain

$$3y^2 = 3x^3 + 3A(x - B)^2 \tag{2.6}$$

Subtracting (2.5) from (2.6) gives:

$$\begin{aligned} 3y^2 &= 3x^3 + 3A(x - B)^2 - (3x^3 + 4Ax^2 - 12ABx + 12AB^2) \\ &= 3Ax^2 - 6ABx + 3AB^2 - 4Ax^2 + 12ABx - 12AB^2 \\ &= -Ax^2 + 6ABx - 9AB^2 \\ &= -A(x - 3B)^2. \end{aligned}$$

We see that in this case we must have $A = -3a^2$ for some $a \in \mathbb{Z}$. Notice that this is not enough to guarantee points of order 3 on Γ. We only conclude that for it to be possible for Γ to contain points of order 3 with $x \neq 0$, it is imperative that A be of this form.

Let $\Gamma[3]$ denote the points of order dividing 3 in Γ. Then, summarizing our results for this section, we get

$$\#\Gamma[3] = \begin{cases} 3 & \text{if } A = a^2 \text{ and possibly when } A = -3a^2, \text{ for some } a \in \mathbb{Z}; \\ 1 & \text{otherwise.} \end{cases}$$

Chapter 3

A Useful Homomorphism

The homomorphism described below is not the one described as 'useful' by Tate in [Tat92]. However, because it is actually extremely useful, the name has been applied to it by me anyway.

The map has already been shown to be a homomorphism in, for example, [Top91]. However, the proof there is not very easy to understand without a lot of background knowledge. I take the opportunity here to prove, in a much easier, more direct way and using a lot less theory, that the map is, indeed, a homomorphism. Unfortunately, the proof is somewhat longer than in [Top91], but this is the price to pay for lucidity.

3.1 Description of the Map α

Consider an elliptic curve given by an equation of the form:

$$E : y^2 = x^3 + A(x - B)^2.$$

We see that

$$x^3 = y^2 - A(x - B)^2;$$

therefore

$$x^3 = (y + (x - B)\sqrt{A})(y - (x - B)\sqrt{A}). \tag{3.1}$$

The map $\alpha : \Gamma \to \mathbb{Q}(\sqrt{A})^*/\mathbb{Q}(\sqrt{A})^{*3}$ is defined as

$$\alpha(P) = \begin{cases} 1 \cdot \mathbb{Q}(\sqrt{A})^{*3} & \text{if } P = \mathcal{O}; \\ (y + (x - B)\sqrt{A}) \cdot \mathbb{Q}(\sqrt{A})^{*3} & \text{if } P = (x, y) \in \Gamma. \end{cases} \tag{3.2}$$

Now, α is well-defined if $y+(x-B)\sqrt{A} \neq 0$. This only goes wrong if $A = a^2$ and $P = (0, \pm aB)$. These points therefore need to be defined separately:

$$\alpha(0, aB) = \frac{1}{2aB} \cdot \mathbb{Q}^{*3}$$
$$\alpha(0, -aB) = 2aB \cdot \mathbb{Q}^{*3}$$

We see straight away because of (3.1) that the norm of any element in $\mathrm{im}(\alpha)$ is equal to a third power. This fact will prove useful later on. Before going any further, however, we need to prove α has the homomorphism property.

3.2 Proof of Homomorphism Property

Theorem 5. *α is a homomorphism.*

The proof of this theorem will depend on two lemmas, which we will first prove.

Lemma 5. $\alpha(-P) = \alpha(P)^{-1}$.

Proof. The lemma is obviously true if $P = \mathcal{O}$. Also, it clearly holds if A is a perfect square and P is one of the points of order 3. In all other cases, $x \neq 0$. We start with the fact that $-P = (x, -y)$. Thus

$$\begin{aligned}\alpha(-P) &= \alpha(x, -y) \\ &= (-y + (x - B)\sqrt{A}) \cdot \mathbb{Q}(\sqrt{A})^{*3}.\end{aligned}$$

We also have that

$$\alpha(P)^{-1} = \frac{1}{y + (x - B)\sqrt{A}} \cdot \mathbb{Q}(\sqrt{A})^{*3}.$$

By (3.1) we get

$$\begin{aligned}\alpha(P)^{-1} &= \frac{y - (x - B)\sqrt{A}}{x^3} \cdot \mathbb{Q}(\sqrt{A})^{*3} \\ &= (y - (x - B)\sqrt{A}) \cdot \mathbb{Q}(\sqrt{A})^{*3} \\ &= (-y + (x - B)\sqrt{A}) \cdot \mathbb{Q}(\sqrt{A})^{*3} \\ &= \alpha(-P)\end{aligned}$$

which is what we wanted to prove. □

Lemma 6. *Whenever $P_1 + P_2 + P_3 = \mathcal{O}$, then $\alpha(P_1)\alpha(P_2)\alpha(P_3) = 1 \cdot \mathbb{Q}(\sqrt{A})^{*3}$.*

Proof. We have a few trivial cases of this lemma, such as $P_1 = P_2 = P_3 = \mathcal{O}$ and, if $A = a^2$, $P_1 = (0, aB), P_2 = (0, -aB), P_3 = \mathcal{O}$, and it is obviously true in these cases. We now turn to the nontrivial case.

The triples of points which add to the zero element consist of the intersections of the elliptic curve with a straight line. Let the line be $y = \lambda x + \nu$ and the x coordinates of the intersections x_1, x_2, x_3. Substitute $y = \lambda x + \nu$ into the equation for the elliptic curve:

$$\begin{aligned}y^2 &= x^3 + A(x - B)^2 \\ (\lambda x + \nu)^2 &= x^3 + A(x - B)^2.\end{aligned}$$

Rearranging terms gives us

$$x^3 + (A - \lambda^2)x^2 + (-2AB - 2\lambda\nu)x + (AB^2 - \nu^2) = 0.$$

Now x_1, x_2, x_3 are the roots of the above equation, because these are the points of intersection of the line with the curve. Thus

$$\begin{aligned} x^3 + (A - \lambda^2)x^2 + (-2AB - 2\lambda\nu)x + (AB^2 - \nu^2) &= (x - x_1)(x - x_2)(x - x_3) \\ &= x^3 + (-x_1 - x_2 - x_3)x^2 + (x_2x_3 + x_1x_2 + x_1x_3)x - x_1x_2x_3. \end{aligned}$$

From this it follows that

$$\begin{aligned} x_1 + x_2 + x_3 &= \lambda^2 - A \\ x_2x_3 + x_1x_2 + x_1x_3 &= -2(AB + \lambda\nu) \\ x_1x_2x_3 &= \nu^2 - AB^2. \end{aligned} \tag{3.3}$$

Simply using the definition of α given by (3.2), we find

$$\begin{aligned} \alpha(P_1)\alpha(P_2)\alpha(P_3) &= (y_1 + (x_1 - B)\sqrt{A})(y_2 + (x_2 - B)\sqrt{A})(y_3 + (x_3 - B)\sqrt{A}) \\ = y_1y_2y_3 + y_1A(x_2 - B)(x_3 - B) + y_2A(x_1 - B)(x_3 - B) + y_3A(x_1 - B)(x_2 - B) \\ +\sqrt{A}\big(y_2y_3(x_1 - B) + y_1y_2(x_3 - B) + y_1y_3(x_2 - B) + A(x_1 - B)(x_2 - B)(x_3 - B)\big) \end{aligned} \tag{3.4}$$

where for $i = 1, 2, 3$, because (x_i, y_i) lies on the line $y = \lambda x + \nu$

$$y_i = \lambda x_i + \nu.$$

This we will substitute into equation (3.4). Then we will show that the right hand side of (3.4) is in fact equal to $(\nu - B\sqrt{A})^3$, a perfect cube. This is the desired result and will prove the lemma.

First look at the constant term. This term is

$$y_1y_2y_3 + y_1A(x_2 - B)(x_3 - B) + y_2A(x_1 - B)(x_3 - B) + y_3A(x_1 - B)(x_2 - B).$$

Substitute in $y_i = \lambda x_i + \nu$:

$$\begin{aligned} (\lambda x_1 + \nu)(\lambda x_2 + \nu)(\lambda x_3 + \nu) + (\lambda x_1 + \nu)A(x_2 - B)(x_3 - B) \\ +(\lambda x_2 + \nu)A(x_1 - B)(x_3 - B) + (\lambda x_3 + \nu)A(x_1 - B)(x_2 - B) \end{aligned}$$

which becomes, after some rewriting

$$\begin{aligned} \lambda^3x_1x_2x_3 + \lambda^2\nu(x_1x_2 + x_2x_3 + x_1x_3) + \lambda\nu^2(x_1 + x_2 + x_3) + \nu^3 + 3A\lambda x_1x_2x_3 \\ +A(\nu - 2\lambda b)(x_1x_2 + x_2x_3 + x_1x_3) + A(\lambda B^2 - 2B\nu)(x_1 + x_2 + x_3) + 3\nu B^2. \end{aligned}$$

But we know alternative ways of writing $x_1x_2x_3$, $x_1x_3 + x_2x_3 + x_1x_2$ and $x_1 + x_2 + x_3$ in terms of ν, λ, A, B. These were equations (3.3). These we substitute into the above to obtain:

$$\begin{aligned} \lambda^3(\nu^2 - AB^2) + \lambda^2\nu(-2(AB + \lambda\nu)) + \lambda\nu^2(\lambda^2 - A) + \nu^3 + A(3\lambda(\nu^2 - AB^2) \\ +(\nu - 2\lambda b)(-2(AB + \lambda\nu)) + (\lambda B^2 - 2B\nu)(\lambda^2 - A) + 3\nu B^2) \end{aligned}$$

which yields, after elimination:

$$\nu^3 + 3\nu AB^2. \tag{3.5}$$

Keeping this result in mind, we now move on to the $\sqrt{A}$ term from 3.4. This term is

$$y_2y_3(x_1 - B) + y_1y_2(x_3 - B) + y_1y_3(x_2 - B) + A(x_1 - B)(x_2 - B)(x_3 - B).$$

Again, substitute in $y_i = \lambda x_i + \nu$ to obtain

$$\begin{aligned}(\lambda x_2 + \nu)(\lambda x_3 + \nu)(x_1 - B) + (\lambda x_1 + \nu)(\lambda x_2 + \nu)(x_3 - B)\\ +(\lambda x_1 + \nu)(\lambda x_3 + \nu)(x_2 - B) + A(x_1 - B)(x_2 - B)(x_3 - B).\end{aligned}$$

Multiply out the brackets and rearrange terms to obtain

$$\begin{aligned}&3\lambda^2x_1x_2x_3 + 2\lambda\nu(x_1x_3 + x_2x_3 + x_1x_2) + \nu^2(x_1 + x_2 + x_3) - \lambda^2B(x_1x_3 + x_2x_3 + x_1x_2)\\ &- 2\lambda\nu B(x_1 + x_2 + x_3) - 3B\nu^2 + A\big(x_1x_2x_3 - B(x_1x_3 + x_2x_3 + x_1x_2) + B^2(x_1 + x_2 + x_3) - B^3\big).\end{aligned}$$

Once again, use equations (3.3) to substitute in for x_1, x_2, x_3. This gives us

$$\begin{aligned}&3\lambda^2(\nu^2 - AB^2) + 2\lambda\nu(-2(AB + \lambda\nu)) + \nu^2(\lambda^2 - A) - \lambda^2B(-2(AB + \lambda\nu)) - 2\lambda\nu B(\lambda^2 - A)\\ &- 3B\nu^2 + A\big(\nu^2 - AB^2 - B(-2(AB + \lambda\nu)) + B^2(\lambda^2 - A) - B^3\big)\end{aligned}$$

which yields, after elimination

$$-3B\nu^2 - AB^3. \tag{3.6}$$

Equations 3.5 and 3.6 can now be used to see that

$$\begin{aligned}\alpha(P_1)\alpha(P_2)\alpha(P_3) &= \nu^3 + 3\nu AB^2 + \sqrt{A}(-3B\nu^2 - AB^3)\\ &= (\nu - B\sqrt{A})^3.\end{aligned}$$

From this it follows that

$$\alpha(P_1)\alpha(P_2)\alpha(P_3) = 1 \cdot \mathbb{Q}(\sqrt{A})^{*3}$$

which is what we wanted to prove. □

We are now ready to complete the proof of theorem 5.

