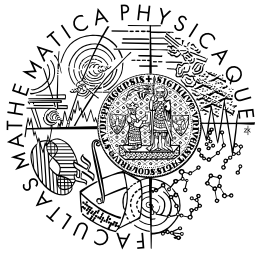


FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

BACHELOR THESIS

Adam Klepáč

Elliptic Curves and Diophantine Equations

Department of Algebra

Supervisor of the bachelor thesis: doc. RNDr. Jan Šťovíček, Ph.D.
Study programme: General Mathematics
Study branch: Mathematical Structures

Prague 2020

I declare that I carried out this bachelor thesis independently, and only with the cited sources, literature and other professional sources. It has not been used to obtain another or the same degree.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In ..... date ....

Author's signature

First and foremost, I thank my supervisor for careful examination of my work, for pointing out little details and more serious mistakes together with hints on possible corrections and betterments, as well as explanatory remarks which enriched my understanding of the subject.

Title: Elliptic Curves and Diophantine Equations

Author: Adam Klepáč

Department: Department of Algebra

Supervisor: doc. RNDr. Jan Šťovíček, Ph.D., Department of Algebra

Abstract: Given an equation of the form $f(x, y) = 0$, where f is a polynomial in two variables with rational coefficients of degree lower or equal to three, we will study the properties of the set of its rational solutions. We will show that if f is irreducible and the degree of f is three, then the corresponding cubic curve is birationally equivalent to a special cubic curve, often called elliptic. Furthermore, we will define a group law on the set of rational points of an elliptic curve and finish with the proof of Nagell-Lutz theorem, which states that all rational points of finite order in such defined group have integral coordinates.

Keywords: Diophantine equations, Elliptic curves, Algebraic geometry

Contents

Used Notation

Symbol	Meaning
$\overline{x}$	The n-tuple $(x_1, \ldots, x_n)$ where $n \in \mathbb{N}$ is given.
$\ell(f)$	The leading coefficient of a given polynomial f.
$c(f)$	The constant term of a given polynomial f.
$a \mid b$	a divides b.
$\gcd(a, b)$	Greatest common divisor of a and b.
$\mathbb{P}(\mathbb{R}^2)$	The projective real plane.
C_f	The algebraic curve defined by $f(x, y) = 0$.
$a \parallel b$	$a \mid b$ and $b \mid a$.
$\mathcal{R}(C)$	The set of rational points of a given curve C.
f_x	The partial derivative of f with respect to x.
$x(P), y(P)$	The x and y-coordinate of the point P.
$\mathrm{ord}(P)$	The order of the element P in a given group.
$\mathfrak{p}(q)$	Prime affinity of the rational number q.
$\mathcal{R}_p^{\nu}(C)$	The points $(x, y) \in \mathcal{R}(C)$ that $\mathfrak{p}(x) \leq -2\nu$ and $\mathfrak{p}(y) \leq -3\nu$.
$t(P), s(P)$	The t and s-coordinate of the point P.
R_p	The subring of rational numbers that $\mathfrak{p}(q) \geq 0$.

Preface

The main subject of the thesis is to acquaint the reader with the basic theory of Diophantine equations and how the study of rational algebraic curves leads to potential solutions thereof.

Most of the facts presented and elucidated in this text are inspired by or based off of books Silverman and Tate [2015], Washington [2008] and Fulton [2008]. Nonetheless, unless explicitly cited, these sources were used solely as a medium to tighten my grasp of the subject, rather than followed step by step. For instance, sections 1.2, 1.3 and 2.1 were almost entirely conceptualized by myself and present ideas not borrowed from any specific source. Furthermore, many claims and proofs thereof were modified to better suit the needs of this text. **Lemma 3.1.2** or **Lemma 3.2.2** make two examples. All the examples and problems, save one, located at the end of each chapter also sprang from my head and were tailored to show the computational side of presented theory.

I have always valued insight above rigorousness. Owing to that, many passages in the text are deliberately vague, offering facts or explanatory remarks without complete proofs. None of these are meant to progress the study, only to bring light upon subjects which may, if first met, escape one's reason, so to speak. I implore you, dear reader, should you not share this sentiment, to overlook and tolerate it.

1. Introduction

1.1 A Diophantine Equation

Let us start strong with arguably the most important definition of the thesis. Although Diophantine[1] equation is a well-known term, it is often associated with integers. Since we are interested (most of the time) in rational equations and their rational solutions, we define it as follows.

Definition 1.1.1 (Diophantine equation)**.** The equation of the form

$$f(\overline{x}) = 0 \tag{1.1.1}$$

where $f \in \mathbb{Q}[x_1, \ldots, x_n]$ for any non-zero $n \in \mathbb{N}$ is called *Diophantine*. The *solution to a Diophantine equation* is any rational n-tuple $\overline{x} \in \mathbb{Q}^n$ satisfying (1.1.1). We call $\deg f$ the *order* of equation (1.1.1).

One of the most famous Diophantine problems is Fermat's[2] Conjecture, also known as Fermat's Last Theorem, which states that for any natural $n > 2$ there are no natural solutions to the equation

$$x^n + y^n = z^n$$

if every one of x, y, z is non-zero.

In the case $n = 1$, it is evident that there are infinitely many solutions. This holds for $n = 2$ as well. This fact is less obvious but still fairly straightforward to prove using modular arithmetic. We will discuss the solutions (existence and number thereof) to a more general equation

$$ax^2 + by^2 + cz^2 = 0$$

in **Section 1.2**. First general proof of Fermat's Last Theorem was given by Sir Andrew Wiles in 1985[3] and is well beyond the scope of this thesis.

However, since this would be a sad note to finish our introduction to Diophantine equations on, we are now going to take a look at a rather famous problem wherein a Diophantine equation arises naturally and which we will be able to (at least partially) solve.

Problem 1.1.1 (A pile of cannonballs. Borrowed from Anglin [1990])**.** Imagine a pile of (hopefully unused) cannonballs forming a square pyramid with each floor having one less cannonball in each dimension. The question is: how many cannonballs do we have to use as a base for the pyramid so that when the pyramid collapses all the cannonballs can form a perfect square?

[1] Diophantus of Alexandria (between 201 and 215 AD - between 285 and 299 AD), Hellenistic mathematician, author of *Arithmetica*. Heath [2009]

[2] Pierre de Fermat (1607 - 1665), French lawyer and mathematician. Pellegrino [2000]

[3] The story behind Wiles's proof was made into a book by Simon Sings. Singh [1997]

Figure 1.1.1: Pyramid of cannonballs.

Omitting the fact that Diophantus of Alexandria most likely did not have cannonballs at his disposal, there is no obvious way this problem leads to an equation such as (1.1.1). Let us formalize it first.

Let $n \in \mathbb{N}$ denote the number of balls on one side of the pyramid's base, that is, n^2 is the number of cannonballs forming the base. According to our assumption, the next floor is made of $(n-1)^2$ balls, the next of $(n-2)^2$, etc. All in all, we have

$$n^2 + (n-1)^2 + \ldots + 1$$

balls forming the pyramid. We want all the balls to form a square, say, of side $m \in \mathbb{N}$ when the pyramid collapses. So, we are looking for such a pair of natural numbers m, n that

$$n^2 + (n-1)^2 + \ldots + 1 = m^2.$$

We are almost there. For us to be able to solve this equation, the left side must be in a form that we can work with comfortably, that is, in a form of an expression whose number of elements is independent of n. One can easily prove using induction that

$$n^2 + (n-1)^2 + \ldots + 1 = \frac{n(n+1)(2n+1)}{6}.$$

Since it is customary to write Diophantine equations using x and y, in order to prevent confusion, we restate our problem as finding all natural solutions to the equation

$$\frac{x(x+1)(2x+1)}{6} = y^2. \tag{1.1.2}$$

We will solve equation (1.1.2) using geometry. This might be a weird approach but it serves to illustrate a method which we are going to employ again and again when working with elliptic curves in later sections. If we plot the curve defined by (1.1.2) in the real plane, it looks like Figure 1.1.2.

Remark. Later, we will call these types of curves *elliptic*. In case you are wondering, the name *elliptic* is purely historical and their connection to ellipses helps us in no significant way.[4]

We will now use our two trivial solutions $(0, 0)$ and $(1, 1)$ to try to find other points of natural, or at least rational, coordinates on the curve. Arguably the

[4]The naming was influenced by the fact that elliptic curves arise when calculating the length of the arc of an ellipse. See Barsagade and Meshram [2014].

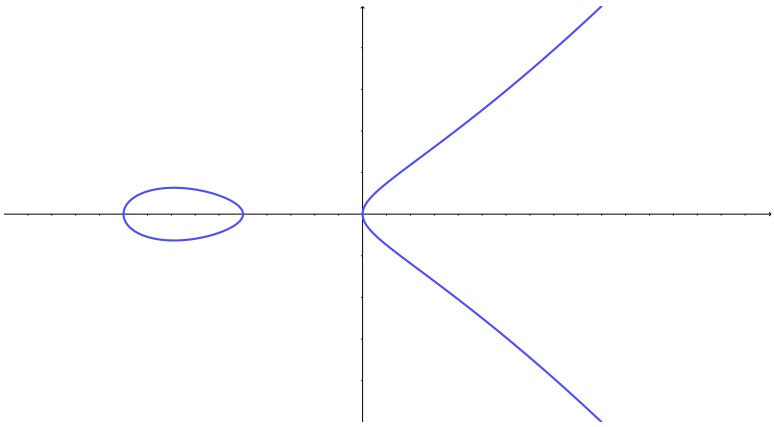


Figure 1.1.2: The curve $y^2 = x(x+1)(2x+1)/6$.

most straightforward way to do so is to find the line connecting said points and take the third point where it intersects the curve.

Obviously, the line connecting $(0,0)$ and $(1,1)$ is $y = x$. The x-coordinate of the intersection is found by solving

$$x^2 = \frac{x(x+1)(2x+1)}{6}.$$

Rearranging terms gives

$$-\frac{x^3}{3} + \frac{x^2}{2} - \frac{x}{6} = 0.$$

Since we know two of the solutions, 0 and 1, we can factor out the corresponding linear factors to obtain

$$-\frac{x\,(x-1)\,(2x-1)}{6} = 0,$$

from which we easily deduce that the x-coordinate of the third intersection is $1/2$. Substituting into (1.1.2) yields points $(1/2, 1/2)$ and $(1/2, -1/2)$. The intersection we were looking for is clearly $(1/2, 1/2)$ but it is obvious that $(1/2, -1/2)$ lies on the curve as well due to symmetry. We could say the same about $(1,1)$ and $(1,-1)$.

Now that we have another point on the curve, we are getting closer to the solution to our problem. Half a cannonball is hardly a satisfying answer if one is concerned about applications in warfare, but we can use the new points to get other points on the curve, again by intersecting. We could use the line passing through $(1/2,-1/2)$ and $(1/2,1/2)$ but that is a vertical line and does not intersect the curve in any third point.

Remark. As a side note, in the future we will need every line to intersect a cubic curve in exactly three points so we are addressing this issue in **Section 1.3**.

Let us use another line. For example, take $y = 3x - 2$, the line passing through $(1,1)$ and $(1/2,-1/2)$. To get the third intersection, we solve

$$(3x-2)^2 = \frac{x(x+1)(2x+1)}{6}.$$

Without indulging in detailed algebraic manipulation, we kindly spare you the act and present the solution, namely $x = 24$. There - it is natural! If we have 24 balls forming the base of the pyramid, then y must be natural as well. Truly, another substitution gives $y = 70$. So we have gotten a non-trivial solution to our Cannonballs Problem, 24 balls at the side of the base and 70 in the final square.

We shall stop here. With our ultimate goal being to find all the natural solutions, we disclose the secret that there are no other natural solutions besides $(0, 0), (1, 1)$ and $(24, 70)$. The proof of this fact is not trivial but not exceedingly difficult, either. It can be found in Anglin [1990].

The purpose of this problem was to present the method of intersecting a rational line with a cubic curve to obtain previously unknown rational points. Since a line intersects any cubic curve in exactly three points (a remark soon to be formalized and proven), connecting two rational points on a curve has a chance to yield a third one. Even better, drawing a tangent line to some rational point is often enough to get another.

We now digress a little and take a look at simpler Diophantine equations to show that Diophantine equations in two variables of order three are in a sense the simplest type that is not yet fully understood.

1.2 Lines and Conics

As promised, in this section we shall study Diophantine equations in one variable of any order or in two variables of orders one and two. Let us start with the former. If $f \in \mathbb{Q}[x]$, $\deg f = n \in \mathbb{N}$ chosen arbitrarily, there exists an elementary algorithm of finding all rational solutions to

$$f(x) = 0. \tag{1.2.1}$$

The algorithm consists of trying all possible combinations of numerators and denominators from a finite set determined by the following lemma. Before we state it, we note that we can assume the polynomial f in (1.2.1) to have integer coefficients if we multiply the equation by the greatest common multiple of the denominators of the coefficients of f.

Lemma 1.2.1 (Gauss's lemma)**.** *Let $n \in \mathbb{N}$ be non-zero. Let $f \in \mathbb{Z}[x]$, $\deg f = n$, $p/q \in \mathbb{Q}$ where $\gcd(p, q) = 1$. If p/q is the root of f, then $p \mid c(f)$ and $q \mid \ell(f)$.*

The proof of Gauss's lemma can be found in probably every beginner book about algebra but let us do it nonetheless since it is fairly trivial, thus a good warm-up as the first proof of the thesis.

Proof. Let $p/q \in \mathbb{Q}$ be the root of f. Let $a_0, \ldots, a_n \in \mathbb{Q}$ and

$$f(x) = \sum_{i=0}^{n} a_i x^i.$$

By substituting $x = p/q$ we get

$$f\left(\frac{p}{q}\right) = \sum_{i=0}^{n} a_i \left(\frac{p}{q}\right)^i = 0.$$

Multiplying by q^n and rearranging a little yields

$$a_0 q^n + a_1 p q^{n-1} + \ldots a_{n-1} p^{n-1} q = -a_n p^n.$$

Since p divides the right side, it must divide the left side as well. Obviously, p divides every one of $a_i p^i q^{n-i}$ for $i = 1, \ldots, n-1$. It follows that $p \mid a_0$ since $\gcd(p, q) = 1$ by assumption. The conclusion $q \mid a_n$ follows analogously from

$$a_1 p q^{n-1} + \ldots + a_n p^n = -a_0 q^n. \qquad \square$$

This is everything we need to solve (1.2.1). It is sufficient to try every rational number p/q satisfying $p \mid c(f)$ and $q \mid \ell(f)$.

With polynomials in one variable out of the way, time is nigh to step up and add a new variable. We set the order of the equation to be 1, to talk about lines. The general equation of a rational line is

$$ax + by + c = 0 \tag{1.2.2}$$

for $a, b, c \in \mathbb{Q}$ and at least one of a, b non-zero.

Unsurprisingly, every rational line has infinitely many rational points. For example the tuple $(q, (-c - aq)/b)$ (or $(-c/a, q)$ for $b = 0$) is evidently rational for any $q \in \mathbb{Q}$ and does indeed lie on a line defined by (1.2.2). Given that we want to make ample use of intersections, let us convince ourselves that two rational lines truly intersect each other in a rational point. It may sound trivial, and it is. For the sake orderliness, however, we formulate it as an unnamed claim and prove it in utmost brevity.

Claim 1.2.2. *Two non-parallel rational lines intersect at a rational point.*

Remark. As we have stated in the previous section, the 'non-parallel' condition is only temporary. We will have a way of making certain that every two lines *do* intersect, including parallel ones.

Proof. Let

$$\begin{aligned} ax + by + c &= 0, \\ dx + ey + f &= 0 \end{aligned}$$

where $a, \ldots, f \in \mathbb{Q}$ be our two rational lines. Substituting $y = -(c + ax)/b$ into the second equation gives

$$dx - e\left(\frac{ax + c}{b}\right) + f = 0$$

which after elementary manipulation reduces to

$$x = \frac{bf - ce}{ae - bd}.$$

Since we assumed the lines to be non-parallel, the vectors $(a, b)^T$ and $(d, e)^T$ are linearly independent. A basic claim from linear algebra states that in such case

$$\det \begin{pmatrix} a & d \\ b & e \end{pmatrix} = ae - bd \neq 0,$$

thus the fraction is well-defined. Substituting back to $ax + by + c = 0$ gives us the second coordinate

$$y = \frac{-af + cd}{ae - bd}.$$

This completes the proof for the point (x, y) is obviously rational. □

Finally, we are ready to move to conics, that is, curves defined by Diophantine equations

$$f(x, y) = 0$$

where $\deg f = 2$. If we wished to write the equation more explicitly, we would be left with

$$ax^2 + by^2 + cxy + dx + ey + f = 0, \tag{1.2.3}$$

where $a, \ldots, f \in \mathbb{Q}$ and at least one of a, b, c non-zero.

Let us start with the easy part. We shall prove that when there is at least one rational solution to (1.2.3) then there are infinitely many. One way to do so is by projecting the curve defined by (1.2.3) onto a line.

Let P be the rational solution to (1.2.3), hence a rational point on the conic that we style C. Take a rational line L given by $kx + ly + m = 0$ for $k, l, m \in \mathbb{Q}$, k or l non-zero, such that $P \notin L$. If we take any rational point on L, say Q, the line connecting P and Q will be rational. We will call it L_{PQ}. Since a line meets a conic in two points, there exists another intersection point of L_{PQ} and C besides P. We are aiming to prove that this point is rational as well. This is actually quite easy and requires no additional calculations. Nonetheless, we formulate it as a claim, yet again.

Claim 1.2.3. *Let P be a rational point on C and Q a rational point on L. Then all the intersection points of L_{PQ} and C are rational.*

Proof. L_{PQ} is a rational line, hence its equation is

$$kx + ly + m = 0$$

for $k, l, m \in \mathbb{Q}$, k or l non-zero. If $l \neq 0$, then plugging $y = (-m - kx)/l$ into our conic equation (1.2.3) yields a quadratic equation in one variable, which we very well know how to solve. The exact solutions are irrelevant but we know they are of the form

$$x = \frac{\alpha \pm \sqrt{\Delta}}{\beta},$$

where α, β, Δ are rational terms dependent on $a, \ldots, f, k, l$. Since one of the solutions is P, a rational point, it immediately follows that $\sqrt{\Delta} \in \mathbb{Q}$. Then the other solution is necessarily rational as well.

The case $k \neq 0$ is handled similarly, only the substitution $x = (-m - ly)/k$ is required. □

It is not hard to see that this way we get a (almost) one-to-one correspondence between the rational points on the conic C and the rational points on the line L. Since L is by assumption rational, there are infinitely many such points. We do

not really need to limit ourselves to rational points, either. We can project any point on the conic C, save the one point P' wherefor $L_{PP'}$ is parallel to L, onto a chosen line L. So, with this we have taken care of the number of solutions to (1.2.3).

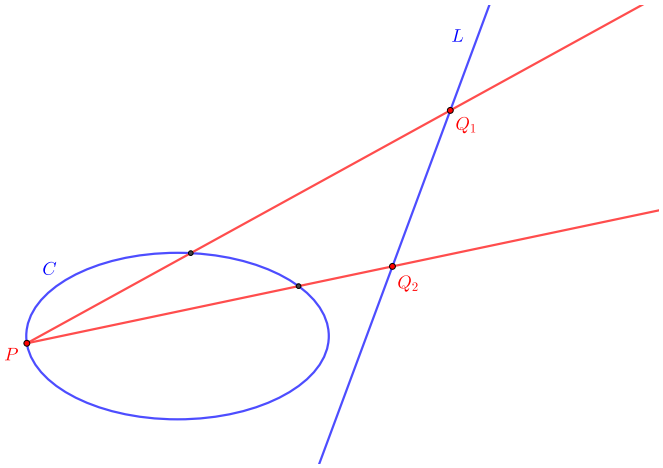


Figure 1.2.1: Projecting the curve C onto the line L.

We further take a glimpse at how to check whether a given conic even has a rational point or not. We are going to prove a theorem by Legendre[5] which gives us a satisfying condition for the equation

$$ax^2 + by^2 + cz^2 = 0, \quad a, b, c \in \mathbb{Z} \tag{1.2.4}$$

to have a rational solution. But first, we have to 'link' the solutions of (1.2.3) to the solutions of (1.2.4). This will occupy us for a few paragraphs.

The following construction is partially adopted from Lee [2012], p. 1 - 2. Less detailed parts of proofs were completed and numerous explanatory remarks added.

