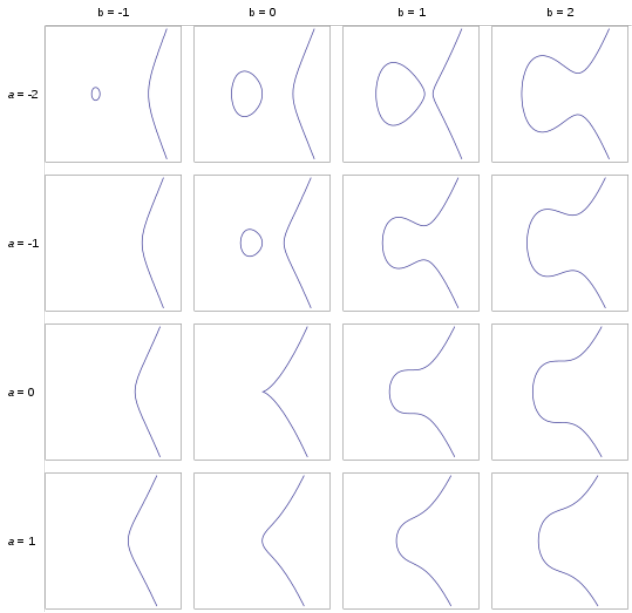
# The Arithmetic of Elliptic Curves

David Kurniadi Angdinata

Monday, 2 July 2018 - Friday, 28 September 2018




*"It is possible to write endlessly on elliptic curves. (This is not a threat.)"[1]*

**Abstract**

In the field of algebraic geometry, elliptic curves are deeply studied rich structures with far-fetching computational applications to classical number theory and contemporary cryptography. It is a fundamental tool in Wiles' proof of Fermat's last theorem, as well as the main object of discussion in the Birch and Swinnerton-Dyer conjecture, an open problem in number theory deemed worthy of being called one of the Millennium Prize Problems by the Clay Mathematics Institute. In this project, three of the four most fundamental theorems in the arithmetic of elliptic curves, namely the Hasse-Weil theorem, the Nagell-Lutz theorem, and the Mordell-Weil theorem, are proven in their respective special forms. Schoof's algorithm for counting rational points over Galois fields will also be briefly discussed, allowing for an application to integer factorisation and primality testing. An introductory section and a brief appendix on fields, varieties, curves, and groups are also included for completion.

# Contents

# Preface

The aim of this project is to provide a gentle introduction to the deep theory of *elliptic curves*. My approach for the report is to deliver information in the form of general propositions and fundamental theorems, providing adequate proofs whenever possible. Admittedly, almost all of the work here is unoriginal and should have been done elsewhere in a similar fashion, but I have tried to make the flow of information as coherent as possible, consulting various online resources as well as the two books [2] and [3].

As the theory of elliptic curves requires some technical background in algebraic geometry, which in turn requires prerequisites in commutative algebra, both of which I have zero background in, the report is rather superficial and may not provide as good of an insight to deeper theory. In addition to the first two years of undergraduate mathematics, the first three preliminary appendices A.1, A.2, and A.3 will provide all the required background to understand the first introductory section, while a few additional notions in appendix A.4 will allow the rest to be fully accessible to middle-year undergraduates such as myself.

The first section introduces elliptic curves while hiding away the definitions and results taken from algebraic geometry. For instance, the use of explicit *Weierstrass equations* and formulae for the *group law* is an active attempt to avoid bringing in the *Riemann-Roch theorem* in algebraic geometry to prove that they are related. As such, many proofs in this section are omitted, but are all given a direct reference.

The second section discusses elliptic curves over finite fields, which hinges on *Hasse's theorem* to explain *Schoof's algorithm* for counting rational points. This in turn paves the path for applications in the last section, as well as an alternative method of counting rational points in the following section. Proofs are mostly given in full, except for an overly lengthy but elementary proof based on induction.

The third section discusses elliptic curves over the rationals, which can be split into two parts due to the *fundamental theorem of finitely generated abelian groups*. The *Nagell-Lutz theorem* and *reduction modulo prime* are two related ways to compute the *torsion subgroup*, while *Mordell's theorem* proves that the fundamental theorem indeed holds and provides a semi-workable method to compute the *rank*. Again, proofs are mostly given in full, except for an assumption made in the last part of Mordell's theorem.

The last section touches on some applications to classical arithmetic, including integer factorisation and primality proving, as well as the basics of contemporary cryptography, which could potentially be explored into if time permitted. There was originally an intention to cover complex elliptic curves in here instead, leading to a brief exposition of Fermat's last theorem, but was omitted due to lack of time.

The appendices include the aforementioned preliminaries, as well as proofs of two algorithms and listings of code. The proofs are placed here as they are deemed less relevant and too lengthy to be included in the main text. All code under code listings are in the functional *Haskell* programming language compiled by the *Glassgow Haskell Compiler*, which is markedly different from many implementations publicly available.