Proof. Let $P_1 + P_2 + P_3 = \mathcal{O}$. Then $P_1 + P_2 = -P_3$, and also $\alpha(P_1 + P_2) = \alpha(-P_3)$. By lemma 5, $\alpha(-P_3) = \alpha(P_3)^{-1}$. Thus

$$\alpha(P_1 + P_2) = \alpha(P_3)^{-1}. \tag{3.7}$$

Lemma 6 asserts that $\alpha(P_1)\alpha(P_2)\alpha(P_3) = 1$, which means that $\alpha(P_1)\alpha(P_2) = \frac{1}{\alpha(P_3)}$. Thus

$$\alpha(P_1)\alpha(P_2) = \alpha(P_3)^{-1}. \tag{3.8}$$

Using equations (3.7) and (3.8), we see that $\alpha(P_1 + P_2) = \alpha(P_1)\alpha(P_2)$, which is the homomorphism property. Thus we have proved that α is a homomorphism. □

Chapter 4

The Image of the Homomorphism α

For the map α to be useful in our investigation of the rank of Γ, we need to show it has a finite image. This will be done in two separate cases. In the first case, A is a perfect square. In the second case, A is anything but a perfect square.

4.1 Proof in the Case that A is a Perfect Square

In the first case, the elliptic curve is given by an equation of the form

$$y^2 = x^3 + a^2(x - B)^2$$

with $a, B \in \mathbb{Z}$. The map α then becomes

$$\alpha(x, y) = (y + a(x - B)) \cdot \mathbb{Q}^{*3}.$$

We want to prove that α has a finite image. Following [Tat92], let

$$x = \frac{m}{e^2}$$
$$y = \frac{n}{e^3}$$

with $\gcd(n, e) = \gcd(m, e) = 1$. This is substituted into the equation of the elliptic curve, giving

$$n^2 = m^3 + a^2m^2e^2 - 2a^2Bme^4 + a^2B^2e^6. \tag{4.1}$$

Factorize to obtain

$$m^3 = (n + ame - aBe^3)(n - ame + aBe^3).$$

Substituting $x = \frac{m}{e^2}, y = \frac{n}{e^3}$ into α gives

$$\begin{aligned} \alpha\left(\frac{m}{e^2}, \frac{n}{e^3}\right) &= \left(\frac{n}{e^3} + a\frac{m}{e^2} - aB\right) \cdot \mathbb{Q}^{*3} \\ &= (n + ame - aBe^3) \cdot \mathbb{Q}^{*3} \end{aligned}$$

It is important here to note that $\mathbb{Z}$ is a unique factorization domain. This means that if $(n+ame-aBe^3)$ and $(n-ame+aBe^3)$ have no prime factors in common, then $(n+ame-aBe^3)$

is a perfect cube. If this is the case, $\alpha(x, y) = 1 \cdot \mathbb{Q}^{*3}$.

Let us assume now that $n+ame-aBe^3$ and $n-ame+aBe^3$ do have prime factors in common. Let $d = \gcd(n + ame - aBe^3, n - ame + aBe^3)$. Then

$$n + ame - aBe^3 = d \cdot p_1^{r_1} \cdot \ldots \cdot p_t^{r_t} \cdot (\text{integer})^3$$

where $p_i|d$ and $r_i \in \mathbb{Z}$. Thus

$$\alpha(x, y) = d \cdot p_1^{r_1} \cdot \ldots \cdot p_t^{r_t} \cdot \mathbb{Q}^{*3}.$$

If we want to prove the image of α to be finite, we need to prove the following theorem.

Theorem 6. *The prime divisors of d are contained in a finite set.*

Proof. The first thing to do is to look more closely at d, and rewrite it.

$$\begin{aligned} d &= \gcd(n + ame - aBe^3, n - ame + aBe^3) \\ &= \gcd(n + ame - aBe^3, n - ame + aBe^3 - (n + ame - aBe^3)) \\ &= \gcd(n + ame - aBe^3, -2ame + 2aBe^3) \\ &= \gcd(n + ae(m - Be^2), -2ae(m - Be^2). \end{aligned}$$

Because n and e are relatively prime, so are $n + ae(m - Be^2)$ and e. Thus

$$d = \gcd(n + ae(m - Be^2), -2a(m - Be^2)).$$

There are only a fixed, finite number of primes in $-2a$. We will therefore only need to look at whether $d' = \gcd(n + ae(m - Be^2), m - Be^2)$ contains prime factors taken from a finite set.

If $n + ae(m - Be^2)$ and $m - Be^2$ have primes factors in common, then n and $m - Be^3$ have these same prime factors in common. Assume that we have

$$\begin{aligned} d &= p_1 \ldots p_i \\ n &= p_1 \ldots p_i s \\ m - Be^2 &= p_1 \ldots p_i t \end{aligned}$$

for some $s, t \in \mathbb{Z}$ with $\gcd(s, t) = 1$. Then, starting with equation (4.1):

$$\begin{aligned} n^2 &= m^3 + a^2m^2e^2 - 2a^2Bme^4 + a^2B^2e^6 \\ n^2 &= m^3 + a^2m^2e^2 - a^2Bme^4 - a^2Be^4(m - Be^2) \\ p_1^2 \ldots p_i^2 s^2 &= m^3 + a^2m^2e^2 - a^2Bme^4 - a^2Be^4(p_1 \ldots p_i t) \\ p_1^2 \ldots p_i^2 s^2 + a^2Be^4(p_1 \ldots p_i t) &= m^3 + a^2m^2e^2 - a^2Bme^4 \\ p_1 \ldots p_i(p_1 \ldots p_i s^2 + a^2Be^4 t) &= m^3 + a^2me^2(m - Be^2) \\ p_1 \ldots p_i(p_1 \ldots p_i s^2 + a^2Be^4 t) &= m^3 + a^2me^2(p_1 \ldots p_i t) \\ p_1 \ldots p_i(p_1 \ldots p_i s^2 + a^2Be^4 t - a^2me^2 t) &= m^3. \end{aligned}$$

But then $p_1 \dots p_i$ also divides m, thus the primes $p_1, \dots, p_i$ must be prime divisors of both m and n. It can now be seen from the equation for the elliptic curve in (4.1) which primes these can be:

$$n^2 = m^3 + a^2m^2e^2 - 2a^2Bme^4 + a^2B^2e^6$$
$$n^2 - m^3 - a^2m^2e^2 + 2a^2Bme^4 = a^2B^2e^6$$

Thus any prime which divides both n and m must divide either e, which is impossible, or a^2B^2. This means that d' can only contain primes from the finite set $\{p \mid p \text{ prime}, p|aB\}$. □

Thus we have now proved the image of α to be finite. We have done even more than that, we have found exactly what can be in the image of α. For

$$\begin{aligned}\alpha\left(\frac{m}{e^2}, \frac{n}{e^3}\right) &= \left(\frac{n}{e^3} + a\frac{m}{e^2} - aB\right) \cdot \mathbb{Q}^{*3} \\ &= (n + ame - aBe^3) \cdot \mathbb{Q}^{*3} \\ &= (\text{integer})^3 p_1^{\varepsilon_1} \dots p_j^{\varepsilon_j} \cdot \mathbb{Q}^{*3} \\ &= p_1^{\varepsilon_1} \dots p_j^{\varepsilon_j} \cdot \mathbb{Q}^{*3}\end{aligned}$$

where $\varepsilon_i \in \{0, 1, 2\}$ and the primes p_i are contained in the finite set $\{p \mid p \text{ prime }, p|2aB\}$.

4.2 Proof of Finite Image in All Other Cases

We have the elliptic curve given by

$$E : y^2 = x^3 + A(x - B)^2$$

and the map α. We will now prove that α has a finite image, given that A is not a square. Once again, we rewrite E with $x = \frac{m}{e^2}$ and $y = \frac{n}{e^3}$, where $\gcd(m, e) = \gcd(n, e) = 1$. This gives

$$n^2 = m^3 + A(me - Be^3)^2,$$

and rearrange to obtain

$$m^3 = n^2 - A(me - Be^3)^2.$$

Thus

$$m^3 = (n + e(m - Be^2)\sqrt{A})(n - e(m - Be^2)\sqrt{A}).$$

The map α sends the point $\left(\frac{m}{e^2}, \frac{n}{e^3}\right)$ to the element $(n + e(m - Be^2)\sqrt{A}) \cdot \mathbb{Q}(\sqrt{A})^{*3}$. Although we may not have unique prime factorization in the ring of integers of $\mathbb{Q}(\sqrt{A})$, we will have unique prime ideal factorization because the ring of integers is a Dedekind domain. Write O^* for the units. We use now that O^* modulo cubes is finite. This follows from the existence of the fundamental unit, stated in section 2.1. This means that the image of α will be proved finite if we can prove the following theorem.

Theorem 7. *Modulo $\mathbb{Q}(\sqrt{A})^{*3}$, the prime ideals which appear in the factorization of the ideal $(n + e(m - Be^2))$ belong to a finite set.*

Proof. Let us look at the prime ideal factorization of the ideal generated by $(n + e(m - Be^2)\sqrt{A})$. This consists of primes which can be either inert, ramified or split. We want to prove that only a finite number of any of these can be used in the factorization of $(n + e(m - Be^2)\sqrt{A})$, modulo $\mathbb{Q}(\sqrt{A})^{*3}$.

First consider some inert prime p in the factorization of $(n + e(m - Be^2)\sqrt{A})$. The norm of (p) is p^2. The norm of $(n + e(m - Be^2)\sqrt{A})$ is a cube, so we find that p must occur in the factorization of $(n + e(m - Be^2)\sqrt{A})$ to some power 3ε, $\varepsilon \in \mathbb{N}$. But $p^{3\varepsilon} = 1 \cdot \mathbb{Q}(\sqrt{A})^{*3}$, so there are no inert primes contributing to the finite set we are creating.

Now consider some ramified prime $(p) = P^2$. There are only a finite number of ramified primes anyway, so we could ignore this case if we wanted to. However, we can make the statement slightly stronger. Because the norm of $(n + e(m - Be^2)\sqrt{A})$ is a cube, we find that P must also occur to some power 3ε in the factorization. If P is principal, this means that it disappears modulo $\mathbb{Q}(\sqrt{A})^{*3}$. Thus only the nonprincipal ramified primes can contribute. Now we find that since P occurs to a third power, the prime p divides the element $(n + e(m - Be^2)\sqrt{A})$. Thus, as we will see when we handle split primes, $p|AB$.

The last and most difficult case is when we have split primes, which will always be of the form $(p) = P \cdot Q$, $P \neq Q$, in our number rings. There are two cases to consider:

1. both P and Q occur in the prime ideal factorization of $(n + e(m - Be^2)\sqrt{A})$;
2. (without loss of generality) only P occurs in the prime ideal factorization of $(n + e(m - Be^2)\sqrt{A})$.

In the first case, the principal ideal (p) divides $(n+e(m-Be^2)\sqrt{A})$. Thus the element p divides the element $n + e(m - Be^2)\sqrt{A}$. This means that p divides both n and $e(m - Be^2)\sqrt{A}$. But p cannot divide e, as $\gcd(n, e) = 1$. Therefore p divides either A or $m - Be^2$. If $p|(m - Be^2)$, then because $p|m$ and $p \nmid e$, then $p|B$. This means that there are only a finite number of split primes in the first case we are considering, namely those that divide AB.