We have to do some algebraic manipulation. First, let us introduce a new variable z and let $x \coloneqq x/z$, $y \coloneqq y/z$. After substituting into (1.2.3) and multiplying by z^2 we get

$$ax^2 + by^2 + cxy + dxz + eyz + fz^2 = 0. \tag{1.2.5}$$

Remark. Later, we will call this process of introducing a new variable to even the degrees of terms in a polynomial, *homogenization*.

First of all, we will prove a rather simple lemma that shows the connection between rational solutions to (1.2.3) and integer solutions to (1.2.5).

Lemma 1.2.4. *Equation* (1.2.3) *has a rational solution if and only if the equation* (1.2.5) *has a non-trivial integer solution.*

Proof. If $(x, y) = (p_1/q_1, p_2/q_2)$ is the rational solution of (1.2.3) then

$$(x, y, z) = (p_1q_2, p_2q_1, q_1q_2)$$

[5] Adrien-Marie Legendre (1752 - 1833), French mathematician. Duren [2009]

is the solution to (1.2.5).

On the contrary, if (1.2.5) has a non-trivial solution then at least one of x, y, z must be non-zero. If $z \neq 0$, we have finished because $(x/z, y/z)$ is a rational solution to (1.2.3). If $z = 0$, we can assume without loss of generality that $x \neq 0$. After dividing by x^2 and setting $y' \coloneqq y/x$ and $z' \coloneqq z/x$, (1.2.5) transforms into

$$a + b(y')^2 + cy' + dz' + ey'z' + f(z')^2 = 0.$$

However, there is the rational solution $(y/x, z/x)$ to this equation corresponding to the solution (x, y, z) of (1.2.5). By **Claim 1.2.3** and the discussion below, there are infinitely many rational points on the conic defined by the equation above. However, at most two of them can have $z' = 0$ since substituting $z' = 0$ leads to a quadratic equation in y', hence an equation with two distinct solutions at most. Let $(y', z') = (y/x, z/x)$ be the solution with $z' \neq 0$. Then (x, y, z) is a non-trivial solution to (1.2.5) with $x \neq 0$ and $z \neq 0$. This implies that $(x/z, y/z)$ is a non-trivial rational solution to (1.2.3). □

Remark. It's obvious that (1.2.5) has a non-trivial integer solution if and only if it has a non-trivial rational solution. If $(p_1/q_1, p_2/q_2, p_3/q_3)$ is a non-trivial rational solution, then multiplying (1.2.5) by $q_1^2 q_2^2 q_3^2$ gives us a non-trivial integer solution.

We must now transform the equation (1.2.5) into (1.2.4). After some elementary manipulation, (1.2.5) becomes

$$a\left(x + \frac{c}{2a}y + \frac{d}{2a}z\right)^2 + \left(b - \frac{c^2}{4a}\right)y^2 + \left(f - \frac{d^2}{4a}\right)z^2 + \left(e - \frac{cd}{2a}\right)yz.$$

We let

$$x' \coloneqq x + \frac{c}{2a}y + \frac{d}{2a}z$$

and further compute

$$\begin{aligned}&\left(b - \frac{c^2}{4a}\right)y^2 + \left(f - \frac{d^2}{4a}\right)z^2 + \left(e - \frac{cd}{2a}\right)yz \\ &= \left(b - \frac{c^2}{4a}\right)\left(y + \frac{2ae - cd}{4ab - c^2}z\right)^2 + \left(f - \frac{d^2}{4a} - \frac{1}{4a}\left(\frac{2ae - cd}{4ab - c^2}\right)^2\right)z^2.\end{aligned}$$

Thus, ultimately, we let

$$y' \coloneqq y + \frac{2ae - cd}{4ab - c^2}z, \quad z' \coloneqq z$$

and $b', c' \in \mathbb{Q}$ their corresponding coefficients to obtain the equation

$$a(x')^2 + b'(y')^2 + c'(z')^2 = 0. \tag{1.2.6}$$

We can easily see that a, b', c' are rational numbers and the mapping $(x, y, z) \mapsto (x', y', z')$ and its inverse are rational as well. It follows that (x, y, z) is a rational solution to (1.2.5) if and only if (x', y', z') is a rational solution to (1.2.6).

Remark. We should note that the mapping $(x, y, z) \mapsto (x', y', z')$ is indeed well-defined. It could happen, for instance, that $a = 0$ in (1.2.5). Then the fraction $c/2a$ would make no sense. That is true, however, to solve this problem, we can introduce another rational mapping - for example $y \mapsto y + x$ - to introduce an x^2 into (1.2.5) with a non-zero coefficient. Thus, without loss of generality, we can assume all fractions in our definitions of x', y', z' exist.

There is one last step remaining before we can formulate Legendre's theorem. We can obviously assume that a, b', c' are integers if we multiply (1.2.6) by a common denominator. We can also assume that a, b', c' are square-free. Indeed, let for instance $a = k^2 l$ for some non-zero $k, l \in \mathbb{Z}$. We can get rid of the factor k^2 by setting $x' \coloneqq kx''$ and substituting back to (1.2.6). That is a rational transformation and as such alters not the existence or number of rational solutions. Finally, we can assume that a, b', c' are pairwise coprime. Obviously, if a, b', c' share a common factor, we can simply divide by it. Let us imagine that there exists a factor $n \in \mathbb{Z}$ such that $n \mid a, b'$ but $n \nmid c'$. We can set $z' \coloneqq nz''$ and by replacing $a \coloneqq na'', b' \coloneqq nb''$, we can divide the equation by n which eliminates the factor. This procedure necessarily ends within a finite number of steps since each time we divide the equation by a common factor reducing the product $ab'c' = n^2 a''b''c'$ to $na''b''c'$. Hence, in a finite number of steps, we end up with a, b, c pairwise coprime.

With all the tiresome technicalities out of the way we shall now state Legendre's theorem about the existence of solution to (1.2.6). Nevertheless, we shall not prove it here as the proof is in itself quite lengthy and technical.

Theorem 1.2.5 (Legendre's)**.** *Let $a, b, c \in \mathbb{Z}$ be non-zero, square-free and pairwise coprime. Then the Diophantine equation*

$$ax^2 + by^2 + cz^2 = 0$$

has a non-trivial rational solution if and only if

(1) a, b, c do not all have the same sign,

(2) $-ab$, $-bc$ and $-ca$ are quadratic residues modulo c, a and b, respectively.

Proof. See Grosswald [1985], chapter Legendre's Theorem, **Theorem 1.** □

With this, I daresay, we have taken care of conics, too. We know how to check whether a given conic contains a rational point and once we have one rational solution, we can find every other.

One last topic remains to be touched upon before we are equipped to tackle the theory of elliptic curves, and that is projective geometry.

1.3 The Projective Plane

In the previous section we mentioned we would use the projective plane to ensure that every two lines intersect at exactly one point, including parallel ones. Since

most of the time we will be working in the real plane, we define the projective plane as an 'extension' thereof. The complex construction is analogous.

Obviously, the projective plane must contain all the points that the real plane does, for the simple reason that non-parallel lines can intersect at any point whatsoever. However, we also need to add the points where parallel lines would intersect. Notice that I have used the plural *points*, for we need to add many. Infinitely many, in fact. It would make little sense from algebraic or geometric standpoint should every two parallel lines intersect at the same point. So, for every direction parallel lines share, we add a point to the real plane. And that is it, that is the principal idea behind the construction. Without bathing in formalities just yet, we can define the projective real plane as

$$\mathbb{P}(\mathbb{R}^2) = \mathbb{R}^2 \cup \{\text{the directions of lines in } \mathbb{R}^2\}. \tag{1.3.1}$$

This definition, however, is not very precise or useful for computational purposes. We know that the direction of a line in $\mathbb{R}^2$ given by

$$ax + by + c = 0$$

is determined by the numbers $a, b \in \mathbb{R}$. Nonetheless, the line

$$2ax + 2by + d = 0,$$

for instance, has the same direction as the previous one. It is obvious that one point in $\mathbb{P}(\mathbb{R}^2)$ must correspond to both lines. In light of this, we define relation $\sim$ on the set of real triples by

$$(a, b, c) \sim (a', b', c') \overset{\text{def.}}{\iff} \exists \lambda \in \mathbb{R} : (a', b', c') = \lambda(a, b, c).$$

Our 'official' definition of $\mathbb{P}(\mathbb{R}^2)$ will be the quotient set of $\mathbb{R}^3$ by $\sim$ excluding the point $(0, 0, 0)$ since no line has the direction of $(0, 0)$.

Definition 1.3.1 (Projective plane)**.** The *projective real plane* is defined as

$$\mathbb{P}(\mathbb{R}^2) \coloneqq {}^{\mathbb{R}^3 \setminus \{(0,0,0)\}}\!/_{\sim}. \tag{1.3.2}$$

We shall denote

$$[a : b : c] \coloneqq \{(a', b', c') \in \mathbb{R}^3 \mid (a', b', c') \sim (a, b, c) \wedge (a, b, c) \neq (0, 0, 0)\}.$$

The *projective complex plane*, $\mathbb{P}(\mathbb{C}^2)$, is defined exactly the same, with complex numbers in lieu of the reals in all related definitions.

In other words, $\mathbb{P}(\mathbb{R}^2)$ is the set of all triples $[a : b : c]$. We will briefly elucidate why definitions (1.3.1) and (1.3.2) are equivalent.

It is easy to see that to each tuple $(x, y) \in \mathbb{R}^2$ we can assign the point $[x : y : 1] \in \mathbb{P}(\mathbb{R}^2)$. On the other hand, if $[x : y : z] \in \mathbb{P}(\mathbb{R}^2)$ and $z \neq 0$, we can divide by z to get $[x/z : y/z : 1]$ which is by definition equal to $[x : y : z]$. Thus, there is a one-to-one correspondence between points (x, y) of the real plane and points $[x : y : 1]$ of the projective plane. Then what about points $[x : y : 0]$? These are,

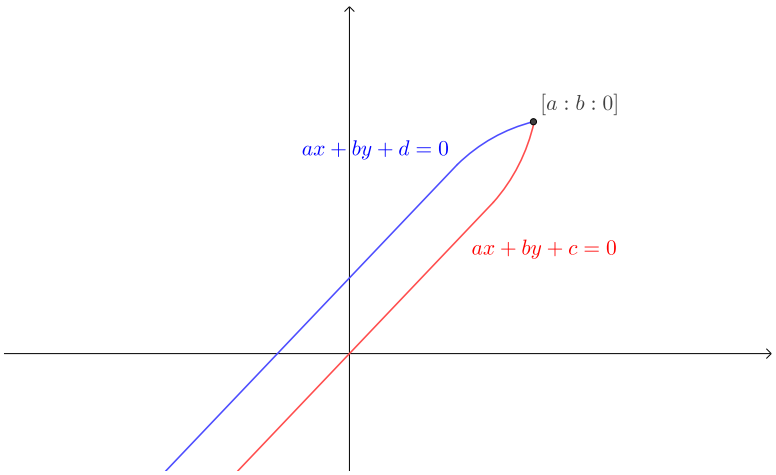


Figure 1.3.1: Two parallel lines intersecting at 'infinity'.

again, in one-to-one correspondence with the directions of lines in $\mathbb{R}^2$. Indeed, by definition $[x : y : 0] = [\lambda x : \lambda y : 0]$ for any non-zero $\lambda \in \mathbb{R}$ which is wholly in accordance with the fact that the directions of lines given by

$$x + y + c = 0, \quad \lambda x + \lambda y + d = 0$$

are the same.

We have shown that points $(x, y) \in \mathbb{R}^2$ correspond to points $[x : y : 1] \in \mathbb{P}(\mathbb{R}^2)$ and directions of lines in $\mathbb{R}^2$ given by tuples $(a, b) \in \mathbb{R}^2$ correspond to triples $[a : b : 0] \in \mathbb{P}(\mathbb{R}^2)$. The last thing we need to look at is how Diophantine equations translate to the projective plane.

Take the equation

$$f(x', y', z') = 0$$

where $f \in \mathbb{Q}[x, y, z]$. What does it mean that a triple $[x' : y' : z'] \in \mathbb{P}(\mathbb{R}^2)$ satisfies such an equation? Since we have $[x' : y' : z'] = [\lambda x' : \lambda y' : \lambda z']$ for all $\lambda \in \mathbb{R}$, the point $(\lambda x', \lambda y', \lambda z')$ must be the root of f for all real λ, too. This occurs if f is *homogeneous*, that is, all terms of f share the same degree. Indeed, if f is homogeneous and (x', y', z') is a root of f, then for any real λ we have

$$f(\lambda x', \lambda y', \lambda z') = \lambda^n f(x', y', z') = 0,$$

so $(\lambda x', \lambda y', \lambda z')$ is the root of f as well.

Provided we would like to work in the projective plane and we have the bijective mapping $(x, y) \mapsto [x : y : 1]$ at our disposal, we must, for a given $f \in \mathbb{Q}[x, y]$, find such a polynomial $g \in \mathbb{Q}[x, y, z]$ that

$$f(x, y) = 0 \iff g(\lambda x, \lambda y, \lambda) = 0.$$

for all $\lambda \in \mathbb{R}$. This necessity is in the heart of the following definition.

Definition 1.3.2 (Homogenization)**.** For a given $f \in \mathbb{Q}[x, y]$, $\deg f = n$, we define its *homogenization* $f^* \in \mathbb{Q}[x, y, z]$ by

$$f^*(x, y, z) \coloneqq z^n f\left(\frac{x}{z}, \frac{y}{z}\right).$$

It is elementary to check that f^* is homogeneous and that $f^*(x, y, 1) = f(x, y)$.

If we take the curves C_f, C_{f^*} defined by f and f^* respectively, it follows directly from the aforewritten definition that $[x : y : z]$ for z non-zero is a rational point on C_{f^*} if and only if $(x/z, y/z)$ is a rational point on C_f. Compare this fact with our findings about rational points on conics, especially the transformation of (1.2.3) to (1.2.5). Hence, if we wish to study the rational solutions to $f(x, y) = 0$ in the real plane, we can instead study the rational solutions to $f^*(x, y, z) = 0$ for z non-zero in the projective plane.

At this point you might (and you should) be wondering why we went through all this for. What is the advantage of working in the projective plane instead of the real one?

The main reason we will be working in the projective plane is Bézout's[6] theorem. It is not only that parallel lines intersect in the projective plane (by definition at the point defined by their shared direction) but any two curves defined by coprime polynomials $f, g \in \mathbb{Q}[x, y]$, of degrees d_f, d_g respectively, cross each other exactly $d_f \cdot d_g$ times, including the multiplicity of such intersections.

We have not defined multiplicity of intersection (or intersection number, the formal term) and we do not mean to. It would be going too deep into technical details for a theorem whereof we will only have employed a very special case. What we need is that a line intersects a cubic curve generally in three points. There exist the special cases of tangent lines and inflexion points which count as multiple intersections but we shall touch upon this topic in the next chapters. Before we state Bézout's theorem, we (finally) properly define a rational algebraic curve.

Definition 1.3.3 (Rational algebraic curve)**.** Let $f \in \mathbb{Q}[x, y]$, $\deg f = n \in \mathbb{N}$, be a polynomial irreducible over $\mathbb{Q}$. The set of real (complex) tuples $(x, y) \in \mathbb{R}^2(\mathbb{C}^2)$ satisfying

$$f(x, y) = 0$$

is called a *rational algebraic curve*. If f is the defining polynomial, we denote C_f the curve defined by f. In the following, the attribute *rational algebraic* will be in most cases omitted. Unless specified otherwise, the term *curve* stands for a rational algebraic curve defined over $\mathbb{R}$.

Remark. Why do we want f to be irreducible? Because if $f = gh$ for some polynomials g, h of lower degree, then the set of rational points on C_f is the union of the set of rational points on C_g with the set of rational points on C_h. As such, there is no benefit in allowing f to be reducible.

In a similar fashion, we define a *rational projective curve* as the set of triples $[x : y : z] \in \mathbb{P}(\mathbb{R}^2)$ (or $\mathbb{P}(\mathbb{C}^2)$) satisfying

$$f(x, y, z) = 0$$

if $f \in \mathbb{Q}[x, y, z]$ is irreducible and homogeneous. It is not hard to prove that if f is irreducible, then so is f^* (see Fulton [2008], Section 4.3, **Proposition 3.** for

[6] Étienne Bézout (1730 - 1783), French mathematician. Grabiner [1970-1980], p. 111 - 114

a more general result). It follows from our findings in previous paragraphs that C_{f^*} is a rational projective curve and $C_f = C_{f^*} \cap \mathbb{R}^2$ (we formally identify (x, y) with $[x : y : 1]$). We will scarcely call C_f the *affine part* of C_{f^*}.

Let us now formulate Bézout's theorem, the very last piece of equipment we need for the theory of rational points on elliptic curves.

Theorem 1.3.1 (Bézout's)**.** *Let $f, g \in \mathbb{Q}[x, y, z]$, $f \nmid g$ be irreducible homogeneous polynomials, of degrees n and m respectively. Then the complex curves C_f, C_g intersect in exactly mn points, in the projective plane and counting multiplicities.*

Proof. See Silverman and Tate [2015], chapter Projective Geometry, p. 242 - 251. □

Remark. We need to assume C_f, C_g are defined over $\mathbb{C}$ since Bézout's theorem only works in algebraically closed fields. This, however, is not an issue because we will only ever intersect cubic curves with lines that already have two other real (even rational) intersections with the curve. Given that two intersections are real, the third must be real as well because complex solutions to a cubic equation always come in conjugate pairs.

Henceforth, we always assume our curves C_f are defined in the projective plane but will omit the z-coordinate. That is, instead of the formal $f^*(x, y, 1)$, we only write $f(x, y)$ if not contextually appropriate otherwise.

1.4 Examples and Problems

Problem 1.4.1. Show that the ellipse $3x^2 + 5y^2 - 4 = 0$ has no rational point.

Solution. We shall use **Legendre's theorem**. We first homogenize $f(x, y) = 3x^2 + 5y^2 - 4 = 0$ to obtain

$$3x^2 + 5y^2 - 4z^2 = 0. \tag{1.4.1}$$

We have $a = 3, b = 5, c = -4$. Obviously, c has a different sign than a and b do. However, c is not square-free. We must first substitute $z' := 2z$ and solve

$$3x^2 + 5y^2 - (z')^2 = 0.$$

We have gotten a new coefficient $c' = -1$. We see that

$$\gcd(a, b) = \gcd(a, c') = \gcd(b, c') = 1.$$

The remaining step is to check the quadratic residue condition. It is obvious that any integer is a quadratic residue modulo $c' = -1$, so

$$-ab = -15 \equiv 0^2 \pmod{-1}$$

holds. Next in the line are $-bc = 5$ and $a = 3$. We are trying to find an integer $k \in \mathbb{Z}$ such that

$$5 \equiv k^2 \pmod{3}.$$

Since $5 \equiv 2 \pmod 3$ and

$$0^2 \equiv 0, \quad 1^2 \equiv 2^2 \equiv 1 \pmod 3,$$

we see that this congruence has no solutions. According to **Legendre's theorem**, there are no rational solutions to (1.4.1) and thus, there are no solutions to our original equation, either. ⊠

Problem 1.4.2. Find all the rational solutions to

$$y^2 + 3xy + 2x - 3y - 1 = 0. \tag{1.4.2}$$

Solution. We first introduce the term x^2 into the equation by setting $y \coloneqq y + x$. We get

$$4x^2 + y^2 + 5xy - x - 3y - 1 = 0.$$

Next, we homogenize and obtain

$$4x^2 + y^2 + 5xy - xz - 3yz - z^2 = 0.$$

In accordance with (1.2.5), we have

$$a = 4,\ b = 1,\ c = 5,\ d = -1,\ e = -3,\ f = -1.$$

We substitute

$$\begin{aligned} x &= x + \frac{5}{8}y - \frac{1}{8}z, \\ y &= y + \frac{19}{9}z. \end{aligned}$$

We determine the corresponding coefficients

$$a = 4, \quad b = -\frac{9}{16}, \quad c = \frac{13}{9}.$$

We shall transform the equation

$$4x^2 - \frac{9}{16}y^2 + \frac{13}{9}z^2$$

to get a, b, c integral, pairwise coprime and square-free. Multiplying by a common denominator $9 \cdot 16$ gives

$$576x^2 - 81y^2 + 208z^2 = 0.$$

Obviously (we multiplied the equation by 9 and 16), none of $576, 81, 208$ is square-free. Hence, we introduce another substitution

$$x \coloneqq 24x, \quad y \coloneqq 9y, \quad z \coloneqq 4z$$

and end up with

$$x^2 - y^2 + 13z^2 = 0.$$

We could now apply **Legendre's theorem** and check for the existence of rational solutions. However, since our equation looks somewhat easy this time around, we are first going to try some random guessing, for good measure.