I will also present several remarks regarding the style of the report, which is an attempt to imitate typical lecture notes and textbooks. Definitions are all given in bold, while italics are reserved for less important terms that are undefined, all of which provided with adequate examples whenever possible. Theorems are important results and propositions those less important, while lemmas serve as intermediate checkpoints to theorems and propositions. All of these are provided immediate proofs after their statements, or postponed for later as *Proof of* statement. Remarks are largely irrelevant to the flow of the main discussion and can be disregarded, but are included for interesting points, which may include previously undefined terms.

In terms of notation, most of the symbols I have used are those found in books, such as $\mathbb{F}_p$, $\mathbb{Z}$, or $\mathbb{Q}$, and should be unambiguous. While there are unfortunate cases of equivalent symbols being used to mean completely different objects due to limitations of the English and Greek alphabet system, I have tried to minimise these or make them clear from context. An example being $f, g, h$ being used for general functions, while homomorphisms are always denoted $\phi, \psi, \chi$ or their variants. In examples like the following,

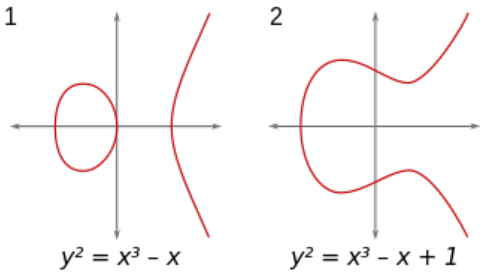
$$f(x, y) = xg(y) + yh(x), \qquad g \in F[y], \qquad h \in F[x],$$

$g$ and $h$ are always existentially quantified, while $f$ and $F$ are initially fixed or explicitly universally quantified. A function $f'$ will always be distinct, but possibly related, to the function $f$, while differentiation with respect to a variable $x$ will always be denoted $d/dx$ or $\partial/\partial x$. No distinction will be made between sums and *formal sums*, or derivatives and *formal derivatives*, as they are clear from the context of this report.

I would like to thank my supervisor Prof Johannes Nicaise for his support and guidance throughout the duration of this project. I had many doubts and questions early on, all of which he clarified with great detail.

# 1 Introduction

Informally, an elliptic curve is a cubic curve with no cusps, self-intersections, or isolated points, whose solutions are confined to a region of space topologically equivalent to a torus. It can represented by a cubic equation in two variables, with its coefficients being elements of a specified field. Two elliptic curves over the field of real numbers are illustrated below.




## 1.1 Definition

A formal definition is as follows.

**Definition** (Elliptic curve)**.** An **elliptic curve** over a perfect field $F$ is an ordered pair $(E, \mathcal{O}_E)$ such that $E$ is a smooth projective plane curve of genus one over $F$ and $\mathcal{O}_E \in E$ is an $F$-rational **base point**.

This definition uses several terms in other fields of mathematics, which are briefly covered in the appendices. In particular, one of the many characterisations of a perfect field is given in Appendix A.1, while several fundamental notions in projective and algebraic geometry such as projective planes and smoothness are laid out in Appendix A.2. Appendix A.3 defines a curve and the genus due to the *genus-degree formula*.

**Remark.** The genus in algebraic geometry is usually defined in general literature by the *Riemann-Roch theorem*, which does coincide with the topological definition.

As the report is a gentle introduction to elliptic curves, further delving into the vast world of algebraic geometry will be avoided, and so explicit formulae will be provided whenever possible. To this end, the various definitions in the appendix can be summarised in the following proposition.

**Proposition 1.1.1.** Let $(E, \mathcal{O}_E)$ be an elliptic curve over a perfect field $F$. Then:

1. $I(E) = \langle e \rangle$ for some homogeneous irreducible polynomial $e$ of three variables,
2. any point $P \in E$ has multiplicity $m_P(e) = 1$, and
3. $e$ have roots confined to a torus and is cubic.

*Proof.* This follows directly from the appendices. □

Thus an elliptic curve can be fully defined in terms of its defining polynomial, which would need to satisfy certain conditions. As per the appendix, an abuse of notation will be used to denote an elliptic curve $(E, \mathcal{O}_E)$ over $F$ *given* by a polynomial $e$, namely

$$E : e(X, Y, Z) = 0 \qquad \iff \qquad E : e(x, y) = 0,$$

which are respectively the homogenised and dehomogenised forms of a polynomial that can be used interchangeably. For the rest of this section, let $E : e(x, y) = 0$ and $E' : e'(x, y) = 0$ be two elliptic curves over a perfect field $F$ with algebraic closure $K = \overline{F}$. The notion of an isomorphism, as for any algebraic geometric structure, would be useful. This is captured in the following definition.