In the second case, only P occurs. Because the norm of the ideal $(n + e(m - Be^2)\sqrt{A})$ is a cube, we know that P must occur to some power 3ϵ.

Recall from chapter 2 that the class group Cl of the number field $\mathbb{Q}(\sqrt{A})$ is always a finite abelian group. Every ideal class of Cl contains an integral ideal of norm not exceeding the Minkowski constant M_R.

Let us now assume that $N(P) > M_R$. Then there are prime ideals $P_1, \ldots, P_t$ such that $N(P_1 \cdot \ldots \cdot P_t) \leq M_R$ and there is a fractional principal ideal F such that $P = F \cdot P_1 \cdot \ldots \cdot P_t$. But this means that $P^{3\epsilon} = F^{3\epsilon} \cdot P_1^{3\epsilon} \cdot \ldots \cdot P_t^{3\epsilon}$. Now $F^{3\epsilon}$ is equivalent to 1 modulo third powers, so $P^{3\epsilon} \equiv P_1^{3\epsilon} \cdot \ldots \cdot P_t^{3\epsilon} \cdot \mathbb{Q}(\sqrt{A})^{*3}$. This means that the only prime ideals we need consider as contributing to the size of $\mathrm{im}(\alpha)$ are those prime ideals P with $N(P) \leq M_R$. This is of course a finite number of prime ideals.

Thus we have proved that the image of α is finite, as required. $\square$

Using this proof, we see that any element α_0 in $\mathrm{im}(\alpha)$ is of the form

$$\alpha_0 = u^{u_0} \cdot P_1^{3\varepsilon_1} \cdot \ldots \cdot P_n^{3\varepsilon_n} \cdot Q_1^{\delta_1} \cdot \ldots \cdot Q_m^{\delta_m} \cdot \mathbb{Q}(\sqrt{A})^{*3}$$

where u is the fundamental unit of the ring of integers, P_i the representatives of each equivalence class with norm less than M_R, and Q_i the split and nonprincipal ramified primes dividing AB. Concerning the powers, $u_0 \in \{0, 1, 2\}$, and δ_i and ε_i are natural numbers with a certain upper bound.

The knowledge acquired here will be useful when we look at some examples in chapter 6.

Chapter 5

A Formula for the Rank

The image of α can be very helpful when we want to know something about the rank of Γ, the group of rational points on E. In fact, we can find a specific formula telling us all we need to know. In this chapter we will derive this formula, and then illustrate its correctness with an example.

5.1 Derivation of Formula

To derive the rank formula, we need to find some expression containing the rank and then modify it in such a way that a workable formula arises. This initial expression can be found by making some very general observations.

Recall the morphism $\Phi : E \to \overline{E}$ we saw in chapter 2:

$$\Phi(x, y) = (\xi, \eta)$$

$$\xi = \frac{9}{x^2}\left(2y^2 + 2AB^2 - x^3 - \frac{2}{3}Ax^2\right)$$
$$\eta = \frac{27y}{x^3}\left(-4ABx + 8AB^2 - x^3\right)$$

A similar map Ψ exists from $\overline{E}$ to E. Recall that $\Psi \circ \Phi$ is the multiplication by 3 map. We now know from the work done in the previous three chapters, that Γ is a finitely generated group. This means that

$$\Gamma \cong \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{r \text{ times}} \oplus (\mathbb{Z}/p_1^{\nu_1}\mathbb{Z}) \oplus \ldots \oplus (\mathbb{Z}/p_s^{\nu_s}\mathbb{Z})$$

where the p_i are primes, and $\nu_i \in \mathbb{N}$. We therefore have generators $P_1, \ldots, P_r, Q_1, \ldots, Q_s \in \Gamma$ such that every $P \in \Gamma$ can be written as

$$P = n_1P_1 + \ldots + n_rP_r + m_1Q_1 + \ldots + m_sQ_s$$

with the integers n_i uniquely determined, and the integers m_j determined modulo $p_j^{\nu_j}$. The number r is called the rank of Γ. We see that

$$3\Gamma \cong 3\mathbb{Z} \oplus \ldots \oplus 3\mathbb{Z} \oplus 3(\mathbb{Z}/p_1^{\nu_1}\mathbb{Z}) \oplus \ldots \oplus 3(\mathbb{Z}/p_s^{\nu_s}\mathbb{Z})$$

from which follows

$$\frac{\Gamma}{3\Gamma} \cong \frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \ldots \oplus \frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{(\mathbb{Z}/p_1^{\nu_1}\mathbb{Z})}{3(\mathbb{Z}/p_1^{\nu_1}\mathbb{Z})} \oplus \ldots \oplus \frac{(\mathbb{Z}/p_s^{\nu_s}\mathbb{Z})}{3(\mathbb{Z}/p_s^{\nu_s}\mathbb{Z})}.$$

Although they may look complicated, the last s terms are really quite simple:

$$\frac{(\mathbb{Z}/p_j^{\nu_j}\mathbb{Z})}{3(\mathbb{Z}/p_j^{\nu_j}\mathbb{Z})} \cong \begin{cases} \mathbb{Z}/3\mathbb{Z} & \text{if } p_j = 3 \\ 0 & \text{if } p_j \neq 3. \end{cases}$$

Thus, we find

$$(\Gamma : 3\Gamma) = 3^{r+\text{number of } j \text{ with } p_j = 3}. \tag{5.1}$$

As before, let $\Gamma[3]$ denote the subgroup of all $P \in \Gamma$ such that $3P = \mathcal{O}$. $\Gamma[3]$ is therefore the group of points of order dividing 3. We will analyse this group to help us simplify equation (5.1). Let

$$3(n_1P_1 + \ldots + n_rP_r + m_1Q_1 + \ldots + m_sQ_s) = \mathcal{O}.$$

Because the P_i have infinite order, we need $n_i = 0$ for all i. The only restriction on the m_j is that $3m_j = 0(\text{mod}p_j^{\nu_j})$. If $p_j \neq 3$ and $3m = 0(\text{mod}\, p_j^{\nu_j})$, then $m = 0(\text{mod}\, p_j^{\nu_j})$. If, however, $p = 3$ and $3m = 0(\text{mod}\, p_j^{\nu_j})$, then $m = 0(\text{mod}\, p_j^{\nu_j - 1})$. This gives us that the order of the subgroup $\Gamma[3]$ is given by

$$\#\Gamma[3] = 3^{\text{number of } j \text{ with } p_j = 3}. \tag{5.2}$$

This should look extremely familiar. Combining equations (5.1) and (5.2) gives us:

$$(\Gamma : 3\Gamma) = 3^r \cdot \#\Gamma[3]$$

thus

$$3^r = \frac{(\Gamma : 3\Gamma)}{\#\Gamma[3]}. \tag{5.3}$$

Equation (5.3) is essentially what we will be working with. To make it slightly easier to work with, we will make just a few more steps before analysing the numerator and denominator of the right hand side.

In chapter 2 we have already looked at the number of points of order 3 our elliptic curve can contain. The difficult term here is therefore the term $(\Gamma : 3\Gamma)$. We still know next to nothing about Γ in general. We would therefore like to express this term differently using the map α. First we rewrite $(\Gamma : 3\Gamma)$ as

$$(\Gamma : 3\Gamma) = (\Gamma : \Psi \circ \Phi(\Gamma)).$$

If we denote by $\overline{\Gamma}$ the group of rational points on $\overline{E}$, we have an inclusion of subgroups $3\Gamma \subseteq \Psi(\overline{\Gamma}) \subseteq \Gamma$, therefore:

$$(\Gamma : 3\Gamma) = (\Gamma : \Psi(\overline{\Gamma})) \cdot (\Psi(\overline{\Gamma}) : \Psi \circ \Phi(\Gamma)). \tag{5.4}$$

At first glance, this may seem to complicate matters further. A general observation will suffice to show the contrary. Let G be an Abelian group and H a subgroup of finite index in G. Let $\Psi : G \to G'$ be a homomorphism of G into some group G'. The index $(\Psi(G) : \Psi(H))$ is

the one we would like to know more about. Using just standard isomorphism theorems from elementary group theory,

$$\frac{\Psi(G)}{\Psi(H)} \cong \frac{G}{H + \ker(\Psi)} \cong \frac{G/H}{(H + \ker(\Psi))/H} \cong \frac{G/H}{\ker(\Psi)/(\ker(\Psi) \cap H)}.$$

The index we wanted can now be expressed as

$$(\Psi(G) : \Psi(H)) = \frac{(G : H)}{(\ker(\Psi) : (\ker(\Psi) \cap H))}. \tag{5.5}$$

In our case we want to use $G = \overline{\Gamma}$ and $H = \Phi(\Gamma)$. Equation (5.4) then becomes

$$(\Gamma : 3\Gamma) = (\Gamma : \Psi(\overline{\Gamma})) \cdot \frac{(\overline{\Gamma} : \Phi(\Gamma))}{(\ker(\Psi) : \ker(\Psi) \cap \Phi(\Gamma))}. \tag{5.6}$$

Filling this in in equation (5.3) gives us:

$$3^r = \frac{(\Gamma : \Psi(\overline{\Gamma})) \cdot (\overline{\Gamma} : \Phi(\Gamma))}{(\ker(\Psi) : \ker(\Psi) \cap \Phi(\Gamma)) \cdot \#\Gamma[3]}. \tag{5.7}$$

This is the initial expression we were looking for. Now we are ready to do some serious replacing of terms. The numerator and denominator can now be analysed separately.

Simplifying the Numerator

The indices we find in the numerator can be computed relatively easily. Recall our homomorphism α, which was defined as:

$$E : y^2 = x^3 + A(x - B)^2$$
$$\alpha(x, y) = (y + (x - B)\sqrt{A}) \cdot \mathbb{Q}(\sqrt{A})^{*3}.$$

We have a similar map for $\overline{E}$, which we call $\overline{\alpha}$:

$$\overline{E} : y^2 = x^3 + \overline{A}(x - \overline{B})^2$$
$$\overline{\alpha}(x, y) = (y + (x - \overline{B})\sqrt{\overline{A}}) \cdot \mathbb{Q}(\sqrt{\overline{A}})^{*3}$$

where $\overline{A} = -27A$ and $\overline{B} = 4A + 27B$. A highly desirable result would now be that $\ker(\overline{\alpha}) = \text{im}(\Phi(\Gamma))$. If this is so, we can see that

$$\overline{\alpha}(\overline{\Gamma}) \cong \frac{\overline{\Gamma}}{\ker\overline{\alpha}} \cong \frac{\overline{\Gamma}}{\Phi(\Gamma)}$$

from which it follows that

$$(\overline{\Gamma} : \Phi(\Gamma)) = \#\overline{\alpha}(\overline{\Gamma}).$$

Similarly, if we can show that $\ker(\alpha) = \text{im}(\Psi(\overline{\Gamma}))$, then we would find that $(\Gamma : \Psi(\overline{\Gamma})) = \#\alpha(\Gamma)$. The proof of this statement is exactly the same as the proof of the first statement, so we will give the proof just once. It will be done in the following lemma.

Lemma 7. *ker*$(\overline{\alpha}) = im\ (\Phi(\Gamma))$.

Proof. Before giving the two customary inclusions, we handle some special points. First of all, $\overline{\mathcal{O}} \in \text{im}(\Phi(\Gamma))$ and $\overline{\mathcal{O}} \in \ker(\overline{\alpha})$. Now assume we have some $(0, y) \in \Gamma$. Then $A = a^2$ and $y = \pm aB$. However, $\Phi(0, \pm aB) = \overline{\mathcal{O}}$, which is obviously in $\ker(\overline{\alpha})$.