Remark. You might have noticed that **Legendre's theorem** gives us no clue about the value of rational solutions to (1.2.6). So, even if we know that a solution exists, guessing is the only option available without further developing the theory of rational points on conics and searching for adequate algorithms.

We first let $z \coloneqq 1$ and try to guess a rational solution to

$$x^2 = y^2 - 13.$$

It is quite evident that $x = 6, y = 7$ is one possible solution. To find the corresponding solution to our original equation (1.4.2), we have to follow the chain of substitutions in reverse.

Doing the calculations, in the background this time, we reach the solution

$$x = \frac{1}{2}, \quad y = \frac{3}{2}.$$

Alas, we are not done yet. Our goal was to find *all* rational solutions to (1.4.2). We are going to use our technique of projecting onto a rational line. Since we already have a rational point $P \coloneqq (1/2, 3/2)$, the best choice would be to take a line parallel to the tangent line at P. That way, every point, save P, of the conic has its projection.

We let f denote the polynomial from (1.4.2). The tangent line at P is given by

$$f_x(P)\left(x - \frac{1}{2}\right) + f_y(P)\left(y - \frac{3}{2}\right) = \frac{13}{2}x + \frac{3}{2}y - \frac{11}{2} = 0.$$

We can choose any rational line parallel to the tangent one at P but let us preferably choose one that crosses not the conic at any point. That way, we can avoid special cases. The direction is given, let

$$13x + 3y + q = 0$$

for $q \in \mathbb{Q}$ be our line. We want the equation

$$13x + 3y + q = y^2 + 3xy + 2x - 3y - 1$$

to have no real solutions. If we view it as a quadratic equation in y, its roots are

$$y = -\frac{3x}{2} \pm \frac{\sqrt{4q + 9x^2 + 8x + 40}}{2} + 3.$$

Hence, we need

$$4q + 9x^2 + 8x + 40$$

to be always negative. Solving this as a quadratic equation in x yields

$$x = \pm\frac{2\sqrt{-9q - 86}}{9} - \frac{4}{9}.$$

Thus, for example, the choice $q = 0$ gives no real solutions for x and it can be easily checked that the function

$$x \mapsto 9x^2 + 8x + 40$$

if negative for every $x \in \mathbb{R}$. We have obtained our projection line

$$L : 13x + 3y = 0.$$

Every rational point on L is of the form $(q, -13q/3)$, $q \in \mathbb{Q}$. The line connecting $Q \coloneqq (q, -13q/3)$ and P is expressed as

$$L_{PQ} : (6q - 3)y + (26q + 9)x - 22q = 0.$$

And finally, its second intersection with the given conic is obtained from the quadratic equation

$$(8q + 18)y^2 - (24q + 21)y + 18q - 9 = 0.$$

Its solutions are

$$y_1 = \frac{3}{2}, \quad y_2 = \frac{6q - 3}{4q + 9}.$$

The solution y_1 corresponds to the point P and the solution y_2 corresponds to the second rational point on the conic with coordinates

$$x = \frac{52q^2 + 234q - 9}{104q^2 + 270q + 81}, \quad y = \frac{6q - 3}{4q + 9}.$$

There, we have found all the existent rational solutions to (1.4.2). With that we close the curtain on the problem and on the chapter. ⊠

2. Elliptic Curves

This chapter we shall dedicate to the basic theory of cubic curves. We will explain the concept of a singular point on an algebraic curve, the usefulness, almost necessity, of working with cubic curves in a simpler form and the construction of a group law on its set of rational points.

First and foremost, a rational algebraic curve (see **Definition 1.3.3**) with defining polynomial of degree three is called a *rational cubic curve*. We will often omit the modifier 'rational' and - to further promote laziness of expression - even the noun 'curve' and will simply call such algebraic curve, a *cubic*.

The explicit equation for a rational cubic taketh the form

$$ax^3 + by^3 + cx^2y + dy^2x + ex^2 + fy^2 + gxy + hx + iy + j = 0 \qquad (2.0.1)$$

for $a, \ldots, j \in \mathbb{Q}$.

The sole image of working with such a thing in absolute abstraction should send shivers down your spine. Just as we did with conics in the previous chapter, we have to find a curve defined by a simpler equation whose set of rational points corresponds to the set of rational points of (2.0.1). This kind of relation is called *birational equivalence*. We will occasionally use this term in later sections and chapters as well so we define it properly here. There is just one preparatory step.

Definition 2.0.1 (Rational mapping)**.** If C, C' are two curves, we call the map

$$\mu : C \to C'$$

rational if there exist $f, g \in \mathbb{Q}[x, y]$ such that $\mu(c) = f(c)/g(c)$ for all $c \in C$ where $g(c) \neq 0$.

Now comes the topping.

Definition 2.0.2 (Birational equivalence)**.** We call two curves C, C' birationally equivalent if there exist finite sets $N_\mu, N_\nu \subset C, M_\mu, M_\nu \subset C'$ and injective rational maps $\mu : C \setminus N_\mu \to C' \setminus M_\mu$, $\nu : C' \setminus M_\nu \to C \setminus N_\nu$ such that $\mu \circ \nu$ and $\nu \circ \mu$ are identities on $C \setminus (N_\mu \cup N_\nu)$ and $C' \setminus (M_\mu \cup M_\nu)$, respectively.

So, without all the gobbledygook, birational equivalence is a rational mapping that works well for almost all points on C and C'. Let us think of them as affine curves for a second. As an example, imagine the map $C \to C'$, $y \mapsto y/x$. It is clearly rational and, by our definition, C is birationally equivalent to C' since the points with their y-coordinate equal to zero (of which there are finitely many) do not get mapped to any point on C'. On the other hand, all the points on C' with their x-coordinate equal to 0 (again, finitely many) get mapped to one point, $(0, 0)$, on C.

Remark. Since we will often talk about the set of rational points on a curve, it would be a good idea to establish some notation. As it stands, for a given curve C, we denote $\mathcal{R}(C)$ the set of rational points of C.

Before we move on to play with (2.0.1) in order to make it just a little less frightening, we are obliged to note that there is, as of yet, no known algorithm to check whether a given cubic contains a rational point or not, nor do we have knowledge about the number of rational solutions to (2.0.1). There may be infinitely many and there may not. For further details, see Silverman and Tate [2015], chapter Introduction, p. 4 - 6.

It also behooves us to mention that the technique of projecting onto a rational line cannot work in the case of cubics. According to **Bézout's theorem**, a line meets a cubic in three points. Because of that, even if we *do* find a rational point on our cubic, the line connecting it with a rational point on another line generally crosses the cubic at two other points which are not necessarily rational, considering they are solutions to a quadratic equation. The intersection number plays a rôle here, more on that in the next section. Hence, in the general case, we could have a two-to-one correspondence at best, which is hardly satisfactory regarding solutions to an equation.

By way of these few paragraphs we ought to have already established the idea that cubics are not easy. That, however noble a deed in itself, does not satisfy us, though. We move on to the next section where we deal with the problem of singular points.

2.1 Singular Cubics

It is fair to first define what a singular point is before deciding we do not like them.

Definition 2.1.1. Given an irreducible polynomial $F \in \mathbb{Q}[x, y]$, we say that a point P is a *singular point* of the curve C_F if

$$F_x(P) = F_y(P) = 0.$$

A curve that has at least one singular point is also called *singular*.

An equivalent definition would be that P is a singular point if a tangent line to C_F at P does not exist.

Remark. We will briefly clarify why we need a tangent line at every (rational) point of our cubic. In **Section 2.3** we define a group law on $\mathcal{R}(C_F)$ by getting the third intersection (guaranteed by **Bézout's theorem**) of the curve with a line connecting two of its rational points. So, when we need (and we will) to 'double' a point, we must cross the cubic with a tangent line at the given point. Thus, for us to be able to define a group law on the entirety of $\mathcal{R}(C_F)$, a tangent line must exist at every rational point.

For the sake of further discussion, we need to confuse you, forgiving reader, a bit and fast forward in time to the next section. There we show in detail that every non-singular curve given by (2.0.1) is birationally equivalent to a curve of the form

$$y^2 = x^3 + ax + b, \tag{2.1.1}$$

for a, b rational.

We will now classify the *singular* cubic curves given by (2.1.1) and see that they are the one amongst few special cases of cubic curves for which we can express all the existent rational solutions in utter explicitness.

If we let $F(x, y) \coloneqq x^3 + ax + b - y^2$, we can take the partial derivatives of F to get

$$\begin{aligned} F_x(x, y) &= 3x^2 + a, \\ F_y(x, y) &= -2y. \end{aligned}$$

It follows that any singular point on C_F must take the shape $(x, 0)$ for $x \in \mathbb{R}$. We further let $f(x) \coloneqq F(x, 0)$ and note that $f'(x) = F_x(x, y)$. Hence, a singular point $(x, 0)$ on C_F satisfies $f'(x) = 0$. However, $(x, 0)$ also satisfies $f(x) = 0$ since it lies on C_F. This means that x is a double or triple root of f. Therein lies the heart of our characterization of singular cubics. More precisely, a cubic of the form

$$y^2 = f(x)$$

is singular if and only if f has at least a double root. Formally, we have only shown that when C_F is a singular point then f has a multiple root. However, the backward implication is easy to see. If f has a double root α, then $f(\alpha) = f'(\alpha) = 0$. Then we also have

$$y^2 = f(\alpha) = 0,$$

so the point corresponding to α is $(\alpha, 0)$. It follows that

$$F_x(\alpha, 0) = f'(\alpha) = 0 \quad \text{and} \quad F_y(\alpha, 0) = 0,$$

which in turn proves that $(\alpha, 0)$ is singular.

On our path to see exactly why the set of rational points of such cubics is expressible explicitly, we are to experience the utter joy of some additional calculations.

We easily compute that

$$f'(x) = 0 \iff x = \pm\sqrt{-\frac{a}{3}}. \tag{2.1.2}$$

To spare some space and to make the following expressions clearer, we shall assume that $x = \sqrt{-a/3}$. The other case demands the linear substitution $x = -x$ where appropriate. In order for $(x, 0)$ to lie on C_F, substituting back to $f(x) = 0$ tells us that the condition

$$b = \frac{2\sqrt{3}}{9}(-a)^{\frac{3}{2}}$$

must also be satisfied. By factoring out $\left(x - \sqrt{-a/3}\right)^2$ from f, we get

$$f(x) = \left(x - \sqrt{-\frac{a}{3}}\right)^2 \left(x + 2\sqrt{-\frac{a}{3}}\right). \tag{2.1.3}$$

We denote $r \coloneqq \sqrt{-a/3}$ and substitute $x' = x - r$ to obtain

$$f(x') = (x')^2(x' + 3r).$$

The mapping $x \mapsto x - \sqrt{-a/3}$ is obviously bijective, hence every singular cubic is given by

$$y^2 = x^2(x + 3r) \tag{2.1.4}$$

for $r \in \mathbb{R}$.

First of all, we will show that r must be rational. By expanding terms in (2.1.3), we see that

$$f(x) = (x - r)^2(x + 2r) = x^3 - 3r^2x + 2r^3.$$

Since f was assumed to be rational, we see that r^2 and r^3 must both be rational, too. Ergo, either $r = 0$ or $r = r^3/r^2$ is rational by the argument above. This further implies that $x - r \mapsto x$ is a rational mapping and by it the rational points on (2.1.3) transform to rational points on (2.1.4).

We will first study the special case $r = 0$. The polynomial $f(x) = x^3$ has a triple root $x = 0$ and thus the cubic $y^2 = x^3$ has only one singular point, $(0, 0)$. For any $q \in \mathbb{Q}$, we see that (q^2, q^3) is a rational solution to $y^2 = x^3$. It is evident that all rational solutions are of this form.

Now, if $r \neq 0$, we are free to dismiss the points $(0, y) \in \mathcal{R}(C_F)$. How so? Notice that the point $(0, 0)$ lies on (2.1.3) only if $r = 0$. As a result, only the cubics given by (2.1.1) of the already discussed form $y^2 = x^3$ have a singular point at $(0, 0)$.

We can thus make use of the rational mapping $y \mapsto yx$ (which is bijective since $x \neq 0$). Substituting to (2.1.4), we get

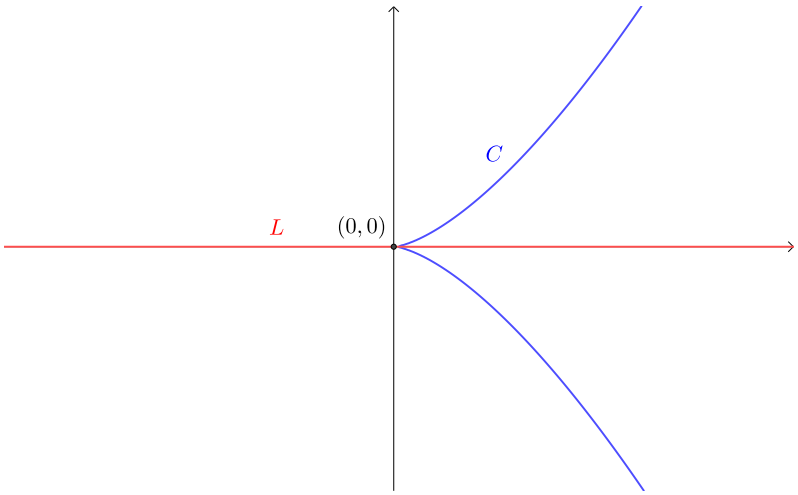
$$y^2 = x + 3r.$$

Since $r \in \mathbb{Q}$, $(q^2 - 3r, q(q^2 - 3r))$ are all the rational points on (2.1.4). Also, the mapping $x - r \mapsto x$ is rational, making every such point correspond to another rational point on our original cubic.

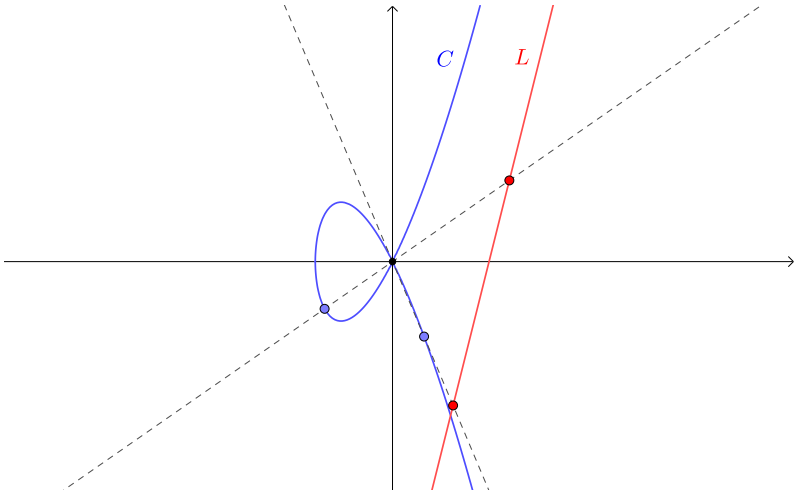
Remark. You might have noticed that rational points behave similarly on singular cubics as they do on conics. It is enough to have one rational point (the singular one) to find infinitely many more. The natural question arises. Could a singular cubic also be projected onto a line? Without partaking a glassful of rigorousness, the answer is yes. Once given a singular rational point on a cubic curve, we can project any other point on the curve onto a chosen line. This works because a line connecting the singular point and any other point on the cubic intersects the cubic *twice* in said singular point. The number of intersections remains three, as it must, but we still get a birational equivalence between a rational line and a singular cubic by means of such projection.

Now that we have hopefully convinced ourselves that singular cubics are little sisters to the non-singular ones, we move on to pay what we owe. That is, we proceed to show that every non-singular cubic is birationally equivalent to a cubic given by (2.1.1).

Before that, however, "Sound the fanfare!" as we finish the section with grace and finally, after more than a dozen pages of preparation, define the second main subject of the thesis.



(a) The curve $C : y^2 = x^3$ intersecting 'thrice' with $L : y = 0$.



(b) Projecting $C : y^2 = x^2(x + 4)$ onto $L : y = 4x - 15$.

Figure 2.1.1: Examples of singular cubics.

Definition 2.1.2 (Elliptic curve)**.** A non-singular rational algebraic curve defined by

$$y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{Q}$ is called *elliptic*.

2.2 Weierstrass's Normal Form

We start with a general rational cubic curve given by (2.0.1) and we assume we are given a rational point P on it. First of all, we will show that we can assume P to be non-singular. This does not mean that we assume the cubic itself to be non-singular, just yet. We simply assume that this particular rational point is not singular. We are about to prove two statements:

(1) Any line passing through a singular point intersects the curve at least twice

at that point.

(2) If the singular point is rational and the intersection is double, then the third intersection is also rational.

Before that, unfortunately, we need to somewhat formalize the multiplicity of intersection, at least in the case of a line intersecting a cubic. If C_L is given by

$$L(x, y) = kx + ly + m = 0$$

and $l \neq 0$, we can substitute $y' \coloneqq (-m - kx)/l$ and produce the equation

$$F(x, y') = 0$$

where F is the polynomial in (2.0.1). Thus, $F(x, y')$ is a polynomial in one variable which decomposes, by the fundamental theorem of algebra, into three linear polynomials over the field of complex numbers. Hence, for $P \in C_F \cap C_L$, we define the multiplicity of intersection of C_F with C_L at P as the multiplicity of the factor that vanishes at P (formally at the x-coordinate of P) in the decomposition of $F(x, y')$.

Now we can jump into proving our two statements from before. Again, we let F be the defining polynomial in (2.0.1).

Lemma 2.2.1 (Ad (1))**.** *Let P be a singular point on C_F. Then any line passing through P intersects C_F at least twice at P.*

Proof. We can assume $P = (0, 0)$, otherwise we translate C_F by means of the linear mapping $(x, y) \mapsto (x - p, y - q)$, supposing $P = (p, q)$.

The equality $F(0, 0) = 0$ implies that the constant term of F, j, is 0. $F_x(0, 0) = 0$ and $F_y(0, 0) = 0$ imply $h = 0$ and $i = 0$, respectively. Our cubic, thus, is none other than

$$ax^3 + by^3 + cx^2y + dxy^2 + ex^2 + fy^2 + gxy = 0. \tag{2.2.1}$$

If our line is given by

$$ux + vy + w = 0,$$

its passing through $(0, 0)$ forces $w = 0$. We surmise $v \neq 0$ since substituting $x = 0$ into (2.2.1) gives

$$by^3 + fy^2 = 0,$$

which has the obvious double solution $y = 0$. Then we have

$$y = -\frac{u}{v}x.$$

To maintain clarity of expression as much as possible, we let $u' \coloneqq -u/v$. Plugging the aforewritten equality into (2.2.1) produces

$$ax^3 + b(u')^3x^3 + cu'x^3 + d(u')^2x^3 + ex^2 + f(u')^2x^2 + gu'x^2 = 0.$$

Sharp eyes certainly unveil the possibility of factorization hidden deep inside this polynomial. Indeed, factoring out x^2, we get

$$x^2(ax + b(u')^3x + cu'x + d(u')^2x + e + f(u')^2 + gu') = 0.$$

This proves our lemma for this equation has the double solution $x = 0$. □

Remark. In a very similar fashion, it can be proven that any tangent line crosses the cubic twice at the point of tangency. If we assume, just as in the previous lemma, that $P = (0, 0)$ is a non-singular point on C_F, then the tangent line to P is given by

$$F_x(0,0)x + F_y(0,0)y = hx + iy = 0.$$

Because P is non-singular, either $h \neq 0$ or $i \neq 0$. Let us assume that $h \neq 0$. Since $F(0,0) = 0$, necessarily $j = 0$ in (2.0.1). Substituting $x := -iy/h$ gives

$$\begin{aligned} &- ai^3y^3 + bh^3y^3 + chi^2y^3 - dh^2iy^3 + ehi^2y^2 + fh^3y^2 - gh^2iy^2 \\ &= -y^2\left(ai^3y - bh^3y - chi^2y + dh^2iy - ehi^2 - fh^3 + gh^2i\right) = 0. \end{aligned}$$

Thus, the factor y^2 corresponding to P is of multiplicity two.