First to show $\ker(\overline{\alpha}) \supseteq \text{im}(\Phi(\Gamma))$. Let $P = (x, y) \in \Gamma$. We are dealing now with the case that $x \neq 0$, and $P \neq \mathcal{O}$. Let $(\xi, \eta) = \Phi(x, y)$. Then (ξ, η) is a point in $\text{im}(\Phi(\Gamma))$. We can take $\delta = -\frac{3y}{x}$ and $\varepsilon = 1 - \frac{3B}{x}$ because $x \neq 0$, and we see that

$$\overline{\alpha}(\xi, \eta) = (\delta + \varepsilon\sqrt{-3A})^3 = 1 \cdot \mathbb{Q}(\sqrt{-3A})^{*3}.$$

Thus any element of $\text{im}(\Phi(\Gamma))$ is also in the kernel of $\overline{\alpha}$.

Conversely, $\ker(\overline{\alpha}) \subseteq \text{im}(\Phi(\Gamma))$. Take some $(\xi, \eta) \in \overline{\Gamma}$ such that $\overline{\alpha}(\xi, \eta) = 1 \cdot \mathbb{Q}(\sqrt{\overline{A}})^{*3}$, but $(\xi, \eta) \neq \mathcal{O}$. This means that if (ξ, η) is indeed in $\text{im}(\Phi(\Gamma))$, then it has as a pre-image neither $\mathcal{O}$ nor some $(0, y)$. From the definition of $\overline{\alpha}$, we also know that $\overline{\alpha}(\xi, \eta) = (\eta + (\xi - \overline{B})\sqrt{\overline{A}}) \cdot \mathbb{Q}(\sqrt{\overline{A}})^{*3}$. For future ease of notation, we fill in straight away that $\overline{A} = -27A$ and $\overline{B} = 4A + 27B$. Thus there exist $\delta, \varepsilon \in \mathbb{Q}$ such that $(\eta + 3(\xi - 4A - 27B)\sqrt{-3A}) = (\delta + \varepsilon\sqrt{-3A})^3$. We can then express ξ and η in δ and ε as follows:

$$\xi = \delta^2\varepsilon - A\varepsilon^3 + 4A + 27B \tag{5.8}$$

$$\eta = \delta^3 - 9A\delta\varepsilon^2 \tag{5.9}$$

Now let

$$x = \frac{3B}{1 - \varepsilon} \tag{5.10}$$

$$y = \frac{-\delta B}{1 - \varepsilon} \tag{5.11}$$

This can be done provided $\varepsilon \neq 1$. This is always the case. If we let $\varepsilon = 1$, then we see that

$$\xi = \delta^2 + 3A + 27B$$
$$\eta = \delta^3 - 9A\delta.$$

Filling these in in $\xi^3 + \overline{A}(\xi - \overline{B})^2 - \eta^2 = 0$ and solving as a quadratic equation in A, we find that A is imaginary unless $B = 0$. However, B cannot be zero, thus $\varepsilon \neq 1$.

There are now two claims to be proved:

1. (x, y) is a point on Γ.
2. $\Phi(x, y) = (\xi, \eta)$.

The first claim is proved by starting with the fact $\xi^3 + \overline{a}(\xi - \overline{b})^2 - \eta^2 = 0$, and then showing that there is some nonzero rational number r such that $\xi^3 + \overline{A}(\xi - \overline{B})^2 - \eta^2 = r \cdot (x^3 + A(x - B)^2 - y^2) = 0$. This statement was proved using the computer program Mathematica, due to the amount of calculation and symbol manipulation involved [WR]. The proof

can be found in appendix A.

The second claim is now easy to prove. We simply express δ and ε in terms of x and y as follows:

$$\varepsilon = 1 - \frac{3B}{x}; \tag{5.12}$$

$$\delta = -\frac{3y}{x}. \tag{5.13}$$

Now fill in equations 5.12 and 5.13 in in the equations for ξ and η given in (5.8) and (5.9). We shall see the definition of ξ from the beginning of this chapter emerge. I shall do this only for ξ, to show that it works, and η will be left for any reader who is still unsure.

$$\begin{aligned}
\xi &= \delta^2\varepsilon - A\varepsilon^3 + 4A + 27B \\
&= \left(-\frac{3y}{x}\right)^2 \left(1 - \frac{3B}{x}\right) - A\left(1 - \frac{3B}{x}\right)^3 + 4A + 27B \\
&= \frac{9y^2}{x^2} - \frac{27By^2}{x^3} - A\left(1 - \frac{9B}{x} + \frac{27B^2}{x^2} - \frac{27B^3}{x^3}\right) + 4A + 27B.
\end{aligned}$$

We have proved the first claim, that (x, y) is a point of Γ, so we can use that $y^2 = x^3 + Ax^2 - 2ABx + AB^2$, and fill it in:

$$\begin{aligned}
\xi &= \frac{9y^2}{x^2} - \frac{27B}{x^3}(x^3 + Ax^2 - 2ABx + AB^2) - A\left(1 - \frac{9B}{x} + \frac{27B^2}{x^2} - \frac{27B^3}{x^3}\right) + 4A + 27B \\
&= \frac{9y^2}{x^2} - \frac{18AB}{x} + \frac{27AB^2}{x^2} + 3A \\
&= \frac{9}{x^2}\left(y^2 - 2ABx + 3AB^2 + \frac{Ax^2}{3}\right) \\
&= \frac{9}{x^2}\left(2y^2 - y^2 - 2ABx + 3AB^2 + \frac{Ax^2}{3}\right) \\
&= \frac{9}{x^2}\left(2y^2 - x^3 - Ax^2 + 2ABx - AB^2 - 2ABx + 3AB^2 + \frac{Ax^2}{3}\right) \\
&= \frac{9}{x^2}\left(2y^2 + 2AB^2 - x^3 - \frac{2}{3}Ax^2\right).
\end{aligned}$$

We can do the same for η. Thus we see that $\Phi(x, y) = (\xi, \eta)$, as required. □

We turn our attention to the denominator of equation (5.7).

Simplifying the Denominator

Recall the denominator of equation (5.7):

$$(\ker(\Psi) : \ker(\Psi) \cap \Phi(\Gamma)) \cdot \#\Gamma[3].$$

We know all we need to know about $\#\Gamma[3]$ from chapter 2. The only difficult term remaining is $(\ker(\Psi) : \ker(\Psi) \cap \Phi(\Gamma))$.

Of what elements does $\ker(\Psi)$ consist? In other words, what elements of $\overline{\Gamma}$ are mapped to $\mathcal{O}$ by Ψ? Obviously, $\Psi(\overline{\mathcal{O}}) = \mathcal{O}$, so we need only restrict our attention to nontrivial points in $\ker(\Psi)$. Remember that

$$\Psi(\xi, \eta) = (x, y)$$

$$x = \frac{9}{\xi^2}\left(2\eta^2 + 2\overline{A}\,\overline{B}^2 - \xi^3 - \frac{2}{3}\overline{A}\xi^2\right)$$
$$y = \frac{27\eta}{\xi^3}\left(-4\overline{A}\,\overline{B}\xi + 8\overline{A}\overline{B}^2 - \xi^3\right).$$

If $\xi \neq 0$, then $(\xi, \eta) \notin \ker(\Psi)$. The point $(0, 0)$ is never an element of $\overline{\Gamma}$, so that leaves only the points $(0, \eta)$ with $\eta \neq 0$ to consider. Such a point will only be a point of $\overline{\Gamma}$ if it satisfies the equation $\eta^2 = \xi^3 + \overline{A}(\xi - \overline{B})^2$. Thus it must satisfy $\eta^2 = \overline{A}\,\overline{B}^2$. This means that $\overline{A}$ must be a perfect square. Because $\overline{A} = -27A$, this means that we must have $A = -3a^2$ for some integer a. Thus

$$\#\ker\Psi = \begin{cases} 3 & \text{if } A = -3a^2; \\ 1 & \text{otherwise.} \end{cases} \tag{5.14}$$

Obviously, the term $(\ker(\Psi) : \ker(\Psi) \cap \Phi(\Gamma))$ disappears if $A \neq -3a^2$. Because $\Psi \circ \Phi$ is the multiplication by 3 map, only elements of order dividing 3 are sent to $\ker(\Psi)$ by Φ. If there are no points of order 3 on Γ, then $\ker(\Psi) \cap \Phi(\Gamma) = \{\overline{\mathcal{O}}\}$. If there are points of order 3, then either $A = a^2$ or $A = -3a^2$. If $A = a^2$, then $\ker(\Psi)$ is trivial. If $A = -3a^2$ and E has 3 points of order dividing 3, then we see that these points are mapped to the three points of $\ker(\Psi)$, so in this case $(\ker(\Psi) : \ker(\Psi) \cap \Phi(\Gamma))$ becomes trivial. Thus

$$(\ker\Psi : \ker\Psi \cap \Phi(\Gamma)) = \begin{cases} 3 & \text{if } A = -3a^2 \text{ and } \Gamma \text{ contains no points of order 3;} \\ 1 & \text{otherwise.} \end{cases} \tag{5.15}$$

Recapitulation and Harvesting

It is time to harvest all we have discovered so far. Our initial expression containing r was equation 5.7:

$$3^r = \frac{(\Gamma : \Psi(\overline{\Gamma})) \cdot (\overline{\Gamma} : \Phi(\Gamma))}{\#(\ker(\Psi) : \ker(\Psi) \cap \Phi(\Gamma)) \cdot \#\Gamma[3]}.$$

Lemma 7 gave us that

$$(\Gamma : \Psi(\overline{\Gamma})) = \#\alpha(\Gamma)$$
$$(\overline{\Gamma} : \Phi(\Gamma)) = \#\overline{\alpha}(\overline{\Gamma}).$$

Equation 5.15 gives us that

$$\#(\ker\Psi : \ker\Psi \cap \Phi(\Gamma)) = \begin{cases} 3 & \text{if } A = -3a^2 \text{ and } E \text{ contains no points of order 3;} \\ 1 & \text{otherwise.} \end{cases}$$

and in chapter 2 we saw that

$$\#\Gamma[3] = \begin{cases} 3 & \text{if } A = a^2 \text{ or in certain cases when } A = -3a^2; \\ 1 & \text{otherwise.} \end{cases}$$

Combining all this gives the following pleasing formula for the rank.

$$3^r = \begin{cases} \frac{1}{3} \cdot \#\alpha(\Gamma) \cdot \#\overline{\alpha}(\overline{\Gamma}) & \text{if } A = -3a^2 \text{ or } A = a^2; \\ \#\alpha(\Gamma) \cdot \#\overline{\alpha}(\overline{\Gamma}) & \text{otherwise.} \end{cases} \tag{5.16}$$

5.2 Example

Take the elliptic curve

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

This curve has rank 2 according to the computer program Magma. Let us look at the images of α and $\overline{\alpha}$ to see that the formula we derived is correct. The associated elliptic curve is

$$\overline{E} : y^2 = x^3 - 216(x-59)^2.$$

A is equal to 8, so it is neither a square nor -3 multiplied by a square. Thus we use that $3^r = \#\alpha(\Gamma) \cdot \#\overline{\alpha}\ (\overline{\Gamma})$. This means that we should find that either both $\alpha(\Gamma)$ and $\overline{\alpha}(\overline{\Gamma})$ contain 3 elements each, or one contains 1 element and the other 9.

The group Γ is generated by $(1,1)$ and $(2,4)$. It is plain to see that $\alpha(1,1) = 1$, so we need only concentrate on the other generator. Letting α work on it gives

$$\begin{aligned} \alpha(2,4) &= (4 + 2\sqrt{2}) \cdot \mathbb{Q}(\sqrt{2})^{*3} \\ &= 2\sqrt{2}(1+\sqrt{2}) \cdot \mathbb{Q}(\sqrt{2})^{*3} \\ &= (1+\sqrt{2}) \cdot \mathbb{Q}(\sqrt{2})^{*3}. \end{aligned}$$

We know that $2(2,4) = (\frac{1}{4}, \frac{17}{8})$. We see that

$$\begin{aligned} \alpha\left(\frac{1}{4}, \frac{17}{8}\right) &= \left(\frac{17}{8} - \frac{3}{2}\sqrt{2}\right) \cdot \mathbb{Q}(\sqrt{2})^{*3} \\ &= (17 - 12\sqrt{2}) \cdot \mathbb{Q}(\sqrt{2})^{*3} \\ &= (7 - 5\sqrt{2}) \cdot (1 - \sqrt{2}) \cdot \mathbb{Q}(\sqrt{2})^{*3} \\ &= (1-\sqrt{2})^3 \cdot (1-\sqrt{2}) \cdot \mathbb{Q}(\sqrt{2})^{*3} \\ &= (1-\sqrt{2}) \cdot \mathbb{Q}(\sqrt{2})^{*3} \\ &= -(1+\sqrt{2})^{-1} \cdot \mathbb{Q}(\sqrt{2})^{*3} \\ &= (1+\sqrt{2})^2 \cdot \mathbb{Q}(\sqrt{2})^{*3}, \end{aligned}$$

illustrating our result that α is a homomorphism. $1 + \sqrt{2}$ is the fundamental unit of $\mathbb{Z}[\sqrt{2}]$, thus we have 3 elements in $\alpha(\Gamma)$. We now turn our attention to $\overline{E}$. The generators here are $(177, 1593)$ and $(118, -944)$. We see that

$$\begin{aligned} \overline{\alpha}(177, 1593) &= 1593 + 708\sqrt{-6} \\ \overline{\alpha}(118, -944) &= -944 + 354\sqrt{-6}. \end{aligned}$$

Some arithmetic is required to see that

$$\begin{aligned}
\overline{\alpha}(177, 1593) &= (1593 + 708\sqrt{-6}) \cdot \mathbb{Q}(\sqrt{-6})^{*3} \\
&= 3 \cdot 59 \cdot (9 + 4\sqrt{-6}) \cdot \mathbb{Q}(\sqrt{-6})^{*3} \\
&= 3 \cdot 59 \cdot -\frac{1}{2} \cdot \sqrt{-6} \cdot (-8 + 3\sqrt{-6}) \cdot \mathbb{Q}(\sqrt{-6})^{*3} \\
&= -\frac{6}{2} \cdot 59 \cdot \frac{1}{2} \cdot \sqrt{-6} \cdot (-8 + 3\sqrt{-6}) \cdot \mathbb{Q}(\sqrt{-6})^{*3} \\
&= (\sqrt{-6})^3 \cdot \frac{1}{4} \cdot 59 \cdot (-8 + 3\sqrt{-6}) \cdot \mathbb{Q}(\sqrt{-6})^{*3} \\
&= 2 \cdot 59 \cdot (-8 + 3\sqrt{-6}) \cdot \mathbb{Q}(\sqrt{-6})^{*3} \\
&= (-944 + 354\sqrt{-6}) \cdot \mathbb{Q}(\sqrt{-6})^{*3}.
\end{aligned}$$

Thus we have at most 3 points in $\overline{\alpha}(\overline{\Gamma})$. To complete the example, we must see that $-944 + 354\sqrt{-6}$ is not a cube. First of all, the norm of this element is $N(-944 + 354\sqrt{-6}) = 944^2 + 6 \cdot 354^2 = 2^3 \cdot 59^3$. We shall look at the ideal generated by this element, namely $I = (-944 + 354\sqrt{-6})$. Although we do not have unique factorization, we do have unique prime ideal factorization. We shall now decompose this ideal into prime ideals.

We know that there is one prime ideal lying over 2, and two prime ideals lying over 59. The prime ideal over 2 is $p_2 = (2, \sqrt{-6})$. The two prime ideals over 59 are $p_{59} = (59, 17 + \sqrt{-6})$ and $q_{59} = (59, -17 + \sqrt{-6})$. Decompose I into prime ideals:

$$I = p_2^3 \cdot p_{59}^2 q_{59}.$$

The principal ideal generated by $-944 + 354\sqrt{-6}$ is not a cube in terms of prime ideals. If $-944 + 354\sqrt{-6}$ itself were a cube of some kind, the ideal generated by its cube root would have to be a product of some of the p_2, p_{59}, q_{59}. Let J be such that it is generated by the element whose cube is $-944 + 354\sqrt{-6}$. Then:

$$\begin{aligned}
J^3 &= I \\
&= p_2^3 \cdot p_{59}^2 q_{59}.
\end{aligned}$$

This implies however that p_{59} and q_{59} are both third powers of ideals. However, both are prime ideals. This is therefore not possible. Thus $-944 + 354\sqrt{-6}$ is not a cube, and there are 3 elements in $\overline{\alpha}(\overline{\Gamma})$. The formula for the rank is shown to hold in this case.

Chapter 6

Examples

In the proof of the fact that the map α has a finite image, we were able to see much more happening than just this bare fact. We were able to see what all the potential points of $\mathrm{im}(\alpha)$ were. In the previous chapter, it was shown how the rank of an elliptic curve is related to the size of $\mathrm{im}(\alpha)$. If we can construct curves that have large $\mathrm{im}(\alpha)$, we will have constructed curves with high rank Γ.

If we look at the proof presented in section 4.2, it seems desirable to work in a field that contains many non-principal ideals whose cube is a principal ideal. This means that we want the class group of the ring of integers to contain many different points of order 3.

In this chapter, we will explore this idea by first presenting two examples, one with a very simple class group and one with a more complicated class group. In the last section, we will try to generate some examples of curves with a higher rank Γ.

6.1 First Example

The first example we shall consider is the curve

$$E : y^2 = x^3 + 3(x-2)^2.$$

In this case, $A = 3$, so A is neither a square nor -3 multiplied by a square. This means that the formula for the rank we shall be using is $3^r = \#\alpha(\Gamma) \cdot \#\overline{\alpha}(\overline{\Gamma})$.

The map α then becomes

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

The ring of integers of $\mathbb{Q}(\sqrt{3})$ is $\mathbb{Z}[\sqrt{3}]$. All the units in $\mathbb{Z}[\sqrt{3}]$ are generated by -1 and $u = 2 - \sqrt{3}$. The class group is generated by ideals of norm at most

$$M_R = \left(\frac{4}{\pi}\right)^0 \cdot \frac{2!}{2^2} \cdot \sqrt{|\Delta|}$$

where Δ is the discriminant of $X^2 - 3$, which is 12. Thus $M_R \approx 1.732$. This means that $\mathbb{Z}[\sqrt{3}]$ is in fact a principal ideal domain.

From section 4.2, we know now that the size of $\mathrm{im}(\alpha)$ can never be very great. Let us look at the primes over 3 and 2:

$$X^2 - 3 \equiv (X-1)^2 \bmod 2$$
$$X^2 - 3 \equiv X^2 \bmod 3$$

so we have a single prime $p_2 = (2, \sqrt{3}-1) = (\sqrt{3}-1)$ lying over 2 and a single prime $p_3 = (\sqrt{3})$ lying over 3. Both 2 and 3 are ramified, and p_2, p_3 are both principal. Thus the size of $\mathrm{im}(\alpha)$ can be at most 3: $\{1, u, u^2\}$. And we easily see that $(1,2) \in \Gamma$, and $\alpha(1,2) = u$. Thus $\#\alpha(\Gamma) = 3$.

The associated curve $\overline{E}$ is given by

$$\overline{E} : y^2 = x^3 - 81(x-66)^2.$$

We will thus be working with the number field $\mathbb{Q}(i)$, which has ring of integers $\mathbb{Z}[i]$. The map $\overline{\alpha}$ becomes

$$\overline{\alpha}(x,y) = y + 9(x-66)i.$$

All the units in this ring are $\{1, -1, i, -i\}$, and these elements are all cubes. The class group is generated by ideals of norm at most

$$M_R = \left(\frac{4}{\pi}\right)^1 \cdot \frac{2!}{2^2} \cdot \sqrt{|\Delta|}$$

where Δ is the discriminant of X^2+1, which is -4. Thus $M_R \approx 1.273$, and we find that $\mathbb{Z}[i]$ is a principal ideal domain. Let us now look at what lies above the primes dividing 81 and 66:

$$X^2 + 1 \equiv (X+1)^2 \bmod 2$$
$$X^2 + 1 \equiv X^2 + 1 \bmod 3$$
$$X^2 + 1 \equiv X^2 + 1 \bmod 11$$

which means that 3 and 11 are inert, and 2 is ramified, with a single prime $p_2 = (2, 1+i) = (1+i)$ lying over it. Thus we find that $\mathrm{im}(\overline{\alpha})$ is contained in $\{1, -1, i, -i\}$. However, $\#\mathrm{im}(\overline{\alpha})$ must be a power of 3. It must also be a subgroup of $\{1, -1, i, -i\}$. Thus we find $\mathrm{im}(\overline{\alpha})$ must be equal to $\{1\}$, so $\#\overline{\alpha}(\overline{\Gamma}) = 1$.

Combining what we have learned, the rank r is found with

$$\begin{aligned} 3^r &= \#\alpha(\Gamma) \cdot \#\overline{\alpha}(\overline{\Gamma}) \\ &= 3 \cdot 1 \\ &= 3 \end{aligned}$$

from which it follows that $r = 1$.

6.2 Second Example

The second example we consider will be

$$E : y^2 = x^3 + 79(x-4)^2.$$

The field we will work in now is $\mathbb{Q}(\sqrt{79})$, which has ring of integers $\mathbb{Z}[\sqrt{79}]$. The units in this ring are generated by -1 and $u = 80 - 9\sqrt{79}$. The class group is now generated by ideals of norm less than

$$M_R = \left(\frac{4}{\pi}\right)^0 \cdot \frac{2!}{2^2} \cdot \sqrt{|\Delta|}$$

where Δ is the discriminant of the polynomial $X^2 - 79$, which is 316. Thus $M_R \approx 8.889$. We first compute the class group. The prime ideals of norm less than 8 are:

$$\begin{aligned} p_2 &= (2, 1+\sqrt{79}) \\ p_3 &= (3, 1+\sqrt{79}) & q_3 &= (3, 1-\sqrt{79}) \\ p_5 &= (5, 2+\sqrt{79}) & q_5 &= (5, 2-\sqrt{79}) \\ p_7 &= (7, 3+\sqrt{79}) & q_7 &= (7, 3-\sqrt{79}). \end{aligned}$$

We can now derive the following relationships between these generators:

$$\begin{aligned} p_2 &= (9+\sqrt{79}) & p_3p_5 &= (-8+\sqrt{79}) \\ p_3q_3 &= (3) & p_3p_7 &= (-10-\sqrt{79}) \\ p_5q_5 &= (5) & p_5q_7 &= (26+3\sqrt{79}) \\ p_7q_7 &= (7) & p_3^3 &= (17+2\sqrt{79}). \end{aligned}$$

We see that p_2 is principal, so we can ignore it in computing the class group. For any p_i, the inverse in the class group is q_i. However, p_3p_5 and p_3p_7 are also principal, so p_5 and p_7 are in the same equivalence class as q_3. In the same way we find that p_3, q_5 and q_7 belong to one equivalence class. The fact that p_3^3 is a principal ideal shows that the order of each element of the class group divides 3. We can show quite easily that p_3 is itself not principal, thus the class group consists of 3 elements.