It awaits us to prove that if the intersection of C_L and C_F at P is only double, then the third intersection point is rational.

Lemma 2.2.2 (Ad (2))**.** *If P is a singular rational point on C_F and C_L is a rational line passing through P which intersects C_F twice at P, then the third intersection point is also rational.*

Proof. Again, we assume $P = (0, 0)$ and

$$\begin{aligned} F(x,y) &= ax^3 + by^3 + cx^2y + dxy^2 + ex^2 + fy^2 + gxy, \\ L(x,y) &= ux + vy. \end{aligned}$$

If $v = 0$, then, from the computations performed in the previous lemma, we get $x = 0$ and

$$y = 0 \quad \text{or} \quad y = -\frac{f}{b},$$

both obviously rational. Supposing $v \neq 0$ and setting $u' := -u/v$, we get $y = u'x$ and

$$x = 0 \quad \text{or} \quad x = -\frac{e + f(u')^2 + gu'}{a + b(u')^3 + cu' + d(u')^2}.$$

It is easy to see that $(x, u'x)$ is rational in both cases, which concludes the proof. □

Remark. What happens should the fractions defining the third intersection be undefined? Would we have no third intersection, then? No. Recall that we only work with the affine parts of C_F and C_L. If we instead take the projective curves C_{F^*} and C_{L^*}, then, by **Bézout's theorem**, if they do not intersect in the affine plane, they intersect at some point at infinity.

In the former case, $v = 0$, it would be the point

$$[0 : -f : b]$$

and in the latter we are looking at

$$[e + f(u')^2 + gu' : u'(e + f(u')^2 + gu') : a + b(u')^3 + cu' + d(u')^2].$$

One last useful fact to observe: if P a singular point on C_F, only a specific class of lines intersect C_F at P thrice. It is either the line $x = 0$ if $f = 0$ or the lines which satisfy

$$e + f(u')^2 + gu' = e + f\left(\frac{u}{v}\right)^2 - g\left(\frac{u}{v}\right) = 0.$$

Having solved this as a quadratic equation in u, we have obtained

$$u = \frac{g \pm \sqrt{-4ef + g^2}}{2f} v.$$

Most importantly for us, this means that if we want another rational point on C_F besides P, the singular one, we can simply choose a rational line which intersects C_F twice at P and take the third intersection, Q. Q is then non-singular either by calculations done in the proof of **Lemma 2.2.1** or by **Bézout's theorem**, due to which the intersection of C_L with C_F at Q must be simple.

Remark. Perceptive readers will have certainly noticed that we have just proven our vague remark about projecting singular cubics onto rational lines from the previous section. Our two lemmata prove that this can be done and even give a slight computational advantage to anybody brazen enough to attempt it.

With the problem of singular points out of the way, we can now proceed to the transformation of C_F into Weierstrass's[1] form.

Because we will be working with tangent lines in the projective plane for a while, we should formalize what a tangent line in the projective plane is and that a tangent line to an affine point in the projective plane corresponds to a tangent line at the same point (by means of $[x : y : 1] \mapsto (x, y)$) in the real plane.

If $P \coloneqq [p_1 : p_2 : p_3] \in C_{F^*}$ is a non-singular point, then the tangent line to C_{F^*} at P is given by (see Gathmann [2018], Chapter 3, **Proposition 3.25**)

$$F_x^*(P)x + F_y^*(P)y + F_z^*(P)z = 0. \tag{2.2.2}$$

If $p_3 = 0$, then this point is not affine. If, on the other hand, $p_3 \neq 0$, then it is by definition equal to $[p_1/p_3 : p_2/p_3 : 1]$. For brevity of expression, we assume that $P = [p_1 : p_2 : 1]$. In order to connect affine tangent lines to projective ones, we need to show that

$$F_x(p_1, p_2)(x - p_1) + F_y(p_1, p_2)(y - p_2) = F_x^*(P)p_1 + F_y^*(P)p_2 + F_z^*(P).$$

Fortunately, it holds and is easy to check with direct calculation that

$$F_x^*(P) = F_x(p_1, p_2) \quad \text{and} \quad F_y^*(P) = F_y(p_1, p_2).$$

From this and the fact that $F_x^*(P)p_1 + F_y^*(P)p_2 + F_z^*(P) = 0$, we get

$$F_z^*(P) = -p_1 F_x^*(P) - p_2 F_y^*(P) = -p_1 F_x(p_1, p_2) - p_2 F_y(p_1, p_2)$$

which begets the desired equality.

[1] Karl Theodor Wilhelm Weierstrass (1815 - 1897), German mathematician, often cited as 'the father of modern analysis'. Kleiner and Knöbl [2015]

So tangent lines work as expected in the projective plane.

There is one last caveat to take care of before we bend our curve unrecognizable. The multiplicity of intersection in the projective plane. This one is a little trickier but it can be shown that we can transfer our definition almost directly.

More precisely, if C_{F^*} is a projective rational cubic and C_{L^*} a rational projective line given by

$$L^*(x, y, z) = kx + ly + mz = 0$$

we can substitute $z \coloneqq (-kx - ly)/m$ into

$$F^*(x, y, z) = 0.$$

Just as before, if $m = 0$, we simply substitute a different variable. We obtain a homogeneous polynomial of degree three in two variables, x and y. By Fulton [2008], chapter Affine Varieties, **Corollary** to **Proposition 5**, this polynomial decomposes into three linear factors over $\mathbb{C}$. It can be shown that each of these factors corresponds to one point of intersection of C_{F^*} with C_{L^*}. We shall not do that here, but it can probably be found in any book properly defining intersection number, for example Fulton [2008], chapter Local Properties of Plane Curves, p. 36 - 40. For our purpose, it is satisfactory to know that a projective tangent line crosses a projective curve twice at the point of tangency, just as in the real plane.

Let, again, P be a non-singular rational point on C_F. We will now present a somewhat standard construction based chiefly on Silverman and Tate [2015], chapter Geometry and Arithmetic, p. 22 - 27. Details left out in the original text were added.

First of all, we homogenize our curve to work in the projective plane. Thus,

$$F^*(x, y, z) = ax^3+by^3+cx^2y+dxy^2+ex^2z+fy^2z+gxyz+hxz^2+iyz^2+jz^3. \quad (2.2.3)$$

We first take the tangent line to C_{F^*} at P. We define this to be the axis $z = 0$ in the new coordinate system. Formally speaking, if

$$ux + vy + wz = 0$$

is the tangent line at P, we use the mapping

$$[x : y : z] \mapsto [x : y : ux + vy + wz].$$

Remark. We can assume $w \neq 0$ here. Since at least one of u, v, w must be non-zero (P is non-singular), say $u \neq 0$, we could instead take $ux + vy + wz = 0$ to be the axis $x = 0$. As F^* is homogeneous, the entire transformation process is symmetrical with respect to any interchange of coordinate axes.

Next, we let Q be the intersection of $z = 0$ with the curve C_{F^*}. This intersection is necessarily simple since $z = 0$ (as the tangent line) passes twice through P. We let the tangent line to C_{F^*} at Q be the axis $x = 0$.

Remark. If the tangent line at P passes thrice through P, that is, P is an inflection point of C_{F^*}, we let $x = 0$ be any line that does not contain P.

Finally, for $y = 0$ we can choose any line passing through P, different from $z = 0$.

Due to our choices of axes, the point P is now $[1 : 0 : 0]$ in the new coordinate system, and $Q = [0 : 1 : 0]$. We will show that in these coordinates we have $a = b = c = 0$ in (2.2.3). Since F^* vanishes at P, we immediately get

$$F^*(P) = F^*(1, 0, 0) = a = 0.$$

Similarly, it follows from $F^*(Q) = 0$ that $b = 0$. Finally, the axis $z = 0$ intersects C_{F^*} twice at P and once at Q. Provided that the intersections are gained as the solutions to

$$F^*(x, y, 0) = 0,$$

plugging in $a = b = 0$, we obtain

$$cx^2y + dxy^2 = 0.$$

After factoring out the term xy, the equation becomes

$$xy(cx + dy) = 0.$$

Since P does not satisfy $x = 0$ and the intersection of $z = 0$ with C_{F^*} is double at P, we get that P must satisfy

$$y = 0 \quad \text{and} \quad cx + dy = 0.$$

It then follows from the second equality that $c = 0$. Our projective curve is thus

$$F^*(x, y, z) = dxy^2 + ex^2z + fy^2z + gxyz + hxz^2 + iyz^2 + jz^3 = 0,$$

where the coefficients $d, \ldots, j$ are generally different than they were before the projective transformation.

We now dehomogenize to work with the affine part of C_{F^*} again. We want to stay projective only as long as we must. Setting $z \coloneqq 1$ we return to

$$F(x, y) = F^*(x, y, 1) = dxy^2 + ex^2 + fy^2 + gxy + hx + iy + j.$$

We divide the equation by d, letting further

$$(e, \ldots, j) \coloneqq \left(\frac{e}{d}, \ldots, \frac{j}{d}\right), \tag{2.2.4}$$

which further transforms the equation into

$$xy^2 + ex^2 + fy^2 + gxy + hx + iy + j = 0.$$

We map $x \mapsto x - f$, which yields

$$xy^2 + (gx + i - fg)y = -ex^2 + (2ef - h)x + fh - ef^2 - j.$$

Although this equation does not look very simple yet, with the introduction of new coefficients, we get the much more transparent form

$$xy^2 + (px + q)y = rx^2 + sx + t,$$

where $p, \ldots, t \in \mathbb{Q}$ are the adequate substitutions. We are very much nearing the end of the thorny path. The last important step remaining is to multiply the equation by x, which gives

$$(xy)^2 + (px + q)xy = rx^3 + sx^2 + tx,$$

substitute $y \coloneqq yx$ and complete the square on the left side. We compute

$$y^2 + (px + q)y = (y + \frac{1}{2}(px + q))^2 - \frac{p^2}{4}x^2 - \frac{pq}{2}x - \frac{q^2}{4}.$$

Thus, through the substitution $y \coloneqq y+(1/2)(px+q)$ our equation finally becomes

$$y^2 = rx^3 + \left(s + \frac{p^2}{4}\right)x^2 + \left(t + \frac{pq}{2}\right)x + \frac{q^2}{4}.$$

Grouping the coefficients each under one (rather packed) letter, we can write

$$y^2 = rx^3 + sx^2 + tx + u. \tag{2.2.5}$$

We finish by two more, somewhat cosmetic, improvements. Firstly, we replace x by rx and y by r^2y to attain

$$r^4y^2 = r^4x^3 + sr^2x^2 + trx + u.$$

Further division by r^4 gives

$$y^2 = x^3 + \frac{s}{r^2}x^2 + \frac{t}{r^3}x + \frac{u}{r^4}.$$

Secondly and ultimately, we replace x by $x - s/3r^2$ which gets rid of the term x^2 and produces

$$y^2 = x^3 + \left(\frac{t}{r^3} - \frac{s^2}{3r^4}\right)x - \frac{st}{3r^5} + \frac{2s^3}{27r^6} + \frac{u}{r^4}.$$

Once again grouping the coefficients, we end up with our desired equation

$$y^2 = x^3 + ax + b,$$

which is typically called *Weierstrass's normal form.*

Remark. A keen eye has surely noticed that we didn't consider the case of $r = 0$ in equation (2.2.5) or $d = 0$ in substitution (2.2.4). These crimes have been committed with clear intent. Notice that in the former case, the equation

$$y^2 = sx^2 + tx + u$$

describes a conic. Hence, if $r = 0$, the curve C_F is birationally equivalent to a conic, thus singular. We've already discussed singular cubics given in Weierstrass's normal form in the previous section. As such, we can gracefully omit this case because singular cubics are of no use in furthering the theory. Case $d = 0$ leads to an analogous situation as xy^2 is the only term of degree 3 in the dehomogenized polynomial.

We tried to make it as clear as possible that all the transformations applied to reshape the original equation (2.0.1) into Weierstrass's normal form were rational. It should also be noted that had we not been given any rational point on the cubic, we could have carried out the transformation exactly as is with any real point. However, since cubics with no rational points are of no relevance to the purpose of this text, we could safely assume that a rational point had been given.

Remark. As far as any semblance of the original curve with its Weierstrass's form goes when plotted in the real plane, there is generally none. See **Figure 2.2.1** for an example of the 'picture deforming' effect the transformation entails.

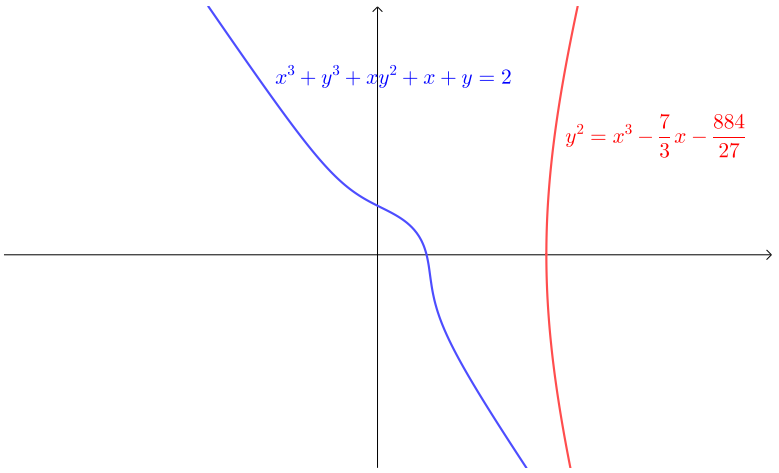


Figure 2.2.1: The curve $x^3 + y^3 + xy^2 + x + y = 2$ and its Weierstrass's form $y^2 = x^3 - (7/3)x - 884/27$.

We have shown that any cubic that cannot be put into Weierstrass's normal form through the procedure above is already birationally equivalent to a rational line. Also, since singular cubics are things of days bygone (more precisely, of **Section 2.1**), we see that the study of rational points on elliptic curves encompasses the study of rational points on all non-singular cubics.

Now, we put our algebraic cells, which have remained asleep for far too long, to work when we define a group law on the set of rational points of an elliptic curve, in the succeeding section.

2.3 Group Law on An Elliptic Curve

In this section we shall take a closer look at how a group law can be defined on the set of rational points of an elliptic curve that transforms it into an abelian group. The presented method is loosely based on Silverman and Tate [2015], chapter Geometry and Arithmetic, p. 15 - 22 and 28 - 32.

As always, we assume our elliptic curve C is given by the equation

$$y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{Q}$ and $x^3 + ax + b$ has no multiple root. The idea behind the definition is the following: given two rational points (which are not singular by

assumption) we can intersect the line that passes through them with C. This, by **Bézout's theorem**, produces a third intersection. We will view this procedure as a binary operation on $\mathcal{R}(C)$. So, given $P, Q \in \mathcal{R}(C)$, we denote $P * Q$ to be the third intersection of L_{PQ} with C. We have not formally proven that the third intersection lies in $\mathcal{R}(C)$. This fact, however, is quite trivial. But, just in case you do not take our word for it, we shall go out of our way to prove it.

The intersections of L_{PQ} with C are obtained by solving a cubic equation in one variable. If $q_1, q_2 \in \mathbb{Q}$ are two its rational solutions, we can factor them out to get an equation in the form

$$\alpha(x - q_1)(x - q_2)(x - r) = 0,$$

where $\alpha \in \mathbb{Q}$, $r \in \mathbb{R}$. To the term x^2, for example, belongs the coefficient $-\alpha(q_1 + q_2 + r)$ which is not rational when $r \notin \mathbb{Q}$. That cannot be for both L_{PQ} and C are given by equations with rational coefficients. So, we have that $r \in \mathbb{Q}$, as well. Hence, $P * Q \in \mathcal{R}(C)$ for any $P, Q \in \mathcal{R}(C)$.

Alas, $*$ is not the right candidate for our group law. It is obviously commutative but it can be shown that it is not associative. That is, in general

$$(P * Q) * R \neq P * (Q * R).$$

We hope you will forgive us this one time for not proving this fact rigorously and instead referring you to **Figure 2.3.1** wherefrom it can be easily inferred. As you will soon see, this section is quite heavy in terms of expression manipulation and we do like to savour our freedom while we can.

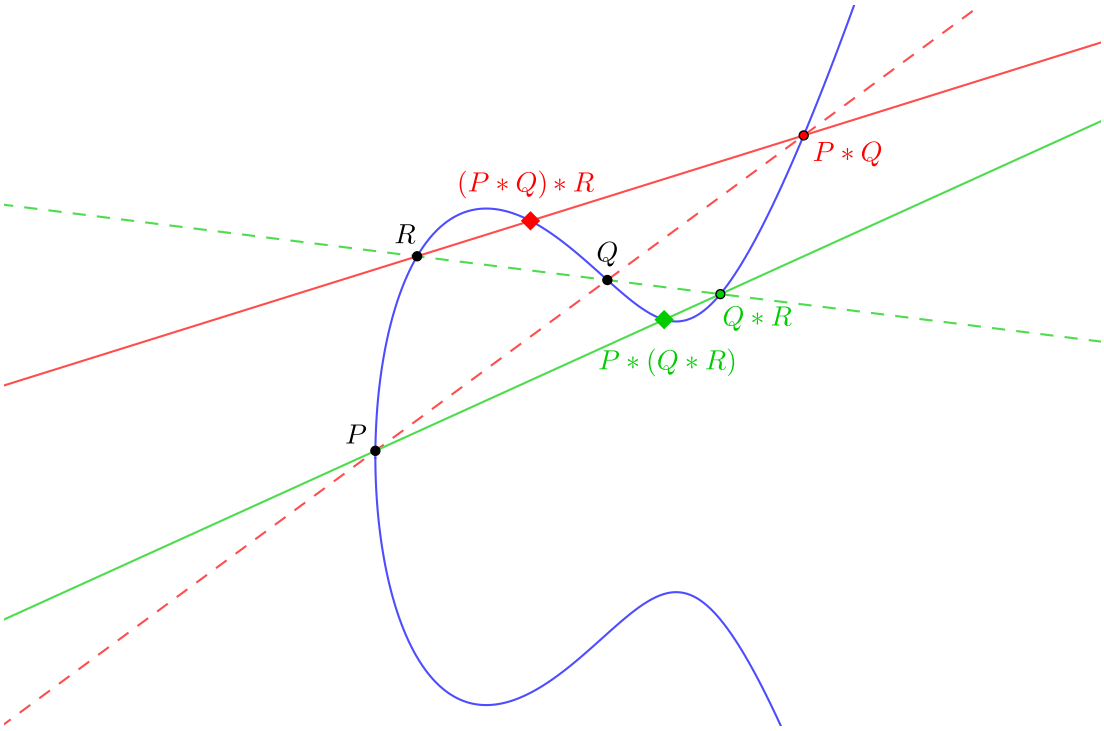


Figure 2.3.1: A 'proof' that $*$ is not associative.

Thankfully, we know how to get around the non-associativity of $*$. Let us fix an arbitrary rational point $\mathbf{0} \in \mathcal{R}(C)$. We will define a new binary operation

$+ : \mathcal{R}(C)^2 \to \mathcal{R}(C)$ by

$$P + Q = \mathbf{0} * (P * Q).$$

Expressed in a more transparent manner, given two rational points P and Q, we take the third intersection of L_{PQ} with C, $P * Q$, and then take the third intersection again, this time of $L_{\mathbf{0},P*Q}$ with C. We denote this point $P + Q$. If you, like we do, believe that visualization is a good method of grasping new ideas, check **Figure 2.3.2**.

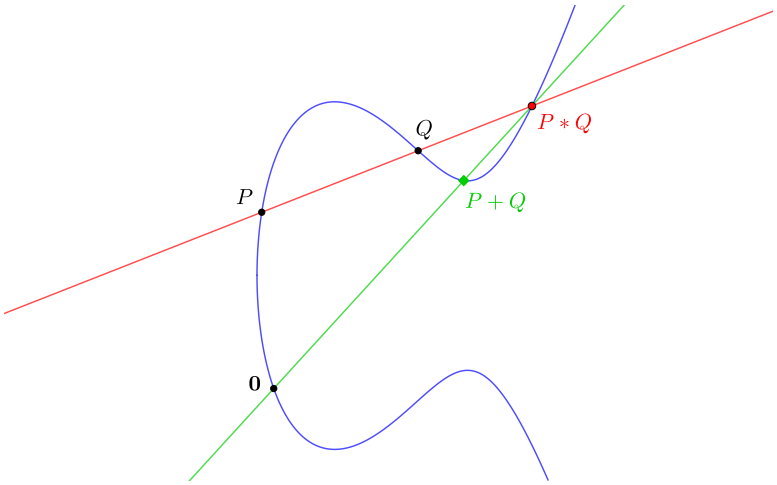


Figure 2.3.2: Illustration of the binary operation $+$.