We can now say what set the image of α must be contained in. Elements of $\mathrm{im}(\alpha)$ must be of the form of generators of

$$u^{\varepsilon} q_3^{\delta}$$

for ε, δ bounded integers. There is no contribution from primes dividing 79 or 4, for these are all ramified, and either in the same class group equivalence class as a power of q_3 or principal. We can find some points on Γ:

$$(9, 52), (-3, -62), (84, 1048), (-86, 62).$$

Putting these points through α gives us the following:

$$\begin{aligned}\alpha(9,52) &= (52+5\sqrt{79})\cdot\mathbb{Q}(\sqrt{79})^{*3}\\ \alpha(-3,-62) &= (-62-7\sqrt{79})\cdot\mathbb{Q}(\sqrt{79})^{*3}\\ \alpha(84,1048) &= (1048+80\sqrt{79})\cdot\mathbb{Q}(\sqrt{79})^{*3}\\ \alpha(-86,62) &= (62-90\sqrt{79})\cdot\mathbb{Q}(\sqrt{79})^{*3}.\end{aligned}$$

Let us look at the ideals generated by the elements on the right-hand side:

$$\begin{aligned}(\alpha(9,52)) &= (52+5\sqrt{79}) = q_3^6\\ (\alpha(-3,-62)) &= (-62-7\sqrt{79}) = q_3^3\\ (\alpha(84,1048)) &= (1048+80\sqrt{79}) = 2^3q_3^3q_7^3\\ (\alpha(-86,62)) &= (62-90\sqrt{79}) = u^2p_2^3p_{43}^3.\end{aligned}$$

where $p_{43} = (6-\sqrt{79})$ is a principal ideal of norm 43.

Because q_7 is in the same equivalence class as p_3, we find that $\alpha(84,1048)$ is in fact the cube of an element. From the other elements, we see that we reach $\{u^2, q_3^3, q_3^6\}$. Thus we find that $\mathrm{im}(\alpha)$ consists of the generators of the ideals

$$\{1, u, u^2, q_3^3, q_3^6, uq_3^3, uq_3^6, u^2q_3^3, u^2q_3^6\}$$

and

$$\#\mathrm{im}(\alpha) = 9.$$

The associated curve $\overline{E}$ is given by

$$\overline{E} : y^2 = x^3 - 2133(x-424)^2.$$

The field we are working in now is $\mathbb{Q}(\sqrt{-237})$, which has ring of integers $\mathbb{Z}[\sqrt{-237}]$. The units in this ring consist of just the set $\{1,-1\}$. The class group is now generated by ideals of norm less than

$$M_R = \left(\frac{4}{\pi}\right)^1 \cdot \frac{2!}{2^2}\cdot\sqrt{|\Delta|}$$

where Δ is the discriminant of the polynomial X^2+237, which is -948. Thus $M_R \approx 19.601$. We find if we do a lengthy calculation that the class number in this case is 12, and the class group is generated by $p_2 = (2, 1+\sqrt{-237})$ of order 2, and $p_7 = (7, 1-\sqrt{-237})$ of order 6.

The primes dividing -2133 and 424 are 2, 3, 53 and 79. We find that 2, 3 and 79 are ramified, and 53 is split into two primes:

$$\begin{aligned}(53) &= p_{53}q_{53}\\ &= (53, 9-\sqrt{-237})\cdot(53,-9-\sqrt{-237}).\end{aligned}$$

Thus elements in $\mathrm{im}(\overline{\alpha})$ look like the generators of

$$p_2^{\varepsilon_1}\cdot p_3^{\varepsilon_2}\cdot p_7^{\varepsilon_3}\cdot p_{53}^{\varepsilon_4}\cdot q_{53}^{\varepsilon_5}\cdot p_{79}^{\varepsilon_6}$$

where $\varepsilon_i \in \mathbb{Z}$, suitably bounded. It is a lot more difficult to find points on $\overline{E}$, but after a lot of work we find the following points:

$$(1749, -40068), (3657, 163134), (11478, -1118718), \left(\frac{92856}{49}, \frac{16050096}{343}\right).$$

Using these points, we find a lower bound of 9 for $\#\mathrm{im}(\overline{\alpha})$.

We now have a lower bound for the rank of E. Simply plug in the rank formula:

$$\begin{aligned} 3^r &= \#\mathrm{im}(\alpha) \cdot \#\mathrm{im}(\overline{\alpha}) \\ &\geq 9 \cdot 9 \\ &= 3^4 \end{aligned}$$

so $r \geq 4$. In fact, in this case the rank is equal to 4, but this cannot be seen from the procedure above.

6.3 Higher Rank Curves

Using Magma, it is possible to search for higher-rank curves. Here, we only had a few tries, and rank 5 curves emerged fairly quickly. The curves stated below were constructed as follows. First, a quadratic number ring with a high 3-torsion was found. Then a suitable B was sought by multiplying together powers of primes that may contribute to increasing the rank by increasing the size of $\mathrm{im}(\alpha)$. We found some curves of rank 4:

$$\begin{aligned} y^2 &= x^3 + 21191(x - 19^2)^2 \\ y^2 &= x^3 + 21191(x - 2^2)^2 \\ y^2 &= x^3 - 6761(x - 2^6)^2. \end{aligned}$$

We also found two curves of rank 5:

$$\begin{aligned} y^2 &= x^3 + 21191(x - 2^4)^2 \\ y^2 &= x^3 + 5098(x - 2^2)^2. \end{aligned}$$

With a more rigorous search, perhaps curves of even higher rank could be found. Also, it seems that Magma does not use the special structure of these kind of curves. The rank calculations would probably be much faster if it did.

There have been searches performed to find curves with a high rank that have a torsion group of 3 points. See [Duj] for many examples of these. Although it is not precisely of our form, we find examples there such as

$$y^2 = x^3 + 841600494735^2$$

which has torsion group $\{\mathcal{O}, (0, \pm 841600494735)\}$ and rank 8.

Chapter 7

Concerning Reductions of the Elliptic Curve

There is another way we may get to know more about the rank of the group of rational points of an elliptic curve E. This is by considering various reductions of the curve. This means that instead of looking at the curve $E : y^2 = x^3 + A(x - B)^2$ over $\mathbb{Q}$, we will reduce A and B modulo some prime p and consider the reduced curve $\widetilde{E} : y^2 = x^3 + \widetilde{A}(x - \widetilde{B})^2$ over the finite field $\mathbb{Z}/p\mathbb{Z}$. If we do this for several primes, there is much we may learn about the nature of Γ.

7.1 The Reduction Map

Consider the elliptic curve

$$E : y^2 = x^3 + A(x - B)^2.$$

Let us choose a notation for the reduction map. Let us write $z \longmapsto \widetilde{z}$ for the map 'reduction modulo p',

$$\mathbb{Z} \to \frac{\mathbb{Z}}{p\mathbb{Z}}; \qquad z \longmapsto \widetilde{z}$$

The coefficients of E can be reduced modulo p, giving a curve $\widetilde{E}$:

$$\widetilde{E} : y^2 = x^3 + \widetilde{A}(x - \widetilde{B})^2.$$

The points on this curve are points (x, y) with $x, y \in \mathbb{Z}/p\mathbb{Z}$, together with the point at infinity $\mathcal{O}$. The first question we must answer is when this new curve is singular. Recall the discriminant of E, which was given by

$$\Delta = A^2B^3(-4A - 27B).$$

The discriminant is 0 whenever there is a singular point on E. In the same way, $\widetilde{E}$ will be singular whenever

$$\widetilde{\Delta} = \widetilde{A}^2\widetilde{B}^3(-4\widetilde{A} - 27\widetilde{B})$$

is zero. We see straight away that $\widetilde{E}$ is singular whenever $p|\Delta$. There is one special case to consider, and that is that $\widetilde{E}$ is also singular if $p = 2$. See [Sil86] for details.

What we would now like to do is reduce rational points on the curve E modulo p to obtain points on $\widetilde{E}$. Let $(x, y) = \left(\frac{m}{e^2}, \frac{n}{e^3}\right) \in \Gamma$. If $p \nmid e$, we can easily reduce modulo p. If $p|e$, we have to write (x, y) as a point in $\mathbb{P}^2$:

$$(x, y) = [me : n : e^3].$$

Now, $p \nmid n$, so

$$\widetilde{[me : n : e^3]} = [\tilde{0} : \tilde{1} : \tilde{0}] = \widetilde{\mathcal{O}}$$

thus (x, y) reduces to $\widetilde{\mathcal{O}}$. Of course, $\mathcal{O}$ also reduces to $\widetilde{\mathcal{O}}$.

The Nagell-Lutz theorem tells us that the torsion points of E all have integer coordinates. The next section briefly deals with these torsion points, which can be easily analysed through reductions.

The question arises whether it matters that $\widetilde{E}$ may be singular. Can we still make use of the reduction if it is? We need some notation before proceeding. Let us denote the nonsingular points of the curve $\widetilde{E}$ by $\widetilde{E}_{\text{ns}}$. Define the subset $E_0(\mathbb{Q})$ as follows:

$$E_0(\mathbb{Q}) = \{P \in \Gamma \mid \widetilde{P} \in \widetilde{E}_{\text{ns}}\}.$$

It can be shown that $E_0(\mathbb{Q})$ is a group, and the reduction map restricted to these points is a homomorphism. So if none of the points of E reduce to a singular point of $\widetilde{E}$, the reduction map is still a homomorphism from the points of E to some subgroup of $\widetilde{E}_{\text{ns}}$.

As an example, consider the curve

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

Reducing modulo 3, we find

$$\widetilde{E} : y^2 = x^3$$

which has exactly one singular point at $(0, 0)$. Is there a point $(x, y) = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$ in Γ that is mapped to $(0, 0)$ by the reduction map? Let us assume there is. Then we can write $m = 3m_1$, $n = 3n_1$ and $\gcd(e, 3) = 1$. This gives us, when we fill it in in the equation of E:

$$\begin{aligned}
\frac{9n_1^2}{e^6} &= \frac{27m_1^3}{e^6} + 3(\frac{3m_1}{e^2} - 1)^2 \\
9n_1^2 &= 27m_1^3 + 3e^2(3m_1 - e^2)^2 \\
3n_1^2 &= 9m_1^3 + e^2(3m_1 - e^2)^2 \\
3n_1^2 - 9m_1^3 &= e^2(3m_1 - e^2)^2
\end{aligned}$$

This means that $3|e^2(3m_1 - e^2)^2$, which means that $3|(3m_1 - e^2)$, so we must have $3|e$. This is a contradiction, so there is no $(x, y) \in \Gamma$ that reduces to the singular point $(0, 0)$. Thus the reduction map is a homomorphism in this case.

7.2 The Torsion Group

It is quite easy to find out something about the torsion group of a curve using reductions modulo p. We want to study the subgroup of finite order points on some elliptic curve E, so let us call this torsion subgroup T:

$$T = \{P = (x, y) \in E \mid P \text{ has finite order}\}.$$

It is easy to show that T is indeed a subgroup of Γ, so we shall not do so here. For suitable choices of p, the reduction map is indeed a homomorphism from T to $\widetilde{E}_{\text{ns}}$. There is now a very important observation to be made, namely that the reduction map is injective in this case. Taking any point $(x, y) \in T$, it is easy to see that it will never be sent to $\widetilde{\mathcal{O}}$. Thus the structure of the torsion group is preserved, and the reduction map is in fact an isomorphism from T to some subgroup of $\widetilde{E}_{\text{ns}}$. This can help us describe exactly the torsion group, as shown in the following examples.

First Example

Let $E : y^2 = x^3 + 3(x-2)^2$. The discriminant is equal to $\Delta = -2^4 \cdot 3^3 \cdot 11$. We can reduce modulo 3, because the singular point is avoided. Reducing modulo 3, we obtain the curve

$$\widetilde{E} : y^2 = x^3$$

and $\widetilde{E}(\mathbb{Z}/3\mathbb{Z})$ can consist of at most the points

$$\{\widetilde{\mathcal{O}}, (\tilde{1}, \pm\tilde{1})\}.$$

Reducing modulo 7, we obtain the curve

$$\widetilde{E} : y^2 = x^3 + \tilde{3}(x - \tilde{2})^2$$

and $\widetilde{E}(\mathbb{Z}/7\mathbb{Z})$ can consist of at most the points

$$\{\widetilde{\mathcal{O}}, (\tilde{1}, \pm\tilde{2}), (\tilde{2}, \pm\tilde{1}), (\tilde{3}, \pm\tilde{3})\}.$$

The points of finite order must form a group that has the group structure of a subgroup of each of these groups, so the only possibility is that there is precisely one point of finite order, namely $\mathcal{O}$.

Second Example

Let $E : y^2 = x^3 + 9(x-2)^2$. The discriminant is equal to $\Delta = -2^4 \cdot 3^6 \cdot 5$. We can reduce modulo p whenever $p \neq 2, 3$. We can reduce modulo 5 because the singular point $(\tilde{1}, \tilde{0})$ is avoided. Reducing modulo 5, we get a group of 6 nonsingular points:

$$\{\mathcal{O}, (\tilde{0}, \pm\tilde{1}), (\tilde{2}, \pm\tilde{1}), (\tilde{1}, \tilde{0})\}.$$

Modulo 7, we get a group of order 9:

$$\{\widetilde{\mathcal{O}}, (\tilde{0}, \pm\tilde{5}), (\tilde{2}, \pm\tilde{1}), (\tilde{3}, \pm\tilde{1}), (\tilde{4}, \pm\tilde{3})\}.$$

Modulo 11, we get a group of order 12:

$$\{\widetilde{\mathcal{O}}, (\tilde{0}, \pm\tilde{5}), (\tilde{3}, \pm\tilde{5}), (\tilde{4}, \pm\tilde{1}), (\tilde{8}, \tilde{0}), (\tilde{9}, \pm\tilde{2}), (\tilde{10}, \pm\tilde{5})\}.$$

This means that the group of finite order points consists of either 1 or 3 points. However, we easily see that the curve E has 2 points of order 3, namely $(0, 6)$ and $(0, -6)$. Thus the torsion subgroup consists of the three points $\{\mathcal{O}, (0, 6), (0, -6)\}$.

7.3 Reductions and Rank

In the ideal case, we would be able to find out something about the rank of Γ without knowing any points at all on E. This should be possible in theory. If we know that the reduction map is surjective, which is true in all our cases, we could adopt the following procedure:

1. Via reductions, determine the torsion subgroup of Γ. Call the number of generators needed to generate this group g_0.
2. Reduce E modulo 'suitable' primes.
3. Take the reduction that yields the group $\widetilde{\Gamma}$ requiring the largest number of generators g_1.
4. $g_1 - g_0$ gives a lower bound for the rank of Γ.

There are many problems with the procedure given above. For a start, determining the number of points on $\widetilde{\Gamma}$ is usually extremely hard work. Also, there is no guarantee that reducing modulo small primes will do the trick; very large primes may be required. This means that many groups $\widetilde{\Gamma}$ may have to be determined. We also do not know when to stop searching for an even better group $\widetilde{\Gamma}$. All in all a very messy procedure.

A simpler case can be studied, namely that we have a number of points given in Γ. Let these points be called $P_1, \ldots, P_t$. Then we know that the subgroup generated by these points is also in Γ. This subgroup can be called H:

$$H = \sum_{i=1}^{t} a_i P_i$$

where $a_i \in \mathbb{Z}$.

The first thing to notice is rather trivial, namely that $\text{rank}(H) \leq \text{rank}(\Gamma)$. The rank of H will therefore give us a lower bound for the rank of Γ. The very great advantage of working with H rather than Γ is that our knowledge about H is very much greater than our knowledge about Γ.

The next step is to see that the following statement is true.

If we have some surjective homomorphism $h : H \to G$ and G cannot be generated by less than s elements, then neither can H.

The group G will be a subgroup of $\widetilde{\Gamma}$, a suitable reduction of Γ, and h will of course be the reduction map. The number of generators needed to generate the reduced points of H will give a lower bound for the number of generators of H. This idea is best demonstrated by giving some examples.

7.4 Examples

First Example

Consider

$$E : y^2 = x^3 + 3(x-2)^2.$$

Some points we might easily find on E are $(1,2)$ and $(1,-2)$. We calculated earlier that the torsion group is $\{\mathcal{O}\}$. This is actually a trivial example, because we easily see that $-(1,2) = (1,-2)$, and so a lower bound for the rank is 1. Given these points, we could never give a higher lower bound than this. Let us see it happening though.

Reduce E modulo 7 to obtain

$$\widetilde{E} : y^2 = x^3 + \tilde{3}(x-\tilde{2})^2.$$

The point $(1,2)$ reduces to $(\tilde{1},\tilde{2})$ and $(1,-2)$ reduces to $(\tilde{1},-\tilde{2})$. These points generate the entire group $\widetilde{\Gamma}$, which was a group of 7 points:

$$\{\mathcal{O}, (\tilde{1},\pm\tilde{2}), (\tilde{2},\pm\tilde{1}), (\tilde{3},\pm\tilde{3})\}.$$

This needs just one generator, so we conclude that the lower bound for the rank is 1 in this case.

Second Example

Consider now

$$E : y^2 = x^3 + 9(x-2)^2.$$

We easily find some points on this curve, such as

$$(-12,\pm 6), (0,\pm 6), (3,\pm 6), (4,\pm 10), (240,\pm 3786).$$

This looks like a very promising curve, perhaps having a large rank. In the previous section, we determined the torsion group, which was $\{\mathcal{O}, (0,\pm 6)\}$, which needed 1 generator.

Now for any pair of points $(x,\pm y)$, we will consider only (x,y), for $-(x,y) = (x,-y)$ and so will not require any other generators. This leaves us with

$$(-12,6), (0,6), (3,6), (4,10), (240,3786).$$

Reducing modulo 7 gives

$$(\tilde{2},\tilde{6}), (\tilde{0},\tilde{6}), (\tilde{3},\tilde{6}), (\tilde{4},\tilde{3}), (\tilde{2},\tilde{6})$$

which generates the entire group $\widetilde{\Gamma}$ of 9 elements. In this case, $\widetilde{\Gamma}$ is a group isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, and therefore requires 2 generators. One of these generators is needed to generate torsion points, so 1 generator is left to generate the infinite order points, and thus contribute to the rank. Thus we find a lower bound of 1 for the rank.

Let us try again with 11. Reducing modulo 11 gives:

$$(\widetilde{10}, \tilde{6}), (\tilde{0}, \tilde{6}), (\tilde{3}, \tilde{6}), (\tilde{4}, \widetilde{10}), (\tilde{9}, \tilde{2}).$$

This looks more promising, but alas, these points generate the full group of order 12. Here, only 1 generator is needed, so this reduction gives a worse lower bound than the previous reduction. We never find we need more generators, no matter what prime we choose to reduce with. Thus we must conclude that our lower bound here is 1, and that ease of finding points on Γ has little to do with the rank of Γ.

Chapter 8

Conclusion

Computing the rank of the group Γ on elliptic curves is difficult. If nothing else has been achieved in this thesis, this fact can be seen as being very true indeed. By constraining ourselves to just one form of elliptic curve, we are able to be slightly more successful in determining the rank of Γ than we might otherwise hope to be.

In this thesis, I chose to explore the realm of elliptic curves occupied by those of the form

$$E : y^2 = x^3 + A(x - B)^2.$$

We managed to use a very useful homomorphism α, and showed how knowledge about its image helped us, not only to prove the Mordell-Weil theorem, but also to create a formula that can be used to determine the rank of Γ exactly.

Unfortunately, we have had to enter the realm of algebraic number theory to do these things. This means that instead of being able to do calculations in the field $\mathbb{Q}$, we have had to do calculations in some more difficult field $\mathbb{Q}(\sqrt{A})$. This means that if we want to use the computer to help us determine higher rank curves, it becomes much more costly to do so. On the other hand, perhaps we ought to be grateful, for we need look only at quadratic number fields, in which we can easily determine entities such as the ring of integers and the fundamental units. Our use of complicated theory need not be too excessive.

Those who have tried to find high-rank elliptic curves in the past seem to have done so either by fixing the torsion group (such as [Duj00]) or by looking at a different, easier form of elliptic curve (such as [Pom74]). A suggestion for future searching might be to expand the forms being searched, or to take a less harsh restriction than fixing the torsion group. In our case, the torsion group may vary in size, and the rank seems to be heavily influenced by the nature of the field where the image of the homomorphism α resides.

It seems to me that the type of elliptic curve discussed in this thesis has been unfairly ignored, many preferring instead to study the form $y^2 = x(x^2 + Ax + B)$. It is obvious that there is much still to be discovered about our kind of curves, and it has been a very great pleasure to have been able to study them.

Appendix A

Proof of Part of Lemma 7

We have two curves

$$E : y^2 = x^3 + A(x - B)^2 \tag{A.1}$$
$$\overline{E} : \eta^2 = \xi^3 + \overline{A}(\xi - \overline{B})^2. \tag{A.2}$$

There are ε, δ with

$$\begin{aligned} \xi &= \delta^2\varepsilon - A\varepsilon^3 + 4A + 27B \\ \eta &= \delta^3 - 9A\delta\varepsilon^2 \end{aligned} \tag{A.3}$$

and $(\xi, \eta) \in \ker(\overline{\alpha})$. We must show that $(x, y) \in \Gamma$, where

$$\begin{aligned} x &= \frac{3B}{1-\varepsilon} \\ y &= \frac{-\delta B}{1-\varepsilon}. \end{aligned} \tag{A.4}$$

We will do this by showing that there is some nonzero $r \in \mathbb{Q}$ such that

$$\xi^3 + \bar{A}(\xi - \bar{B})^2 - \eta^2 = r \cdot (x^3 + A(x - B)^2 - y^2) = 0.$$

Start by expanding $\xi^3 + \bar{A}(\xi - \bar{B})^2 = 0$ and fill in (A.3), $\bar{A} = -27A$ and $\bar{B} = 4A + 27B$ to obtain:

$$\begin{aligned} 0 = {} & 64A^3 + 1296A^2B + 8748AB^2 + 19683B^3 - \delta^6 + 48A^2\delta^2\varepsilon + 648AB\delta^2\varepsilon \\ & + 2187B^2\delta^2\varepsilon + 3A\delta^4\varepsilon^2 + 81B\delta^4\varepsilon^2 - 48A^3\varepsilon^3 - 648A^2B\varepsilon^3 - 2187AB^2\varepsilon^3 \\ & + \delta^6\varepsilon^3 - 51A^2\delta^2\varepsilon^4 - 162AB\delta^2\varepsilon^4 - 3A\delta^4\varepsilon^5 - 15A^3\varepsilon^6 + 81A^2B\varepsilon^6 \\ & + 3A^2\delta^2\varepsilon^7 - A^3\varepsilon^9. \end{aligned} \tag{A.5}$$

Now expand $x^3 + A(x - B)^2 - y^2 = 0$, and fill in (A.4) to obtain

$$-\frac{(4AB^2)}{(-1+\varepsilon)^3} - \frac{(27B^3)}{(-1+\varepsilon)^3} + \frac{(B^2\delta^2)}{(-1+\varepsilon)^3} - \frac{(B^2\delta^2\varepsilon)}{(-1+\varepsilon)^3} + \frac{(3AB^2\varepsilon^2)}{(-1+\varepsilon)^3} + \frac{(AB^2\varepsilon^3)}{(-1+\varepsilon)^3}. \tag{A.6}$$

Now let

$$r = -\frac{(-1+\varepsilon)^3}{B^2} \cdot \Big(729B^2 + 27B\delta^2(1+2\varepsilon) + \delta^4(1+\varepsilon+\varepsilon^2) + A^2(4-2\varepsilon+\varepsilon^2)^2(1+\varepsilon+\varepsilon^2) + A\big(-27B(-8-3\varepsilon^2+2\varepsilon^3) + 2\delta^2(2+4\varepsilon+3\varepsilon^2+\varepsilon^3-\varepsilon^4)\big)\Big). \tag{A.7}$$

This number is well-defined because $B \neq 0$. We now claim that $r \cdot (x^3 + A(x-B)^2 - y^2) = \xi^3 + \bar{A}(\xi - \bar{B})^2 - \eta^2$. This can easily proved by letting a program like Mathematica shunt symbols around.