Remark. You might wonder why we decided to label our arbitrary point $\mathbf{0}$. That is because it acts as the neutral element to operation $+$. We will prove this completely later in the section for a special choice of $\mathbf{0}$. Right now, we give you just a taste: the point $P + \mathbf{0}$ is defined as $\mathbf{0} * (P * \mathbf{0})$. We join the points P and $\mathbf{0}$ to get the point $P * \mathbf{0}$ on C. Then we join $P * \mathbf{0}$ with $\mathbf{0}$. But this line passes through P since that was how we defined $P * \mathbf{0}$ in the first place! Thus, $P = \mathbf{0} * (P * \mathbf{0}) = P + \mathbf{0}$.

Just as it was with $*$, it is obvious that $+$ is commutative. Indeed, for any choice of $P, Q \in \mathcal{R}(C)$, we have

$$P + Q = \mathbf{0} * (P * Q) = \mathbf{0} * (Q * P) = Q + P.$$

However, it is not nearly as easy to prove that $+$ is associative. We wish not to prove this fact for any choice of $\mathbf{0}$ but for a very special point on the curve which has, as you will hopefully soon acknowledge, numerous geometric and algebraic advantages.

Although our definition of $+$ seems to work just fine, it is heavily dependent on the location of $\mathbf{0}$ on the curve. Also, spare a thought to how numerically complicated it is to determine $P + Q$. Let us reiterate the method as series of steps to accomplish:

(1) For a given $P, Q \in \mathcal{R}(C)$ find L_{PQ}, the line passing through them.

(2) Determine $P * Q$, the third point of intersection of L_{PQ} with C.

(3) Calculate the equation of a line passing through $\mathbf{0}$ and $P * Q$.

(4) Determine $P + Q$, the third point of intersection of $L_{\mathbf{0},P*Q}$ with C.

Steps (1) and (2) are independent of $\mathbf{0}$ so there is no way to make them any easier by changing the coordinates of $\mathbf{0}$. However, for steps (3) and (4), there *is* a way. What if the line passing through $\mathbf{0}$ and $P*Q$ were vertical? Due to the symmetry of C, $P + Q$ would just be the reflection of $P * Q$ about the x-axis. This would allow us to get rid of steps (3) and (4) entirely! The last thing to ponder is to what choice of $\mathbf{0}$ could possibly accomplish that.

Recall that C is actually projective, so the easiest method to find the best of the best $\mathbf{0}$, is to take a point $P \in \mathcal{R}(C)$ and find the third intersection of $L_{PP'}$ (where P' is the reflection of P about the x-axis) and C. Such point clearly lies at infinity because if we substitute $x = c$ for some constant $c \in \mathbb{Q}$, that is, an equation of a vertical rational line, into (2.1.1), we get at most two solutions, namely

$$y = \pm\sqrt{c^3 + ac + b},$$

in the affine plane. Therefore, we need to homogenize C to find the third solution. Since C is defined by

$$y^2 = x^3 + ax + b,$$

homogenization gives

$$y^2 z = x^3 + axz^2 + bz^3.$$

The points at infinity are defined as the intersections with $z = 0$. Substitution yields

$$0 = x^3.$$

We see that the line $z = 0$ intersects C thrice at the point $[0 : 1 : 0]$ and thus C has only one point at infinity. We ought to ascertain that this point is truly the intersection of C with any vertical line. A homogenized vertical line looks like

$$x = cz,$$

for $c \in \mathbb{Q}$. It is clear that $x = z = 0$ satisfies this equation. So, we have unearthed our savior of computational power, the point $[0 : 1 : 0]$, which we denote $\mathbf{0}$ and henceforth consider the neutral element with respect to $+$.

With a partially informal introduction to the concept of group law on $\mathcal{R}(C)$, we now proceed to formalize it. We are going to find explicit formulae for the sum of two points and consequently prove that $+$ is indeed associative.

Firstly, we should prove that for every $P = (p_1, p_2) \in \mathcal{R}(C)$, the equality

$$\mathbf{0} * P = (p_1, -p_2)$$

holds. The vertical line passing through P is $x = p_1$. Substituting into (2.1.1) yields

$$y = \pm\sqrt{p_1^3 + ap_1 + b}.$$

However, we know that one of these solutions is equal to p_2. It follows immediately that the other must be equal to $-p_2$. It is also somewhat apparent that if we let $-P = (p_1, -p_2)$, then $P + (-P) = \mathbf{0}$. Indeed, we can write

$$P + (-P) = \mathbf{0} * (P * (-P)) = \mathbf{0} * \mathbf{0} = \mathbf{0}.$$

The second equality holds because $L_{P,-P}$ is a vertical line which intersects C at P, $-P$ and $\mathbf{0}$. The final equality uses the fact that the intersection of $z = 0$ with C is triple. This suggests that the third intersection of $L_{\mathbf{0},\mathbf{0}}$, which is exactly the line $z = 0$, with C is $\mathbf{0}$ again. Now that we have a formula for the inverse of a point, we move on to find one for the sum of points.

Let $Q = (q_1, q_2) \in \mathcal{R}(C)$ be another rational point on C. A simple calculation tells us that the equation of L_{PQ} is

$$y = \frac{p_2 - q_2}{p_1 - q_1}x + \frac{p_1 q_2 - p_2 q_1}{p_1 - q_1}.$$

If $p_1 = q_1$, then due to symmetry, either $Q = P$ or $Q = -P$. In the former case, $P + Q = 2P$ and doubling a point unfortunately requires an exclusive formula which we will deduce later. The latter case implies $P + Q = \mathbf{0}$ which has already been thoroughly discussed. Hence, temporarily, we assume $p_1 \neq q_1$. In order for the expressions to remain readable, we let

$$u \coloneqq \frac{p_2 - q_2}{p_1 - q_1}, \quad v \coloneqq \frac{p_1 q_2 - p_2 q_1}{p_1 - q_1}.$$

Substituting into (2.1.1) produces

$$(ux + v)^2 = x^3 + ax + b.$$

Grouping coefficients we obtain

$$x^3 - u^2 x^2 + (a - 2uv)x + (b - v^2) = 0.$$

Two of the roots of this cubic equation are p_1 and q_1. If we denote the third root r_1, we know thanks to Viète's[2] formulae that the coefficients of the polynomial satisfy

$$p_1 + q_1 + r_1 = u^2.$$

As a consequence, we get

$$r_1 = u^2 - p_1 - q_1, \quad r_2 = ur_1 + v,$$

where $R = (r_1, r_2) = P * Q$. Thus, $P + Q = (r_1, -r_2)$. The last thing remaining is the formula for $2P$. To get $P * P$, we need to find the line that intersects the curve twice at P, in other words, the tangent line to C at P. We denote

$$F(x, y) = x^3 + ax + b - y^2$$

and calculate

$$F_x(P)(x - p_1) + F_y(P)(y - p_2) = (a + 3p_1^2)(x - p_1) - 2p_2(y - p_2) = 0.$$

Expanding the right side, we obtain

$$y = \frac{a + 3p_1^2}{2p_2}x + \frac{2p_2^2 - 3p_1^3 - ap_1}{2p_2}.$$

[2]François Viète (1540 - 1603), French mathematician and astronomer. O'Connor and Robertson [2000]

For now, let us suppose $p_2 \neq 0$; we will deal with this special case shortly.

If we substitute

$$u := \frac{a + 3p_1^2}{2p_2}, \quad v := \frac{2p_2^2 - 3p_1^3 - ap_1}{2p_2},$$

we can once again use Viète's relations and get

$$r_1 = u^2 - 2p_1, \quad r_2 = ur_1 + v,$$

where $R = (r_1, r_2) = P * P$. Then, again, $2P = -R$. Finally, if $p_2 = 0$, we get the tangent line

$$x = p_1.$$

However, this is a vertical line so the other point of intersection of this line with C is $\mathbf{0}$. This means that if $P = (p_1, 0)$, then $2P = \mathbf{0}$. In terms of group theory, P is an element of order 2 in $(\mathcal{R}(C), +, \mathbf{0})$ (we have not yet proven that $(\mathcal{R}(C), +, \mathbf{0})$ is a group but we soon shall). We are going to dedicate the entirety of the succeeding chapter to points of finite order in $\mathcal{R}(C)$ and see that points $(p_1, 0)$ truly hold a special place on our curve.

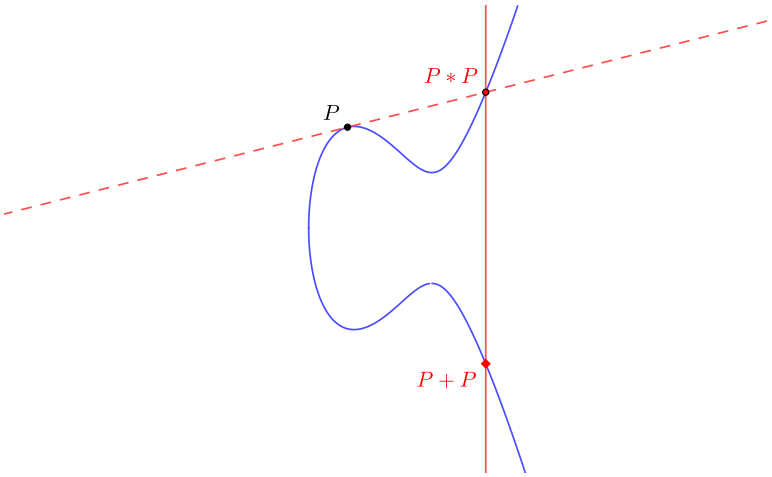


Figure 2.3.3: Doubling the point P.

With the explicit formula for the sum of any two points from $\mathcal{R}(C)$ at our disposal, we set off on the journey of proving that $+$ is associative. Let us formulate it as a claim since we have not had one for a while.

Claim 2.3.1. *The equality*

$$P + (Q + R) = (P + Q) + R$$

holds for all $P, Q, R \in \mathcal{R}(C)$.

Proof. If any of P, Q, R equal $\mathbf{0}$, then the equality holds trivially. We will assume that all the points are non-zero. We will calculate the left side first and for now surmise that we are not doubling a point anywhere. More specifically, we assume

$$Q \neq R \quad \text{and} \quad P \neq Q + R.$$

We should note, that if $Q + R = \mathbf{0}$, or symetrically $P + Q = \mathbf{0}$, associativity is quite straightforward to prove. Let's suppose $Q + R = \mathbf{0}$ or $Q = -R$. Then, we are to show that

$$P = (P + Q) + (-Q).$$

We'll use the symmetry of our curve with respect to the x-axis to that end. The third intersection of the line L_{PQ} passing through P and Q with C is defined to be $P * Q$. We denote this point S. Since $P + Q$ is the reflection of S over the x-axis and $-Q$ is the reflection of Q, it is clear that $L_{P+Q,-Q}$, the line passing through $P + Q$ and $-Q$ is the reflection of $L_{SQ} = L_{PQ}$. But, then, the third intersection of $L_{P+Q,-Q}$ with C is necessarily the reflection of P, the point $-P$. In symbols, $(P + Q) * (-Q) = -P$, which immediately implies $(P + Q) + (-Q) = P$. So, if $Q + R = \mathbf{0}$ or $P + Q = \mathbf{0}$, we have no problems.

In the other case, using our hard-earned formula, we get

$$Q + R = (u^2 - q_1 - r_1, -u(u^2 - q_1 - r_1) - v),$$

where u, v are defined as

$$u = \frac{q_2 - r_2}{q_1 - r_1}, \quad v = \frac{q_1 r_2 - q_2 r_1}{q_1 - r_1}.$$

We denote $S \coloneqq (s_1, s_2) = Q + R$ and write

$$P + S = ((u')^2 - p_1 - s_1, -u'((u')^2 - p_1 - s_1) - v'),$$

where

$$u' \coloneqq \frac{p_2 - s_2}{p_1 - s_1}, \quad v' \coloneqq \frac{p_1 s_2 - p_2 s_1}{p_1 - s_1}.$$

We will denote $x(P)$, $y(P)$ the first and second coordinate of P, respectively. After much simplification and substitutions $w_1 \coloneqq q_1 - r_1$, $w_2 \coloneqq q_2 - r_2$, we get

$$x(P+S) = -p_1 - w_1 - \left(\frac{w_2}{w_1}\right)^2 + \left(\frac{p_2 w_1^3 + (q_1 q_2 - 2q_1 r_2 + 2q_2 r_1 - r_1 r_2) w_1^2 - w_2^3}{w_1^2((p_1 + q_1 + r_1) w_1^2 - w_2^2)}\right)^2.$$

In a similar fashion, if we assume

$$P \neq Q, \quad P + Q \neq R,$$

we can write

$$P + Q = (u^2 - p_1 - q_1, -u(u^2 - p_1 - q_1) - v),$$

denote $T \coloneqq P + Q$ and

$$T + R = ((u')^2 - t_1 - r_1, -u'((u')^2 - t_1 - r_1) - v')$$

for the appropriate choices of u, v, u', v'. Simplifying yields

$$x(T+R) = -p_1 - w_1 - \left(\frac{w_2}{w_1}\right)^2 + \left(\frac{p_2 w_1^3 + (q_1 q_2 - 2q_1 r_2 + 2q_2 r_1 - r_1 r_2) w_1^2 - w_2^3}{w_1^2((p_1 + q_1 + r_1) w_1^2 - w_2^2)}\right)^2,$$

which is exactly the same expression as $x(P+S)$. Since $P+S$ and $T+R$ have the same first coordinate, they can be either the same or opposites of each other. If they are the same, we are finished with this case. Let us suppose that

$$T+R=-(P+S).$$

Then, however, we have

$$(P+S)+(T+R)=(P+(Q+R))+((P+Q)+R)=\mathbf{0}.$$

The points P,Q,R, for which this equality holds would only have to comply by the assumptions made at the start of the proof. To elaborate, since we have already checked that the x-coordinates of $(P+Q)+R$ and $P+(Q+R)$ match for a nearly arbitrary choice of P,Q and R, the y-coordinates of these points are either equal or opposite. Since we're trying to prove the former case holds for all points, we surmise the latter and using the fact we can choose P,Q and R nearly as we wish, we let $P\coloneqq R$. Thanks to the commutativity of $+$, we obtain

$$(R+(Q+R))+((R+Q)+R)=((R+Q)+R)+((R+Q)+R)=2((R+Q)+R).$$

We further let $R\coloneqq -Q$, which gives

$$2((R+Q)+R)=2((-Q+Q)+(-Q))=2(\mathbf{0}+(-Q))=2(-Q).$$

It is obvious that $2(-Q)=\mathbf{0}$ does not hold for every $Q\in\mathcal{R}(C)$. In order for the proof to be complete, we'd have to specifically consider the case $2(-Q)=\mathbf{0}$. However, to spare both time and space, we borrow a result from the following chapter, namely **Lemma 3.1.1**, the proof whereof does not depend on the formula for the sum of points at all. It says that there are at most three points Q satisfying $2Q=\mathbf{0}$. Thus, this case can be checked manually with relative ease and we'll omit it here.

Tracing back, we get that our original supposition was wrong as well and we thus have

$$T+R=P+S.$$

Next, we deal with the case of a double point. If $P=Q=R$ then the equality apparently holds. Due to the symmetry of the equality, all cases of a double point can be gotten from only two, for example, $P=Q$ and $P=Q+R$. Indeed, if we suppose $P=Q$, we attain

$$P+(P+R)=2P+R.$$

With a simple swap of letters, thanks to the commutativity of $+$, this can be written as

$$P+2Q=(P+Q)+Q,$$

which is the same equality we would have obtained had we substituted $R=Q$ into the original expression. Similarly, the case $R=P+Q$ is clearly the same as $P=Q+R$, if one swaps P and R. As it stands, we only need to have studied two cases to have proven all of them.

Nevertheless, the task of proving the equality for a double point will be delegated to you, kind and hard-working reader. The proof has already gotten fairly long and this other case comprises exactly the same machinery we have witnessed so far. No new insights are gained, only a different formula used. □

With this we finish our definition of the group law on $\mathcal{R}(C)$. Henceforth, we will always mean the group $(\mathcal{R}(C), +, \mathbf{0})$ when writing $\mathcal{R}(C)$. Should you still found the number of complicated expressions in this section unsatisfactory, worry not, as we tread ahead to the section of examples and problems where long and senseless computations are ubiquitous.

2.4 Examples and Problems

Problem 2.4.1. Determine all rational singular points of the cubic

$$F(x, y) = 2x^3 + y^3 + 4x^2 - 4xy - 6x - 8y + 16 = 0.$$

Solution. We start by calculating the partial derivatives of F. Doing the computations, one gets

$$\begin{aligned} F_x(x, y) &= 6x^2 + 8x - 4y - 6, \\ F_y(x, y) &= 3y^2 - 4x - 8. \end{aligned}$$

We have to solve the system $F_x(x, y) = F_y(x, y) = 0$. Solving $F_y(x, y) = 0$ as a linear equation in x, we get

$$x = \frac{3}{4}y^2 - 2.$$

Substituting into $F_x(x, y) = 0$, we meet the wandering beauty

$$\frac{27}{8}y^4 - 12y^2 - 4y + 2 = 0.$$

Despite knowing how to solve quartic equations, engaging with one would be far too lengthy. Instead, we pretend we did not know the solution beforehand and make a lucky guess, namely $y = 2$ seems to be one solution. Factoring out the corresponding linear term, we get

$$(y - 2)\left(\frac{27}{8}y^3 + \frac{27}{4}y^2 + \frac{3}{2}y - 1\right) = 0.$$

We are still left with a cubic equation, though. Multiplying by a common denominator, we will attempt to solve

$$27y^3 + 54y^2 + 12y - 8 = 0.$$

It comes to mind that there is one particular lemma we stated but have never actually utilized in practice. Yes, we are talking about **Gauss's lemma**. Since we, naturally, have a strong feeling that there is at least one more rational solution to our equation, we shall try to search for them. By **Gauss's lemma**, if p/q is a root of a polynomial f, then $q \mid \ell(f)$ and $p \mid c(f)$. The only divisors of 8 are 1,2,4 and 8 and the divisors of 27 are 1,3,9 and 27, but we must also count negative numbers. After a while of trying out different combinations (whereof there are 32 if we are not mistaken), we hit on the solution $y = -2/3$. One more factoring then gives

$$(y - 2)\left(y + \frac{2}{3}\right)\left(\frac{27}{8}y^2 + \frac{9}{2} - \frac{3}{2}\right) = 0.$$

By taking the discriminant

$$\Delta = \frac{81}{2}$$

of the remaining quadratic term, we see that $y = 2$ and $y = -2/3$ are the only rational solutions. The corresponding solutions for x are $x = 1$ and $x = -5/3$. Thus, $(1, 2)$ and $(-5/3, -2/3)$ are our two candidates for rational singular points. By plugging these into our original equation, we see that

$$\begin{aligned} F(1, 2) &= 0, \\ F(-5/3, 2/3) &= \frac{256}{9} \neq 0. \end{aligned}$$

Hence, only $(1, 2)$ lies on the cubic and is indeed a rational singular point.

Remark. Recall that we claimed that every singular point on a cubic curve has its second coordinate equal to zero. This is, however, only true for cubics in Weierstrass's form, which C_F is most certainly not. If we had put C_F into Weierstrass's form using the method described in **Section 2.2**, we would have mapped $(1, 2)$ to a point $(p, 0)$ for some $p \in \mathbb{Q}$. We will leave the calculations to you, should you wish to compute p explicitly.

It might seem that we are done but we are not. Our cubic, C_F, is projective. That means it could potentially have a singular point at infinity. We did not need to bother checking that for cubics in Weierstrass's form because they only have one point at infinity whereat there is the tangent line, $z = 0$.

We must further homogenize F to get the equation

$$F^*(x, y, z) = 2x^3 + y^3 + 4x^2z - 4xyz - 6xz^2 - 8yz^2 + 16z^3 = 0.$$

We now calculate the partial derivatives with respect to all *three* variables:

$$\begin{aligned} F^*_x(x, y, z) &= 6x^2 + 8xz - 4yz - 6z^2, \\ F^*_y(x, y, z) &= -4xz + 3y^2 - 8z^2, \\ F^*_z(x, y, z) &= 4x^2 - 4xy - 12xz - 16yz + 48z^2. \end{aligned}$$

Since we are only looking for points at infinity, we set $z = 0$ and get

$$\begin{aligned} F^*_x(x, y, 0) &= 6x^2, \\ F^*_y(x, y, 0) &= 3y^2, \\ F^*_z(x, y, 0) &= 4x^2 - 4xy. \end{aligned}$$

It is obvious that the only point where all partial derivatives vanish is $[0 : 0 : 0]$. However, this point does not lie in $\mathbb{P}(\mathbb{R}^2)$ by definition. In the end, we still have only one rational singular point, $(1, 2)$. ⊠

Problem 2.4.2. Transform the cubic curve

$$F(x, y) = x^3 + y^3 + xy^2 + x + y - 2 = 0$$

into Weierstrass's normal form given the rational point $P = (1, 0)$.

Solution. We will follow the series of steps described in **Section 2.2**. We first homogenize F to get

$$F^*(x, y, z) = x^3 + y^3 + xy^2 + xz^2 + yz^2 - 2z^3 = 0.$$

We calculate the tangent line at $P = [1 : 0 : 1]$ defined by

$$F_x^*(P)(x-1) + F_y^*(P)y + F_z^*(P)(z-1) = 4x + y - 4z = 0. \tag{2.4.1}$$

This calculation also confirms that P is not singular. We find the intersection of C_{F^*} with $4x + y - 4z = 0$. After substituting $y \coloneqq 4(z - x)$ and expanding terms, we arrive at

$$-47x^3 + 160x^2z - 179xz^2 + 66z^3 = 0.$$

We know the tangent line at P intersects C_{F^*} twice at P and once in a rational point Q. Ergo, we can factor out $(x - z)^2$ corresponding to the intersection at P. Through a little exercise in polynomial division we acquire

$$(x - z)^2(-47x + 66z) = 0.$$

Substituting $z \coloneqq 1$ and $x \coloneqq 66/47$ back into (2.4.1) yields

$$y = -\frac{76}{47}.$$

Hence, $Q = [66 : -76 : 47]$. We calculate the tangent line at Q:

$$21053x + 9505y - 14194z = 0.$$

Thus, we map $x \mapsto 21053x + 9505y - 14194z$. Finally, for the line $y = 0$ we choose any line passing through P different from $4x + y - 4z = 0$, for example, $x + y - z = 0$. The last mapping is then $y \mapsto x + y - z$. In order to transform our curve, we need to find the inverse mapping. This is most easily done through matrix notation. Our mapping is

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} 21053 & 9505 & -14194 \\ 1 & 1 & -1 \\ 4 & 1 & -4 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

If we strain ourselves (or our computers in this case), we compute the inverse mapping to be

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \frac{1}{6859} & -\frac{22}{19} & -\frac{1563}{6859} \\ 0 & \frac{4}{3} & -\frac{1}{3} \\ \frac{1}{6859} & -\frac{47}{57} & -\frac{11548}{20577} \end{pmatrix} \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}.$$

Substituting back to $F^*(x, y, z) = 0$ yields an equation of the form

$$F^*(x, y, z) = xy^2 + ax^2z + bxyz + cy^2z + dxz^2 + eyz^2 + fz^3 = 0,$$

where $a, \ldots, g \in \mathbb{Q}$ are very long fractions. We dehomogenize and get

$$F(x, y) = xy^2 + ax^2 + bxy + cy^2 + dx + ey + f = 0.$$

With a further change of variables which copies the steps described in **Section 2.2** exactly, we end up with

$$y^2 = x^3 - x^2 - 2x - 32 = 0.$$

One last substitution $x = x + 1/3$ yields

$$y^2 = x^3 - \frac{7}{3}x - \frac{884}{27},$$

which is the desired form. ⊠

Example 2.4.1 (Borrowed from Silverman and Tate [2015], chapter Geometry and Arithmetic, Exercise 1.18)**.** On the cubic curve

$$y^2 = x^3 + 17$$

lie the rational points

$$P_1 = (-2, 3),\ P_2 = (-1, 4),\ P_3 = (2, 5),\ P_4 = (4, 9),\ P_5 = (8, 23).$$

Each one of P_2, P_4 and P_5 can be expressed as $mP_1 + nP_3$ for an appropriate choice of $m, n \in \mathbb{Z}$.

Proof. In order to calculate mP_1, we first need to double the point. We have our doubling formula

$$2P = (u^2 - 2p_1, -u(u^2 - 2p_1) - v)$$

where $P = (p_1, p_2)$ and

$$u = \frac{a + 3p_1^2}{2p_2}, \quad v = \frac{2p_2^2 - 3p_1^3 - ap_1}{2p_2}.$$

Plugging in $a = 0, p_1 = -2, p_2 = 3$, we get

$$u = 2 \quad \text{and} \quad v = 7.$$

And consequently

$$2P_1 = (8, -23) = -P_5,$$

so we have already found one relation, $P_5 = -2P_1$. If we now make use of the new relation and compute the sum of P_3 and P_5, we get

$$P_3 + P_5 = (u^2 - x(P_3) - x(P_5), -u(u^2 - x(P_3) - x(P_5)) - v)$$

where

$$u = \frac{y(P_3) - y(P_5)}{x(P_3) - x(P_5)} \quad \text{and} \quad v = \frac{x(P_3)y(P_5) - y(P_3)x(P_5)}{x(P_3) - x(P_5)}.$$

Substituting the adequate values, we obtain $u = 3$, $v = 1$ and thus

$$P_3 + P_5 = (-1, 4) = P_2.$$

We have just discovered the second relation:

$$P_2 = P_5 + P_3 = -2P_1 + P_3.$$

It remains to express P_4 as $mP_1 + nP_3$. After a while of toying with the sum formula, we have obtained

$$P_1 - P_3 = (4, 9) = P_4.$$

With this relation, we have expressed all the points P_2, P_4, P_5 as linear combinations of P_1 and P_3, which concludes the proof. □

3. The Nagell-Lutz Theorem

You might have noticed that we did not make too much progress on Diophantine equations in the last chapter. True, we did demonstrate that rational solutions to any cubic equation correspond to the rational points on a curve in Weierstrass's form but we did not get any closer to the number or nature thereof. This chapter's main aim is to give some insight into exactly that.

Most of the content of this chapter is adopted from Silverman and Tate [2015], chapter Points of Finite Order. Although the exposition of facts was largely restructured, the ideas behind many, albeit not all, concepts and proofs belong there.

In the previous chapter we hit upon the points of order two in $\mathcal{R}(C)$, specifically the points with their second coordinate equal to zero. This was not a coincidence. In fact, all points of order two lie on the x-axis. There exist a precisely defined criteria which the points of finite order in $\mathcal{R}(C)$ satisfy. Their formulation is the subject of Nagell-Lutz[1] theorem and the proof of their correctness, the essence of this chapter. We will not leave you in the dark for long, as we state the theorem right here, to give you a precise idea what we shall be working on.

Theorem 3.0.1 (Nagell-Lutz)**.** *Let*

$$y^2 = f(x) = x^3 + ax + b \tag{3.0.1}$$

be an elliptic curve and $a, b \in \mathbb{Z}$. We denote

$$\Delta := -4a^3 - 27b^2$$

the discriminant of f. If $P \in \mathcal{R}(C)$ and $\mathrm{ord}(P) < \infty$, then $x(P)$ and $y(P)$ are integers and either $y(P) = 0$, in which case $\mathrm{ord}(P) = 2$, or $y(P)^2 \mid \Delta$.

Remark. Authors of Silverman and Tate [2015] prove the weaker criterion $y \mid \Delta$ instead of $y^2 \mid \Delta$. We have chosen to prove the latter, which is also computationally more efficient. The proof of the stronger criterion was left as an exercise in the original book (see the same source, chapter Points of Finite Order, Exercise 2.11).

You might ask, "How does this theorem help with anything?" It is true that this theorem does not help us find any rational solutions in the first place. Sadly, as we already stated, there is as of yet no general method to accomplish this feat. It, however, *does* help in identifying equations with infinite number of solutions.

Just as the theorem states, if P is a rational point whose coordinates are not integers, then there are infinitely many points in $\mathcal{R}(C)$ or, said differently, infinitely many rational solutions to (3.0.1). We can even generate these solutions by adding P to itself again and again. Since, $\mathrm{ord}(P) = \infty$, the points

$$P, 2P, 3P, \ldots$$

[1] Trygve Nagell (1895 - 1988), Norwegian mathematician & Élisabeth Lutz (1914 - 2008), French mathematician. Ellingsrud [2009], Knapp [1999]

all lie in $\mathcal{R}(C)$ and are never equal to $\mathbf{0}$. The general 'algorithm' is to find all the points of finite order by adding points with integral coordinates to themselves or to one another. If there exists any other rational solution that is not on the list, then there are infinitely many more.

Among others, there is one more thing the **Nagell-Lutz theorem** is good for, especially from the perspective of group theory. It aids in determining what is traditionally called the *torsion part* of $\mathcal{R}(C)$, that is, the subgroup of $\mathcal{R}(C)$ generated by the elements of finite order. In this regard, it is often coupled with Mazur's[2] theorem which determines the structure of the torsion part of $\mathcal{R}(C)$ precisely. We will state Mazur's theorem at the end of the chapter as a bonus fact but intend not to prove it.

With our goal clear and the path leading to it very much not, we start off by studying the points of orders two and three, which are somewhat easier to catalogue than the rest.

3.1 Points of Order Two and Three

We have already met the points of order two when we derived the explicit formulae for $+$. We saw that all points of the shape $(p, 0)$ are of order two. However, the backward implication also holds. Every point of order two must have its y-coordinate equal to zero. Indeed, we can rewrite the condition

$$2P = \mathbf{0}$$

into a more translucent

$$P = -P.$$

One obvious solution is $P = \mathbf{0}$ but, for this point is by definition of order one, we can exclude it and henceforth suppose $P \neq \mathbf{0}$. Since $-(p_1, p_2) = (p_1, -p_2)$, we get $p_2 = -p_2$, which only occurs if $p_2 = 0$. Substituting $y = 0$ back to (3.0.1), we get

$$x^3 + ax + b = 0.$$

This means that there are at most three rational points of order two. Provided that we also forbade f to have multiple roots and complex solutions to a cubic equation are always conjugates of each other, there are always three, one or zero rational solutions to the equation above. The case where there are three is illustrated in **Figure 3.1.1**.

We have thus proven one half of the following lemma.

Lemma 3.1.1 (Points of order two)**.** *The following statements hold.*

(a) If $P \in \mathcal{R}(C)$ and $P \neq \mathbf{0}$ then $\operatorname{ord}(P) = 2$ *if and only if $y(P) = 0$.*

(b) The set of points of order lower or equal to two forms a subgroup of $\mathcal{R}(C)$ with one, two or four elements.

[2]Barry Charles Mazur (born 1937), American mathematician. O'Connor and Robertson [2009]

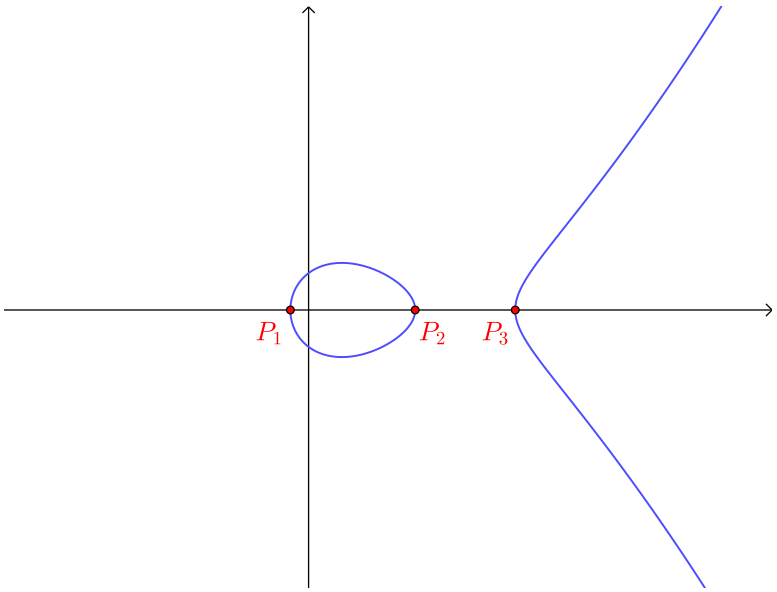


Figure 3.1.1: Three points of order two.

Proof. We have proven part (a) above. As for part (b), there is always one element of order one, namely $\mathbf{0}$. Depending on the number of rational solutions to the equation $f(x) = 0$, we either get zero, one or three other rational points of order two. It is obvious that the sum of any such two points gives the third since they all lie on the line $y = 0$. Hence, the points of order two or less truly form a subgroup of $\mathcal{R}(C)$. □

Remark. We can hear you, group theorists, shouting at us from your desks. Yes, the subgroup just mentioned is in all three cases isomorphic to a very well known group. If it is trivial, then it is of course isomorphic to $\mathbb{Z}_1$. If there is only one rational point of order two, then we have the isomorphism with $\mathbb{Z}_2$. In the last case, when there are three points of order two and one point of order one, the subgroup is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. One possible mapping is

$$\mathbf{0} \mapsto (0,0), \quad P_1 \mapsto (0,1), \quad P_2 \mapsto (1,0), \quad P_3 \mapsto (1,1).$$

Right now, you might be getting the feeling that if everything goes as smoothly as it has, we are done with the points of finite order before dinner. Worry not, though, since the points of order three are not nearly as easy to deal with, not to mention the higher orders.

A point $P \in \mathcal{R}(C)$ is of order three if

$$3P = \mathbf{0}$$

or, equivalently,

$$2P = -P.$$

We need to solve this last equation. Let us start with the x-coordinate. Thanks to our formulae derived in **Section 2.3**, we can calculate the x-coordinate of $2P$, where $P = (p_1, p_2)$, as

$$x(2P) = -2p_1 + \frac{(a + 3p_1^2)^2}{4p_2^2}.$$

For better readability, we let $x \coloneqq p_1$, $y \coloneqq p_2$ and solve the equation

$$-2x + \frac{(a + 3x^2)^2}{4y^2} = x.$$

Expanding terms and putting everything on the left side, we get

$$9x^4 + 6x^2a - 12xy^2 + a^2 = 0.$$

We can further substitute $y^2 = x^3 + ax + b$ to produce

$$3x^4 + 6ax^2 + 12bx - a^2 = 0. \tag{3.1.1}$$

We could find the roots of this quartic polynomial but it is unnecessary. Of true importance to us is the fact that there are at most four rational roots. We could now determine which points satisfy the equation

$$y(2P) = y(-P)$$

but we also need not. Since $x(2P) = x(-P)$ there are only two possible options. Either $y(2P) = y(-P)$, in which case we are done, or $y(2P) = -y(-P)$. However, $-y(-P) = y(P)$, which would mean

$$2P = P$$

or, in other words, $P = \mathbf{0}$, a case which we excluded at the start. Consequently, we have $y(2P) = y(-P)$ and it follows that all rational roots of (3.1.1) are points of order three.

Contrariwise, if $x(P)$ satisfies (3.1.1) for some $P \in \mathcal{R}(C)$, then $x(2P) = x(-P)$ and, again, either

$$2P = P \quad \text{or} \quad 2P = -P.$$

With the first case leading to $P = \mathbf{0}$, which we prohibited, we have $3P = \mathbf{0}$. Once again, we have proven one part of the lemma characterizing points of order three, which we now bring to light in all its glory.

Lemma 3.1.2 (Points of order three)**.** *The following statements hold.*

(a) A point $P \in \mathcal{R}(C)$, $P \neq \mathbf{0}$ is of order three if and only if $x(P)$ satisfies (3.1.1)*.*

(b) The set of points of order one or three forms a subgroup of $\mathcal{R}(C)$ which has one or three elements.

Proof. As in the previous lemma, (a) is already proven.

Let us denote g the quartic polynomial in (3.1.1). To prove (b), we unfortunately need to study the nature of the roots of g a little. First of all, we are going to prove that g has two real roots at most. For that, it is most convenient to study the discriminant of g. Since g is a repressed quartic (the term x^3 is missing), according to Rees [1922], if the discriminant, Δ, is negative, then g has two real

and two imaginary roots, all distinct. Sparing you the lengthy computation, we have reached the result

$$\Delta(g) = -110592a^6 - 1492992a^3b^2 - 5038848b^4.$$

It might not look like it but this number is a actually a multiple of a square. Indeed, you can verify that

$$\Delta(g) = -110592(a^3 + \frac{27}{4}b^2)^2.$$

This means that $\Delta \leq 0$ for any $a, b \in \mathbb{Q}$. It remains to show that $\Delta \neq 0$.

For that, we need to notice a not at all obvious relation. Doing the calculations, we see that

$$g'(x) = 12x^3 + 12ax + 12b = 12f(x).$$

So, if any x is at least a double root of g, it would have to be the root of f as well. However, the points $P = (x, y)$ where x is the root of f have their y-coordinate equal to zero. We have just proven that these are of order two. This leads to a contradiction since, according to (a), if $g(x) = 0$, then (x, y) has order three. Hence, we have $\Delta < 0$.

To reiterate, for any point $(x, y) \in \mathcal{R}(C)$ we know that $y = 0$ if and only if $\text{ord}((x, y)) = 2$, thus the two real roots x_1, x_2 of g correspond to four points - (x_1, y_1), (x_2, y_2) and their negatives.

However, it is easy to see that points of order three, together with $\mathbf{0}$, form a group. Indeed, if $P_1, P_2 \in \mathcal{R}(C)$, $\text{ord}(P_1) = \text{ord}(P_2) = 3$, then

$$3(-P_1) = -3P_1 = \mathbf{0} \quad \text{and} \quad 3(P_1 + P_2) = 3P_1 + 3P_2 = \mathbf{0}.$$

Since this group contains an element of order three, by Lagrange's[3] theorem, its order must be divisible by three. Nonetheless, we have just proven that g has zero, one or two real roots. All in all, we see that, since $3 \nmid 5$, two of these roots must correspond to points with a complex y-coordinate. If the other two points have rational coordinates, then there are two points of order three in $\mathcal{R}(C)$ and if they do not, there are none. This is what we wished to prove. □

Remark. Both **Lemma 3.1.1** and **Lemma 3.1.2** are stated differently here than they are in Silverman and Tate [2015]. We did not wish to include points of real and complex coordinates as the original authors did. The proof of the former lemma stayed more or less the same but the proof of the latter, especially part (b), thus required a very different approach.

Before we march forward and leave points of two and three in the dust forever, we mention a, to us not very important but still interesting, property of the points of order three. They are in reality points of inflection on C. Indeed, the condition

$$2P = -P$$

implies that if we take the tangent line at P and then connect the third intersection with $\mathbf{0}$, we get $-P$. That, however, can only happen if the third intersection

[3]Joseph-Louis Lagrange (1736 - 1813), French mathematician and astronomer. Struik [2020]

is the point P again. Since this fact does not help us study the points of finite order with the approach we have chosen, we leave it unproven and instead rely on geometrical intuition.

With points of orders two and three completely characterized, we enter the next section where we talk about the importance of the discriminant (which we used as the upper boundary for points of finite order in **Nagell-Lutz theorem**) and how it connects to the order of rational points.

3.2 The Discriminant

We have been mentioning discriminants here and there throughout the chapter but have never really defined them properly. We shall not do so in complete generality but instead shall only focus on discriminants of cubic polynomials.

Definition 3.2.1 (Discriminant)**.** If $f \in \mathbb{Z}[x, y]$, $\deg f = 3$ and x_1, x_2, x_3 are its (generally complex) roots, we define the *discriminant* of f as the quantity

$$\Delta(f) \coloneqq (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2.$$

We will write Δ instead of $\Delta(f)$ where the corresponding polynomial is clear from context.

We believe you have noticed this definition of the discriminant is different from the number we used in **Nagell-Lutz theorem**. Since both definitions of the discriminant come to be important later on, we are going to show their equivalence, at least in the case of

$$f(x) = x^3 + ax + b.$$

Before that however, we notice that by substituting $x \coloneqq x/d^2$, $y \coloneqq y/d^3$ into the equation above and multiplying by d, we end up with

$$y^2 = x^3 + d^4ax + d^6b.$$

So, if we choose $d \in \mathbb{Z}$ large enough, for example such that it is divisible by both the denominator of a and the denominator of b, we can transform our equation into one with integral coefficients. Hence, because we need to make vast use of the criterion of divisibility between integers, we assume our elliptic curve to be given by an integral equation.