Now to show that $r \neq 0$. In order for r to be nonzero, the numerator must be nonzero. By definition, $(1-\varepsilon) \neq 0$, so we need look only at the rest of the numerator. This is

$$\begin{aligned} &16A^2 + 216AB + 729B^2 + 4A\delta^2 + 27B\delta^2 + \delta^4 + 8A\delta^2\varepsilon + 54B\delta^2\varepsilon + \delta^4\varepsilon + 12A^2\varepsilon^2 \\ &+81AB\varepsilon^2 + 6A\delta^2\varepsilon^2 + \delta^4\varepsilon^2 - 8A^2\varepsilon^3 - 54AB\varepsilon^3 + 2A\delta^2\varepsilon^3 + 9A^2\varepsilon^4 - 2A\delta^2\varepsilon^4 - 3A^2\varepsilon^5 + A^2\varepsilon^6. \end{aligned} \tag{A.8}$$

If (A.8) can be 0, what are the consequences for B? We can interpret the above as a quadratic equation in B. By setting it equal to 0 and solving for B, we obtain

$$B = \frac{1}{54}\left(-8A - \delta^2 - 2\delta^2\varepsilon - 3A\varepsilon^2 + 2A\varepsilon^3 \pm \sqrt{3}\sqrt{-\delta^4 - 6A\delta^2\varepsilon^2 - 9A^2\varepsilon^4}\right). \tag{A.9}$$

Let us analyse the term under the square root sign. This term is

$$-\delta^4 - 6A\delta^2\varepsilon^2 - 9A^2\varepsilon^4 = -(\delta^2 + 3A\varepsilon^2)^2. \tag{A.10}$$

Thus B becomes imaginary unless $\delta^2 + 3A\varepsilon^2 = 0$. This means that

$$\delta^2 = -3A\varepsilon^2$$

so A is of the form $-3a^2$ or, equivalently, $\bar{A}$ is a perfect square.

Let us say that $\bar{A}$ is a perfect square, and let $\overline{A} = \overline{a}^2$. The points on $\overline{E}$ with $\xi = 0$ are the two points of order 3, namely $(0, \pm\overline{a}\overline{B})$. These points are not in $\ker(\overline{\alpha})$. Thus if we find that by letting $\delta^2 = -3A\varepsilon^2$, we get $\xi = 0$, we will have found a contradiction, for by assumption $(\xi, \eta) \in \ker(\overline{\alpha})$. Let us now fill in $\delta^2 = -3A\varepsilon^2$ in the equation for ξ found in (A.2).

$$\begin{aligned} \xi &= \delta^2\varepsilon - A\varepsilon^3 + 4A + 27B \\ &= -3A\varepsilon^3 - A\varepsilon^3 + 4A + 27B \\ &= -4A\varepsilon^3 + 4A + 27B. \end{aligned}$$

Also, from the expression of B given in (A.9):

$$\begin{aligned} B &= \frac{1}{54}(-8A - \delta^2 - 2\delta^2\varepsilon - 3A\varepsilon^2 + 2A\varepsilon^3) \\ &= \frac{1}{27}(-4A + 4A\varepsilon^3). \end{aligned}$$

Filling this in gives us $\xi = 0$, which was not allowed. Thus we have proved the claim that $(x, y) \in \Gamma$.

Appendix B

Proof of Lemma 3

Let us restate the lemma before proving it.

Lemma 3. *There is a constant κ, depending on A, B, so that*

$$h(3P) \geq 9h(P) - \kappa$$

for all $P \in \Gamma$.

The proof of this lemma depends on a more general lemma found in [Tat92]. This lemma is stated below.

Lemma 8. *Let $\phi(X)$ and $\psi(X)$ be polynomials with integer coefficients and no common (complex) roots. Let d be the maximum of the degrees of ϕ and ψ.*

(a) There is an integer $R \geq 1$, depending on ϕ and ψ, so that for all rational numbers $\frac{m}{n}$ which are not roots of ψ,

$$\gcd\left(n^2\phi\left(\frac{m}{n}\right), n^d\psi\left(\frac{m}{n}\right)\right) \text{ divides } R.$$

(b) There are constants κ_1 and κ_2, depending on ϕ and ψ, so that for all rational numbers $\frac{m}{n}$ which are not roots of ψ,

$$dh\left(\frac{m}{n}\right) - \kappa_1 \leq h\left(\frac{\phi(m/n)}{\psi(m/n)}\right) \leq dh\left(\frac{m}{n}\right) + \kappa_2.$$

This lemma will not be proved here. We can now add some of our extra knowledge to show that lemma 3 is in fact an instance of this more general lemma. Lemma 3 will hereby be proved.

Proof. Let E be given by

$$\begin{aligned} E : y^2 &= f(x) \\ &= x^3 + ax^2 + bx + c \end{aligned}$$

where $f(x)$ has no double zeroes.

Consider some $P = (x_1, y_1) \in E$. Let $3P = (x_3, y_3)$. What we want to do is write

$$x_3 = \frac{\phi(x_1)}{\psi(x_1)}$$

and show that $d = \max\{\deg(\phi),\deg(\psi)\} = 9$. We then use lemma 8, and the required result follows.

The addition formula we use can be found in [Sil86]. First we use the addition formulas to obtain for $(x_2, y_2) = 2(x_1, y_1)$:

$$\begin{aligned}
x_2 &= \frac{1}{4y_1^2} \cdot (b^2 + 4abx_1 + 4a^2x_1^2 + 6bx_1^2 + 12ax_1^3 + 9x_1^4 - 4ay_1^2 - 8x_1y_1^2) \\
y_2 &= -\frac{1}{8y_1^3} \cdot \big(b^3 + 8a^3x_1^3 + 27x_1^6 + 3b^2x_1(2a + 3x_1) + 8cy_1^2 - 28x_1^3y_1^2 \\
&\qquad + b(12a^2x_1^2 + 36ax_1^3 + 27x_1^4 - 4ay_1^2 - 4x_1y_1^2) \\
&\qquad + 4a^2(9x_1^4 - 2x_1y_1^2) + a(54x_1^5 - 28x_1^2y_1^2)\big).
\end{aligned}$$

Now use the addition formulas again to add (x_1, y_1) to (x_2, y_2), and replace y_1^2 by $x_1^3 + ax_1^2 + bx_1 + c$ to obtain

$$x_3 = \frac{\phi(x_1)}{\psi(x_1)}$$

where

$$\begin{aligned}
\phi(x_1) &= 8b^3c - 32abc^2 + 64c^3 + 9b^4x_1 - 24ab^2cx_1 - 48a^2c^2x_1 + 96bc^2x_1 + 24ab^3x_1^2 \\
&\quad - 96a^2bcx_1^2 + 48b^2cx_1^2 + 16a^2b^2x_1^3 + 36b^3x_1^3 - 64a^3cx_1^3 - 112abcx_1^3 + 48c^2x_1^3 \\
&\quad + 48ab^2x_1^4 - 192a^2cx_1^4 - 24bcx_1^4 + 30b^2x_1^5 - 216acx_1^5 - 8abx_1^6 - 96cx_1^6 - 12bx_1^7 + x_1^9 \\
\psi(x_1) &= b^4 - 8ab^2c + 16a^2c^2 - 24b^2cx_1 + 96ac^2x_1 - 12b^3x_1^2 + 48abcx_1^2 + 144c^2x_1^2 \\
&\quad - 8ab^2x_1^3 + 32a^2cx_1^3 + 144bcx_1^3 + 30b^2x_1^4 + 120acx_1^4 + 48abx_1^5 + 72cx_1^5 \\
&\quad + 16a^2x_1^6 + 36bx_1^6 + 24ax_1^7 + 9x_1^8.
\end{aligned}$$

We can easily see now that $d = 9$, as required, provided that $\phi(x_1)$ and $\psi(x_1)$ have no roots in common. To see this, we rewrite $\phi(x_1)$ and $\psi(x_1)$ as

$$\begin{aligned}
\phi(x_1) &= 8f(x_1)\big(f'(x_1)^3 - 2f(x_1)f'(x_1)f''(x_1) + 8f(x_1)^2\big) + x_1\big(f'(x_1)^2 - 2f(x_1)f''(x_1)\big)^2; \\
\psi(x_1) &= \big(f'(x_1)^2 - 2f(x_1)f''(x_1)\big)^2.
\end{aligned}$$

Let us now assume that $\phi(x_1)$ and $\psi(x_1)$ have zeroes in common. From $\psi(x_1) = 0$ we see that

$$f'(x_1)^2 = 2f(x_1)f''(x_1).$$

This we fill in in $\phi(x_1)$ to obtain

$$\begin{aligned}
\phi(x_1) &= 8f(x_1)\big(f'(x_1)^3 - 2f(x_1)f'(x_1)f''(x_1) + 8f(x_1)^2\big) \\
&= 8f(x_1)\big(f'(x_1) \cdot 2f(x_1)f''(x_1) - 2f(x_1)f'(x_1)f''(x_1) + 8f(x_1)^2\big) \\
&= 64f(x_1)^3.
\end{aligned}$$

Thus the zeroes of the numerator are the zeroes of $f(x_1)$. Can the denominator have these zeroes? If it does, then we see that

$$\begin{aligned} f(x_1) &= 0 \\ f'(x_1)^2 &= 2f(x_1)f''(x_1) \\ &= 0. \end{aligned}$$

Thus it is also a zero of $f'(x_1)$. However, we know that this is impossible, for $f(x_1)$ has no double zeroes, so $f(x_1)$ and $f'(x_1)$ cannot share a common zero. Thus the numerator and the denominator of x_3 share no common zero. The required result now follows from lemma 8.

□

Bibliography

[Duj] Andrej Dujella. High rank elliptic curves with prescribed torsion. `http://web.math.hr/~duje/tors/tors.html`.

[Duj00] Andrej Dujella. Diophantine triples and construction of high-rank elliptic curves over $\mathcal{Q}$ with three non-trivial 2-torsion points. *Rocky Mountain J. Math.*, 30(1):157–164, 2000.

[Kna92] Anthony W. Knapp. *Elliptic Curves*. Princeton University Press, 1992.

[Pom74] David E. Penney & Carl Pomerance. A search for elliptic curves with large rank. *Mathematics of Computation*, 28(127):851–853, 1974.

[Ros80] Kenneth Ireland & Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer, 2nd ed. edition, 1980.

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1986.

[Ste08] P. Stevenhagen. *Number Rings*. Universiteit Leiden, 2008.

[Tat92] Joseph H. Silverman & John Tate. *Rational Points on Elliptic Curves*. Springer-Verlag, 1992.

[Top91] Jaap Top. Descent by 3-isogeny and 3-rank of quadratic fields. In Fernando Q. Gouvêa & Noriko Yui, editor, *Advances in Number Theory*, pages 303–317. Oxford Science Publications, 1991.

[Top07] Jaap Top. Plaster- and string models, December 2007. `www.math.rug.nl/~top/lectures/BYU.pdf`.

[WB97] Catherine Playoust Wieb Bosma, John Cannon. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3–4):235–265, 1997.

[WR] Inc. Wolfram Research. *Mathematica*. Version 7.0 edition.