Lemma 3.2.1 (Discriminating)**.** *If $f \in \mathbb{Z}[x, y]$ is an irreducible polynomial of degree three in the form*

$$f(x) = x^3 + ax + b$$

and x_1, x_2, x_3 are its complex roots, then

$$\Delta = -4a^3 - 27b^2.$$

Proof. If we let

$$w \coloneqq \frac{27b}{2} + \frac{\sqrt{108a^3 + 729b^2}}{2},$$

then, by Kurosh [1972], chapter Evaluating Roots of Polynomials, p. 226 - 230, roots of f can be written as

$$x_k = \frac{a}{\sqrt[3]{w}e^{2\pi ik}} - \frac{\sqrt[3]{w}e^{2\pi ik}}{3}.$$

After much simplification, we get

$$(x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = \frac{\sqrt{3}i(27a^3 + w^2)}{9w}.$$

Elevating to the second power gives

$$-\frac{27a^6}{w^2} - 2a^3 - \frac{w^2}{27}.$$

Finally, undoing the substitution and, yet again, simplifying, one gets

$$-4a^3 - 27b^2,$$

which completes the, arduously technical, proof. □

If, for now, we assume the trustworthiness of **Nagell-Lutz theorem**, then thanks to our definition of the discriminant, we are sure that there is a limited number of rational points of finite order in $\mathcal{R}(C)$. When the roots of f are distinct, which we always implicitly surmise, it follows that $\Delta \neq 0$. Thanks to that, there is only a finite set of integers $y \in \mathbb{Z}$ that satisfy $y^2 \mid \Delta$. When we substitute these integers into the equation

$$y^2 = f(x),$$

we end up with an equation in one variable and in the shape

$$h(x) = 0,$$

where $h(x) \coloneqq f(x) - y^2$. The polynomial h has integral coefficients, thus, by **Gauss's lemma**, if $x \in \mathbb{Z}$ is the root of h, then $x \mid c(h)$ for $\ell(h) = 1$. We see that there is only a finite number of integral pairs (x, y) which satisfy the criteria.

We were happy to share an algorithm based on an unproven hypothesis. Now that you were acquainted with the way points of finite order can be found, the time is nigh to show that **Nagell-Lutz theorem** can actually be proven, albeit using non-trivial methods.

Before we finally prove at least one part, the easier one, we need to bury ourselves in some additional computation, which will prove itself to be helpful later in the section. The duplication formula for a point P says that

$$x(2P) = u^2 - 2x(P),$$

where

$$u = \frac{3x(P)^2 + a}{2y(P)}.$$

We let $P \coloneqq (x, y)$ and will aim to rewrite the formula purely in terms of x. We note that for $f(x) = x^3 + ax + b$ we have $f'(x) = 3x^2 + a$. Thus

$$u = \frac{f'(x)}{2y}.$$

Further calculations give

$$\begin{aligned} x(2P) &= \frac{f'(x)^2}{4y^2} - 2x = \frac{f'(x)^2 - 8xy^2}{4y^2} = \frac{f'(x)^2 - 8xf(x)}{4f(x)} \\ &= \frac{x^4 - 2ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b}. \end{aligned}$$

Let us denote the polynomial in the numerator $\phi(x)$. Hence, we have

$$x(2P) = \frac{\phi(x)}{4f(x)}.$$

Ultimately, we need to share with you the fact that we can write $\Delta(f)$ as

$$\Delta(f) = (3x^3 - 5ax - 27b)f(x) + (-3x^2 - 4a)\phi(x). \tag{3.2.1}$$

One can easily verify this formula and the level of entertainment paired with the amount of gained insight would be matched perhaps only by the all-encompassing **Lemma 3.2.1** but we implore you to trust us with its correctness, this one time.

What we needed this formula for, is the following lemma. If we assume the first part of **Nagell-Lutz theorem**, namely that points of finite order have integral coordinates, we can prove the second part. Also, it is quite evident that $\operatorname{ord}(P) < \infty$ implies $\operatorname{ord}(2P) < \infty$.

We decided to style this lemma rather poetically in respect to the common saying, "The sky's the limit," as it can be interpreted to limit the 'height' of points of integral coordinates.

Lemma 3.2.2 (The discriminant's the limit)**.** *Let $P \in \mathcal{R}(C)$, $P \neq \mathbf{0}$ such that P and $2P$ have integral coordinates. Then either $y(P) = 0$ or $y(P)^2 \mid \Delta$.*

Proof. We may assume that $y(P) \neq 0$, otherwise $\operatorname{ord}(P) = 2$ and $2P = \mathbf{0}$.

Since for any point P

$$y(P)^2 = f(x(P)),$$

obviously $y(P)^2 \mid f(x(P))$. Thanks to the preparation we did above the lemma, we know that

$$x(2P) = \frac{\phi(x(P))}{4f(x(P))} = \frac{\phi(x(P))}{4y(P)^2}.$$

We assumed $x(2P)$ to be integral, so it follows that $y^2(P) \mid \phi(x(P))$. Taking (3.2.1) into consideration, we have ascertained that $y(P)^2 \mid \Delta$. □

With the easier part of **Nagell-Lutz theorem** successfully proven, we are very much on our way to prove the fact that each point of finite order has integral coordinates. The proof is long and difficult enough to make the content of its own section.

3.3 The Proof of Nagell-Lutz Theorem

Even though we have already proven the easier part of **Nagell-Lutz theorem**, the main part about points of finite order having integral coordinates remains veiled by the robe of uncertainty.

Now, and for the rest of the section, let $P \coloneqq (p_1, p_2)$ be a point of finite order in $\mathcal{R}(C)$. We shall employ a very peculiar approach in proving that p_1 and p_2 are integers. We are going to prove that there are no prime numbers dividing the denominators of p_1 and p_2. That leaves us with the only option available - that the denominators of p_1 and p_2 are equal to 1, which is tantamount to claiming they are both integers.

To such end, we choose an arbitrary prime number p and define the *prime affinity* of a rational number $q \in \mathbb{Q}$ (with respect to p) as the number $\nu \in \mathbb{Z}$ such that

$$q = \frac{m}{n} p^{\nu},$$

where m, n, p are pairwise coprime. In such case, we denote $\mathfrak{p}(q) = \nu$.

Remark. We should note that prime affinity is indeed well-defined. If $q = q_1/q_2$, then there are unique numbers $m, n, \alpha, \beta \in \mathbb{Z}$ such that

$$q_1 = mp^{\alpha}, \quad q_2 = np^{\beta}$$

and m, n, p are pairwise coprime. Then we have

$$q = \frac{q_1}{q_2} = \frac{mp^{\alpha}}{np^{\beta}} = \frac{m}{n} p^{\alpha - \beta}.$$

We let $\nu \coloneqq \alpha - \beta$.

The next step is to see what happens if the number p divides the denominator of p_1 or p_2. That is,

$$\mathfrak{p}(p_1) = -\mu \quad \text{and} \quad \mathfrak{p}(p_2) = -\sigma$$

for some $\mu, \sigma \in \mathbb{N}$. We will now show that μ, σ cannot be arbitrary.

Lemma 3.3.1. *Let $P \in \mathcal{R}(C)$, $P \neq \mathbf{0}$ and $\operatorname{ord}(P) < \infty$. If $\mu, \sigma \in \mathbb{N}$ are such that $\mathfrak{p}(p_1) = -\mu$, $\mathfrak{p}(p_2) = -\sigma$, then there exists a natural number $\nu \in \mathbb{N}$ that*

$$\mu = 2\nu \quad \textit{and} \quad \sigma = 3\nu.$$

Proof. We let

$$p_1 = \frac{m}{np^{\nu}}, \quad p_2 = \frac{k}{lp^{\sigma}}$$

for the adequate choices of $m, n, k, l \in \mathbb{Z}$. Plugging $x = p_1$, $y = p_2$ into (3.0.1), we obtain

$$\frac{am}{np^{\mu}} + b + \frac{m^3}{n^3 p^{3\mu}} = \frac{k^2}{l^2 p^{2\sigma}}.$$

Putting terms over a common denominator, we further get

$$\frac{amn^2 p^{2\mu} + bn^3 p^{3\mu} + m^3}{n^3 p^{3\mu}} = \frac{k^2}{l^2 p^{2\sigma}}.$$

By assumption, $\gcd(p, l) = \gcd(p, k) = 1$, so

$$\mathfrak{p}\left(\frac{k^2}{l^2 p^{2\sigma}}\right) = -2\sigma.$$

Since $p \nmid m$, we also know that

$$p \nmid amn^2p^{2\mu} + bn^3p^{3\mu} + m^3.$$

However, this implies

$$\mathfrak{p}\left(\frac{amn^2p^{2\mu} + bn^3p^{3\mu} + m^3}{n^3p^{3\mu}}\right) = -3\mu.$$

This proves that $2\sigma = 3\mu$ and, consequently, $2 \mid \mu$, $3 \mid \sigma$. Thus, $\mu > 0$ if and only if $\sigma > 0$ and, in this case, there exists a non-zero natural number $\nu \in \mathbb{N}$ such that $\mu = 2\nu$ and $\sigma = 3\nu$. □

Similarly, had we assumed that $\sigma > 0$, by the same chain of calculations we would have reached exactly the same result. As it stands, whenever p divides the denominator of p_1 or p_2, it necessarily divides the denominator of the other; and the powers are 2ν and 3ν for some natural number, respectively.

Since we so painstakingly defined the group law on $\mathcal{R}(C)$, it is time to employ our undoubted proficiency in group theory, yet again. The just proven lemma inspires the succeeding definition.

Definition 3.3.1. For a given prime number p and natural number $\nu > 0$, we denote

$$\mathcal{R}_p^\nu(C) = \{(x, y) \in \mathcal{R}(C) \mid \mathfrak{p}(x) \leq -2\nu \wedge \mathfrak{p}(y) \leq -3\nu\},$$

that is, the set of all the rational points (x, y) such that $p^{2\nu}$ divides the denominator of x or, equivalently, $p^{3\nu}$ divides the denominator of y. We include the point $\mathbf{0}$ in every such set by convention.

Remark. Do notice that for any $\mu < \sigma$ natural, we have the inclusion

$$\mathcal{R}_p^\mu(C) \supset \mathcal{R}_p^\sigma(C).$$

Hence, in our newly defined notation, the problem of the denominator not being divisible by a prime number p was transformed into the task of showing that no point of finite order can lie in $\mathcal{R}_p^1(C)$. Firstly, nonetheless, we are to show that each one of $\mathcal{R}_p^\nu(C)$ is a subgroup of $\mathcal{R}(C)$.

Remember that when p divides the denominator of p_1, then a higher power of p divides the denominator of p_2. We also defined $\mathcal{R}_p^\nu(C)$ as the set of rational tuples whose coordinates' prime affinity is lower than some multiple of ν. We wish to turn this around, or, in other words, we would like to apply a transformation to our curve such that when $(x, y) \in \mathcal{R}_p^\nu(C)$, then instead the numerators of the coordinates of the transformed tuple would be divisible by p to the power of some multiple of ν. Thus, we apply the mapping

$$\frac{x}{y} \mapsto t, \quad \frac{1}{y} \mapsto s$$

and shall for the moment be working with our curve in the (t, s) plane. Now, if $(x, y) \in \mathcal{R}_p^\nu(C)$ for some ν, then we can write

$$x = \frac{m}{np^{2(\nu+i)}}, \quad y = \frac{k}{lp^{3(\nu+i)}}$$

where $i \geq 0$. Applying the aforementioned mapping, we produce

$$t = \frac{ml}{nk}p^{\nu+i}, \quad s = \frac{l}{k}p^{3(\nu+i)}.$$

Count our objective accomplished since now $p^{\nu+i}$ divides the numerator of t and $p^{3(\nu+i)}$ divides the numerator of s.

Remark. We are certain you have noticed that the mapping is not bijective, or better said, it is bijective almost everywhere. There is a finite number of points wherefor their image is not defined, namely the points with $y = 0$. However, as we have proven in **Section 3.1**, these points are of order two and we already studied those thoroughly. Thus, we do not need to include them in the (t, s) plane.

It is evident that $(x, y) \in \mathcal{R}_p^\nu(C)$ if and only if

$$\mathfrak{p}(t) \geq p^\nu \quad \text{and} \quad \mathfrak{p}(s) \geq p^{3\nu}.$$

To verify that $\mathcal{R}_p^\nu(C)$ are subgroups, we need to ascertain that for every two points $P_1, P_2 \in \mathcal{R}_p^\nu(C)$ their negatives and their sum lie in $\mathcal{R}_p^\nu(C)$. Unfortunately, this entails finding the formula for the sum of points again the (t, s) plane. We promise it will be worth the time and effort in the end, though.

There is another way to look at the mapping $t \coloneqq x/y, s \coloneqq 1/y$. If we visit the projective plane for a minute and, as always, we identify the point (x, y) with $[x : y : 1] \in \mathbb{P}(\mathbb{R}^2)$, then, if $y \neq 0$, this point is by definition equivalent to $[x/y : 1 : 1/y] = [t : 1 : s]$. So, from the projective perspective, we have not really done much at all. We have simply chosen to identify the point (x, y) for $y \neq 0$ with $[t : 1 : s]$, instead of $[x : y : 1]$.

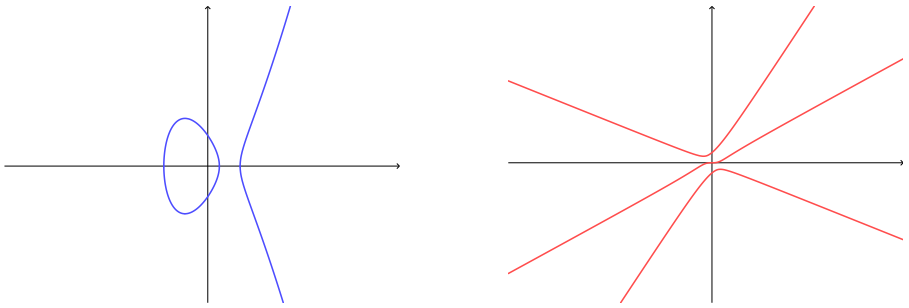
"What happens with the points where $y = 0$?" you ask. Those get mapped to points $[t : 0 : s]$, that is, to points at infinity. However, as we have already stated, this is of little matter to us since those are of order two and we came to understand them not long ago. It also follows from the identification of (x, y) with $[t : 1 : s]$ that lines get mapped to lines and cubic to cubics. It should be noted, too, that the mapping has the additional advantage of bringing $\mathbf{0}$ down to earth, literally, since $\mathbf{0} = [0 : 1 : 0]$ is the point $(0, 0)$ in the (t, s) plane.

For further calculations, we state, and it can be verified by simple substitution, that a rational line in the (t, s) plane is given by

$$at + b + cs = 0,$$

if $ax + by + c = 0$ was a rational line in the (x, y) plane. Also, our elliptic curve unfortunately does not stay elliptic but it is still a cubic curve. That is, with the substitutions performed, we now work with

$$s = t^3 + ats^2 + bs^3. \tag{3.3.1}$$



(a) The curve $y^2 = x^3 - 5x + 3$. (b) The curve $s = t^3 - 5s^2t + 3s^3$.

Figure 3.3.1: The 'same' curve in two different planes.

There is more thing left before we put or calculators to use again. For further developments, it is advantageous to define a special ring R_p, as the ring of rational numbers whose denominator is not divisible by p. To put it in prime affinity terms, a rational number q lies in R_p if and only if $\mathfrak{p}(q) \geq 0$. Notice that R_p is indeed a ring, and thus a subring of the field of rational numbers. If $q_1, q_2 \in R_p$, then the denominator of their sum and product is not divisible by p, either, so they lie in R_p. It is also rather apparent that the ideals $p^\nu R_p$ consist of all the rational numbers whose prime affinity is higher than p^ν. In other words, for a point P in the (t, s) plane to lie in $\mathcal{R}_p^\nu(C)$ is the same as require that $t(P) \in p^\nu R_p$ and $s(P) \in p^{3\nu} R_p$, where $t(P), s(P)$ denote the t and s-coordinate of P, respectively.

In the following text, we will need one particular property of R_p. It is, in fact, a unique factorization domain with exactly one prime element - p. First of all, every element of R_p can be written as mp^ν/n for some natural $\nu \in \mathbb{N}$ where m, n, p are pairwise coprime. It follows that the only invertible elements (units) in R_p are rational numbers of prime affinity 0. Indeed, if $mp^\nu/n \in R_p$, then its inverse in $\mathbb{Q}$ is n/mp^ν which, however, lies in R_p if and only if $\nu = 0$. As a consequence, the only primes in R_p are of the shape mp/n. In other words, p is the only prime in R_p up to multiplication by invertible elements.

The fact that R_p is a unique factorization domain stems from the following lemma.

Lemma 3.3.2. *Let R_p be the subring of rational numbers with denominator prime to p. Then R_p is a principal ideal domain.*

Proof. To show that R_p is a principal ideal domain, as the we need to check that every ideal is principal, that is is generated by just one element. We will first make use of the fact that every subring of rational numbers is noetherian. This result can be found for example in Gilmer [1970]. Thus, we know that every ideal $I < R_p$ is finitely generated. Let for instance

$$I = (a_1, a_2, \ldots, a_n).$$

Since each one of a_i lies in R_p, it can be uniquely written as $a_i = m_i p^{\nu_i}/n_i$. Now, if we let $\nu := \min\{\nu_i \mid i \leq n\}$, then $I = p^\nu R_p$. Indeed, if, without loss of generality, $a_1 = m_1 p^\nu / n_1$, then for every other $i \leq n$, we have that

$$a_i = \frac{m_i p^{\nu_i}}{n_i} = \frac{n_1 m_i}{m_1 n_i} p^{\nu_i - \nu} a_1.$$

The fraction $n_1 m_i p^{\nu_i - \nu}/m_1 n_i$ lies in R_p because $\nu_i \geq \nu$. This completes the proof. □

It is a well-known fact, and not too demanding to prove, that every principal ideal domain is also a unique factorization domain. Thus, we have that R_p is a unique factorization domain with only one prime element.

We will make ample use of this fact after we derive the formulae for addition of points in the (t, s) plane. We denote $P_1 = (t_1, s_1), P_2 = (t_2, s_2) \in \mathcal{R}_p^\nu(C)$, $P_1 \neq P_2$. For now, we assume that $t_2 \neq t_1$ and deal with this case later. Then the line connecting P_1 and P_2 is given by

$$s = ut + v$$

where

$$u = \frac{s_1 - s_2}{t_1 - t_2}, \quad v = \frac{t_1 s_2 - s_1 t_2}{t_1 - t_2}.$$

Substituting into (3.3.1) and collecting powers of t gives

$$\left(au^2 + bu^3 + 1\right) t^3 + \left(2auv + 3bu^2 v\right) t^2 + \left(av^2 + 3buv^2 - u\right) t + bv^3 - v = 0.$$

Let us denote $P_1 * P_2 = (t_3, s_3)$. We know that the roots of this polynomial are t_1, t_2 and t_3. By Viète's relations

$$t_1 + t_2 + t_3 = -\frac{2auv + 3bu^2 v}{au^2 + bu^3 + 1}.$$

Now that we acquired the formula for $P_1 * P_2$, finding $P_1 + P_2$ is easy. It is easily verifiable by substituting into (3.3.1) that whenever $(t, s) \in C$, then $(-t, -s) \in C$. So, the line passing through $P_1 * P_2$ and $\mathbf{0} = (0, 0)$ meets the cubic at $(-t_3, -s_3)$, which is by definition $P_1 + P_2$.

To make any progress, we must prove that of $u \in p^{2\nu} R_p$. Why? Because then we will prove that $t_3 \in p^\nu R_p$. This stems from the fact that both t_1 and t_2 lie in $p^\nu R_p$ and also the numerator of

$$-\frac{2auv + 3bu^2 v}{au^2 + bu^3 + 1}$$

lies in $p^{2\nu} R_p$. Since $au^2 + bu^3$ also lies in $p^{2\nu} R_p$, we have that $1 + au^2 + bu^3$ is a unit in R_p. Thus, the whole expression lies in $p^{2\nu} R_p$ and, in turn, t_3 lies in $p^\nu R_p$.

Furthermore, we notice that

$$v = s_1 - ut_1$$

since the line $s = ut + v$ passes through $P_1 = (t_1, s_1)$. If we keep supposing $u \in p^{2\nu} R_p$, then, provided that $s_1 \in p^{3\nu} R_p$, we get $s_3 \in p^{3\nu} R_p$ as well. This is indeed true, because if $u \in p^{2\nu} R_p$ and also $t_1 \in p^\nu R_p$, then obviously $ut_1 \in p^{3\nu} R_p$. As a consequence, $v \in p^{3\nu} R_p$.

Summarizing our thoughts, if we prove that $u \in p^{2\nu} R_p$, then $t_3 \in p^\nu R_p$ and $s_3 \in p^{3\nu} R_p$, which is exactly the condition for a point in the (t, s) plane to lie in $\mathcal{R}_p^\nu(C)$. We would then prove that $\mathcal{R}_p^\nu(C)$ is closed under addition.

At the start, we assumed that P_1 and P_2 were distinct. However, we will soon see that one formula can be used for adding two points and for doubling a point.

To show that $u \in p^{2\nu}R_p$, we first rewrite u a little. If we substitute s_1 and s_2 into (3.3.1), we get (after some factorization)

$$\begin{aligned} s_1 - s_2 &= (t_1^3 - t_2^3) + a(s_1^2 t_1 - s_2^2 t_2) + b(s_1^3 - s_2^3) \\ &= (t_1^3 - t_2^3) + a((t_1 - t_2)s_1^2 + t_2(s_1^2 - s_2^2)) + b(s_1^3 - s_2^3). \end{aligned}$$

Putting all terms on the right side and factoring $t_1 - t_2$ and $s_1 - s_2$ from terms divisible by these quantities, we get

$$0 = (t_1 - t_2)(t_1^2 + t_1 t_2 + t_2^2 + a s_1^2) + (s_1 - s_2)(t_2(s_1 + s_2) + b(s_1^2 + s_1 s_2 + s_2^2) - 1).$$

We rewrite this as

$$0 = \alpha(t_1 - t_2) + \beta(s_1 - s_2)$$

where α, β are the corresponding expressions. We thus get

$$\frac{s_1 - s_2}{t_1 - t_2} = -\frac{\alpha}{\beta}.$$

Substituting back, we arrive at

$$u = \frac{s_1 - s_2}{t_1 - t_2} = \frac{t_1^2 + t_1 t_2 + t_2^2 + a s_1^2}{1 - a t_2(s_1 + s_2) - b(s_1^2 + s_1 s_2 + s_2^2)}. \tag{3.3.2}$$

You might wonder why we exchanged a simple formula for a way more florid one. There are two reasons, with one of them becoming apparent promptly.

Rules of differential calculus dictate that the slope of a tangent line at $P_1 = (t_1, s_1)$ to our curve C is given by

$$\frac{\mathrm{d}s}{\mathrm{d}t}(P_1) = 3t_1^2 + a s_1^2 + 2a t_1 s_1 \frac{\mathrm{d}s}{\mathrm{d}t}(P_1) + 3b s_1^2 \frac{\mathrm{d}s}{\mathrm{d}t}(P_1).$$

Factoring out and dividing gives

$$\frac{\mathrm{d}s}{\mathrm{d}t}(P_1) = \frac{3t_1^2 + a s_1^2}{1 - 2a t_1 s_1 - 3b s_1^2}.$$

Notice that this formula is exactly the same as (3.3.2) when we substitute $t_1 = t_2$ and $s_1 = s_2$.

Now, for the second reason we employed our intricate formula for u. Do you see the term 1 in its denominator? Of course you do. This little insignificant 1 ensures that the denominator of u is a unit in R_p. That is because

$$-a t_2(s_1 + s_2) - b(s_1^2 + s_1 s_2 + s_2^2)$$

lies in $p^{3\nu}R_p$. Also, in the numerator of u, there is a sum of products of terms all belonging $p^{\nu}R_p$. Which means that the numerator of u lies in $p^{2\nu}R_p$. Since we have just observed that the denominator of u is a unit in R_p, we have that $u \in p^{2\nu}R_p$. But that is precisely what we wanted! Now, there remains only the case of two distinct point sharing the same t-coordinate.

If $t(P_1) = t(P_2)$ then the line connecting P_1 with P_2 is a vertical line $t = t(P_1) = t_1$. We denote (t_3, s_3) the third intersection of $t = t_1$ with C. It is obvious that $t_3 = t_1$, thus $t_3 \in p^\nu R_p$. We show that $s_3 \in p^{3\nu} R_p$ by a series of expression transformations akin to the ones afore. We denote $t \coloneqq t_1 = t_2 = t_3$ and look at (3.3.1) as a cubic equation in s, that is

$$bs^3 + at^2 - s + t^3 = 0.$$

Since $t_1 = t_2 = t_3$, this polynomial has the roots s_1, s_2 and s_3. By Viète's relations

$$s_1 + s_2 + s_3 = \frac{-at}{b}.$$

From (3.3.1) we substitute

$$t \coloneqq \frac{t^3 - s_3 + bs_3^3}{as_3^2}.$$

Plugging this into our relation, we get

$$s_1 + s_2 + s_3 = \frac{-t^3 + s_3 - bs_3^3}{bs_3^2}.$$

We also know (again, from Viète's relations) that

$$s_1 s_2 s_3 = t^3.$$

Substituting $s_3 = t^3/s_1 s_2$ and simplifying yields

$$s_1 + s_2 + s_3 = \frac{-t^3 s_1^3 s_2^3 + t^3 s_1^2 s_2^2 - bt^9}{bt^2 s_1 s_2}.$$

Using the final relation

$$s_1 s_2 = -\frac{1}{b} - s_1 s_3 - s_2 s_3$$

and then substituting $s_3 = t^3/s_1 s_2$ again, gives, after straightforward computation,

$$s_1 + s_2 + s_3 = \frac{-ts_1^4 s_2^4 + t^3 s_1^3 s_2^3 - bt^7}{1 + bt^3 s_1 + bt^3 s_2}.$$

Since $b \in \mathbb{Z}$, definitely $\mathfrak{p}(b) \geq 0$. Owing to that, the expression $bt^3 s_1 + bt^3 s_2 \in p^{3\nu} R_p$. Hence, the denominator is invertible in R_p. The numerator most certainly lies in $p^{3\nu} R_p$ and together with the fact that $s_1, s_2 \in p^{3\nu} R_p$, we get that $s_3 \in p^{3\nu} R_p$. Thus, we have shown that $(t_3, s_3) \in \mathcal{R}_p^\nu(C)$, which rids us of the special case because $P_1 + P_2 = -(t_3, s_3)$.

With the special case resolved, we have now proven that every $\mathcal{R}_p^\nu(C)$ is closed under addition of any two points on the plane, that it is a subgroup of $\mathcal{R}(C)$.

A good question that should arise right now is, "What is all this good for?" For a lot, mind you. To jump right to the first application of our findings, if we take a look back at the formula for the sum of two points, we have

$$t(P_1) + t(P_2) + t(P_1 * P_2) = -\frac{2auv + 3bu^2 v}{au^2 + bu^3 + 1}.$$

We already observed that the denominator of this expression is invertible in R_p. We know that $u \in p^{2\nu} R_p$ and $v \in p^{3\nu} R_p$. Upon closer inspection, we see that the

numerator lies in $p^{5\nu}R_p$ and thus the whole fraction lies in $p^{5\nu}R_p$. Hence, we have that

$$t(P_1) + t(P_2) + t(P_1 * P_2) \in p^{5\nu}R_p.$$

Since $t(P_1 + P_2) = -t(P_1 * P_2)$ we also get, using everyone's favorite congruence notation, that

$$t(P_1) + t(P_2) \equiv t(P_1 + P_2) \pmod{p^{5\nu}R_p}.$$

This congruence is important because of the fact that it relates the operation $+$ in $\mathcal{R}_p^\nu(C)$, which is a geometrical operation on the set of rational points, and the operation $+$ in $p^{5\nu}R_p$, which is a traditional addition of two rational numbers.

One is then prompted to define the map

$$\iota : \mathcal{R}_p^\nu(C) \to p^\nu R_p, \quad P \mapsto t(P).$$

This map does not, unfortunately, define a homomorphism, since in general $t(P_1) + t(P_2) \neq t(P_1 + P_2)$ in $p^\nu R_p$. However, this relation *is* true in the quotient group $p^\nu R_p / p^{5\nu} R_p$ as we have just observed. Thus, the map

$$\mathcal{R}_p^\nu(C) \to {}^{p^\nu R_p}\!\diagup_{p^{5\nu}R_p}$$

is a homomorphism. Its kernel are obviously all the points P with $\mathfrak{p}(t(P)) \geq p^{5\nu}$, that is, all points in $\mathcal{R}_p^{5\nu}(C)$. Hence, finally, founding ourselves in the principles of group theory, we have found a monomorphism

$$\iota : {}^{\mathcal{R}_p^\nu(C)}\!\diagup_{\mathcal{R}_p^{5\nu}(C)} \hookrightarrow {}^{p^\nu R_p}\!\diagup_{p^{5\nu}R_p}.$$

We send $\mathbf{0} \mapsto 0$ by convention.

Remark. It is not too demanding to prove, but we shall not do it here, that $p^\nu R_p / p^{5\nu} R_p$ is a cyclic group of order $p^{4\nu}$. Thus, through the monomorphism ι, $\mathcal{R}_p^\nu(C)/\mathcal{R}_p^{5\nu}(C)$ is a cyclic group of order p^σ for some $0 \leq \sigma \leq 4\nu$.

All of the work will see its fruits, when we now prove the main part of **Nagell-Lutz theorem** and also the final claim of the thesis.

Claim 3.3.3 (Points of finite order)**.** *For every prime number p, the group $\mathcal{R}_p^1(C)$ contains no non-zero points of finite order.*

Proof. Let $P \in \mathcal{R}(C), P = (p_1, p_2)$, $\mathrm{ord}(P) = m \in \mathbb{N}$. Since $P \neq \mathbf{0}$, we know that $m \neq 1$. We assume that $P \in \mathcal{R}_p^1(C)$ and arrive at a contradiction.

Although P can also lie in some smaller $\mathcal{R}_p^\nu(C)$, it obviously cannot lie in *every* group $\mathcal{R}_p^\nu(C)$ since that would imply that the denominator (P is in the (x, y) plane) of p_1 would be divisible by p^ν for arbitrarily large ν. Hence, we find the number $\nu > 0$ such that $P \in \mathcal{R}_p^\nu(C)$ but $P \notin \mathcal{R}_p^{\nu+1}(C)$. We will study two cases, depending on whether p divides m or not.

First, we assume that $p \nmid m$. We have seen that the congruence

$$t(P) + t(P) \equiv t(P + P) \pmod{p^{5\nu}R_p}$$

holds. By its repeated application m-times, we get

$$mt(P) \equiv t(mP) \pmod{p^{5\nu} R_p}.$$

However, since $p \nmid m$, m is invertible in $p^{5\nu} R_p$. This congruence thus becomes

$$t(P) \equiv 0 \pmod{p^{5\nu} R_p},$$

which implies $P \in \mathcal{R}_p^{5\nu}(C)$ and in return contradicts the assumption that $P \notin \mathcal{R}_p^{\nu+1}(C)$.

Let us now suppose that $p \mid m$. We can thus write $m = np$ for some $n \in \mathbb{N}$. We shall instead study the point $P' = nP$. Since $\mathrm{ord}(P) = m$, it follows that $\mathrm{ord}(P') = p$. Because $\mathcal{R}_p^1(C)$ is closed under addition, we have that $P' \in \mathcal{R}_p^1(C)$. Just as in the previous case, we find a number $\nu > 0$ such that $P' \in \mathcal{R}_p^{\nu}(C)$ but $P' \notin \mathcal{R}_p^{\nu+1}(C)$. We have the congruence

$$0 = t(\mathbf{0}) = t(pP') \equiv pt(P') \pmod{p^{5\nu} R_p}.$$

We thus have

$$t(P') \equiv 0 \pmod{p^{5\nu-1} R_p},$$

which, again, implies $P' \in \mathcal{R}_p^{5\nu-1}(C)$ and contradicts $P' \notin \mathcal{R}_p^{\nu+1}(C)$.

Since both cases led to a contradiction, we have proven that $P \notin \mathcal{R}_p^1(C)$. □

With this, we have completely overcome the ordeal of proving **Nagell-Lutz theorem**. When P is a point of finite order, then no prime divides the denominator of the coordinates of P. This can only occur if both coordinates are integral.

Before we march away once and for all, we state the promised Mazur's theorem, which classifies the points of finite order with greater precision.

Theorem 3.3.4 (Mazur's)**.** *If C is a non-singular cubic curve, then all the rational points of finite order form a subgroup of $\mathcal{R}(C)$ which assumes one of the following forms:*

(1) a cyclic group of order n for $1 \leq n \leq 10$ or $n = 12$,

(2) the product of a cyclic group of order two with a cyclic group of order $2n$ for $1 \leq n \leq 4$.

Proof. See for example Kamienny and Mazur [1995], p. 81 - 100. □

3.4 Examples and Problems

Since the chapter was chiefly dedicated to points of finite order, it seems appropriate to include a concrete example of how the search for all points of finite order on an elliptic curve actually goes.

Problem 3.4.1. Find all the points of finite order on

$$y^2 = f(x) = x^3 - 43x + 166.$$

Solution. We first calculate the discriminant of f. We have

$$\Delta = -4a^3 - 27b^2 = -425984.$$

When testing the divisibility of Δ by different integers, it is beneficial to factorize it. A computational software or a lot of patience yields

$$425984 = 2^{15} \cdot 13.$$

We start with the points of order two. If $y = 0$, then we are looking for the integral solutions to

$$x^3 - 43x + 166 = 0.$$

Since any integral solution must by **Gauss's lemma** divide $166 = 2 * 83$, we do not have many options. The only divisors are $1, 2, 83, 166$ and their negatives. Having tried these options, we have reached the conclusion that there are no points of order two on our curve. Hence, we proceed to find points of higher order.

Since y^2 must divide Δ, y must be a power of 2, lower than 2^7. The options are thus $1, 2, 4, 8,$ $16, 32, 64$ and 128, together with their negatives. We deal, for the sake of randomness, explicitly with 8 and -1. The rest is left to computing enthusiasts. If $y = 8$, we need to find all integral solutions to

$$x^3 - 43x + 166 - 64 = x^3 - 43x + 102 = 0.$$

The divisors of 102 are $1, 2, 3, 6, 17, 34, 51$ and 102, again, with their negatives. Repeated substitutions declare that $x = 3$ is the only integral solution. Thus, we have found the point $(3, 8)$ on our curve. We will determine its order. By repeatedly doubling the point, we reach the conclusion that

$$8(3, 8) = (3, 8),$$

thus, $\text{ord}((3, 8)) = 7$.

Now, if $y = -1$, the process is analogous. We are now looking at the integral solutions to

$$x^3 - 43x + 165 = 0.$$

The divisors of 165 are $1, 3, 5, 11, 15, 33, 55$ and 165. Plugging those numbers in reveals that there are no points of finite order with y-coordinate equal to -1.

Had we continued in this fashion for quite a while longer, we would have ascertained that there are only six points of finite order on our curve, namely $(3, 8)$, $(11, 32)$, $(5, 16)$ and their negatives. Since $\text{ord}((3, 8)) = 7$, thanks to Lagrange's theorem and **Mazur's theorem**, we now know that the rational points of finite order on our curve form a cyclic group of order 7. ⊠

Conclusion

We have introduced the theory of Diophantine equations and shown how the study of algebraic curves leads to potential rational solutions. We have dealt with the theory of rational conics, having shown that the nature of their set of rational points is fully understood.

Furthermore, we thoroughly studied cubic curves, showed that cubics with singular points are understood just as well as conics and that every cubic curve is birationally equivalent to a cubic curve in Weierstrass's normal form, which we called elliptic. On the set of rational points of an elliptic curve, we defined a commutative group law by intersecting lines passing through the points of the curve with the curve itself.

Finally, we pondered the structure of the torsion part of the set of rational points of an elliptic curve and proved the important Nagell-Lutz theorem which determines the set of rational points precisely.

All in all, the theory of elliptic curves and algebraic geometry in general is a mathematical discipline which has yielded many non-trivial results throughout the last century and also one which I incline towards the most. The preparation for the thesis, mostly involving attempts to understand difficult concepts, and its writing, often met with caveats which took time to overcome, have in times of success brought me sincere joy and I hope this is not the last bit of algebraic geometry that is seen written by my hand.

Bibliography

Joseph H. Silverman and John T. Tate. *Rational Points on Elliptic Curves*. Springer, 2 edition, June 2015. ISBN 3319307576.

Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography*. Chapman and Hall/CRC, 2 edition, April 2008. ISBN 9781420071467.

William Fulton. *Algebraic Curves: An Introduction to Algebraic Geometry*. 3 edition, January 2008. URL `http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf`.

Sir Thomas Heath. *Diophantus of Alexandria: A Study in the History of Greek Algebra*. Martino Fine Books, April 2009. ISBN 978-1578987542.

Dana Pellegrino. Pierre de Fermat. 2000. URL `https://sites.math.rutgers.edu/~cherlin/History/Papers2000/pellegrino.html`.

Simon Singh. *Fermat's Last Theorem*. Fourth Estate Ltd, 1997. ISBN 978-1857025217.

W. S. Anglin. The square pyramid puzzle. *The American Mathematical Monthly*, 97(2):120–124, February 1990.

Minal Wankhede Barsagade and Suchitra Meshram. Overview of history of elliptic curves and its use in cryptography. *International Journal of Scientific & Engineering Research*, 5, April 2014. ISSN 2229-5518.

Peter Duren. Changing faces: The mistaken portrait of Legendre. *Notices of the American Mathematical Society*, 56(11):1440–1443, December 2009.

Joseph Lee. Rational points on conics. *MIT OpenCourseWare*, 2012. URL `https://ocw.mit.edu/courses/mathematics/18-781-theory-of-numbers-spring-2012/lecture-notes/MIT18_781S12_lec24.pdf`.

Emil Grosswald. *Representations of Integers as Sums of Squares*. Springer, 1985. ISBN 978-1-4613-8568-4.

Judith Grabiner. *Dictionary of Scientific Bibliography*. Schribner, 2 edition, 1970-1980. ISBN 978-0-684-10114-9.

Stefan Kleiner and Ralf Knöbl. *Duden, das Aussprachewörterbuch*. Bibliographisches Institut, 7 edition, 2015. ISBN 978-3-411-04067-4.

Andreas Gathmann. Class Notes TU Kaiserslautern 2018. 2018. URL `https://www.mathematik.uni-kl.de/~gathmann/class/curves-2018/curves-2018.pdf`.

J. J. O'Connor and E. F. Robertson. François Viète. *MacTutor History of Mathematics archive*, January 2000. URL `https://mathshistory.st-andrews.ac.uk/Biographies/Viete/`.

Geir Ellingsrud. Trygve Nagell. *Norsk biografisk leksikon*, September 2009. URL https://nbl.snl.no/Trygve_Nagell.

Anthony W. Knapp. André Weil: A prologue. *Notices of the American Mathematical Society*, 46(4):434–439, 1999. URL http://www.ams.org/notices/199904/mem-weil-prologue.pdf.

J. J. O'Connor and E. F. Robertson. Barry Charles Mazur. *MacTutor History of Mathematics archive*, September 2009. URL https://mathshistory.st-andrews.ac.uk/Biographies/Mazur_Barry/.

E. L. Rees. Graphical discussion of the roots of a quartic equation. *The American Mathematical Monthly*, 29(2):51–55, 1922. doi: 10.1080/00029890.1922.11986100. URL https://doi.org/10.1080/00029890.1922.11986100.

Dirk Jan Struik. Joseph-Louis Lagrange, comte de l'Empire. *Encyclopædia Britannica*, 2020. URL https://www.britannica.com/biography/Joseph-Louis-Lagrange-comte-de-lEmpire.

A. G. Kurosh. *Higher algebra*. MIR, 1972. Translated from Russian.

Robert Gilmer. Integral domains with noetherian rings. *Commentarii Mathematici Helvetici*, (45):129–134, 1970.

Sheldon Kamienny and Barry Mazur. Rational torsion of prime order in elliptic curves over number fields. *Astérisque*, 3(228), 1995.

List of Figures