**Definition** (Isomorphism)**.** $(E, \mathcal{O}_E)$ and $(E', \mathcal{O}_{E'})$ are **isomorphic**, denoted by $(E, \mathcal{O}_E) \cong (E', \mathcal{O}_{E'})$, iff there is an isomorphism $\phi : E \to E'$ such that $\phi(\mathcal{O}_E) = \mathcal{O}_{E'}$.

**Remark.** Isomorphism defines an equivalence relation of elliptic curves, such that two elliptic curves from an equivalence class are indistinguishable.

Again, this abstract notion can be made explicit later by the defining polynomials of the elliptic curves.

## 1.2 Weierstrass equations

The definition of an elliptic curve boils down to its defining polynomial, which will be made explicit in this subsection. A family of curves related to elliptic curves will be defined beforehand.

**Definition** (Weierstrass curve)**.** A **Weierstrass curve** is a projective plane curve $W$ over $F$ *given* by the **Weierstrass equation**

$$W : w(x, y) = 0 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in F,$$

with associated quantities:

$$b_2 = a_1^2 + 4a_2, \qquad b_4 = a_1a_3 + 2a_4, \qquad b_6 = a_3^2 + 4a_6, \qquad b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

$$c_4 = b_2^2 - 24b_4, \qquad c_6 = 36b_2b_4 - b_2^3 - 216b_6, \qquad \Delta_W = 9b_2b_4b_6 - b_2^2b_8 - 8b_4^3 - 27b_6^2, \qquad j_W = c_4^3/\Delta_W.$$

It holds that $4b_8 = b_2b_6 - b_4^2$ and $1728\Delta_W = c_4^3 - c_6^2$. It can be easily verified that Weierstrass curves, with the additional condition of smoothness, would almost satisfy Proposition 1.1.1. The only remaining requirement is having an additional base point in its definition, which can be easily fixed as follows.

**Definition** (Point at infinity)**.** The **point at infinity** of is the point $\mathcal{O} = [0, 1, 0]$.

In contrast to general projective geometry, the *line at infinity* $L : l(X, Y, Z) = Z = 0$ intersects a Weierstrass curve only at $\mathcal{O}$, where $X = Z = 0$ and $Y \neq 0$. As such, any other point would have $Z \neq 0$ and can be treated as an affine point $(a, b)$. Now since $0, 1 \in F$, the point $\mathcal{O}$ is actually an $F$-rational point, and can be paired with a smooth Weierstrass curve $W$ to give an elliptic curve $(W, \mathcal{O})$. Conversely, any elliptic curve can also be explicitly given by a smooth Weierstrass curve through an isomorphism as follows.

**Proposition 1.2.1.** $(E, \mathcal{O}_E) \cong (W, \mathcal{O})$ for some smooth Weierstrass curve $W$ over $F$.

*Proof.* Omitted, see III.3.1a in [2]. □

There are even computerised algorithms to transform a general smooth projective plane cubic curve with a given arbitrary $F$-rational flex point, or an elliptic curve, into a Weierstrass curve with the $F$-rational point $\mathcal{O}$. The following algorithm summarises the process in [4] proven in the appendix.

**Algorithm 1.2.2** (Transformation of a cubic curve into Weierstrass form)**.** Input: a cubic curve $E$ over $F$ with an $F$-rational flex point $P \in E$. Output: $E$ in Weierstrass form.

1. Get the unique tangent line $L$ at $P$.
2. Find the intersection $L \cap E$ to get a point $Q \in L \setminus E$ distinct to $P$.
3. Write down an invertible matrix $M = \begin{pmatrix} Q & P & R \end{pmatrix}$, where $R \in \{[1, 0, 0], [0, 1, 0], [0, 0, 1]\}$.
4. Transform $[X, Y, Z] \mapsto M[X, Y, Z]^T$ to get a scaled Weierstrass equation.
5. Rescale $[X, Y, Z] \mapsto [X, Y, cZ]$ for some $c \in K^*$ to get a Weierstrass equation.

The following example illustrates an implementation of the algorithm.

**Example.** Let $E : e(X, Y, Z) = 0 : X^3 + Y^3 = Z^3$ be a smooth projective plane cubic curve over $\mathbb{R}$ with an $\mathbb{R}$-rational flex $P = [1, -1, 0] \in E$. Then the unique tangent at $P$ is

$$L : \begin{pmatrix} 1 \\ 1, 0, 0 \end{pmatrix} \left.\frac{\partial e}{\partial X}\right|_P (X - 1) + \begin{pmatrix} 1 \\ 0, 1, 0 \end{pmatrix} \left.\frac{\partial e}{\partial Y}\right|_P (Y + 1) + \begin{pmatrix} 1 \\ 0, 0, 1 \end{pmatrix} \left.\frac{\partial e}{\partial Z}\right|_P Z = 3(X + Y) = 0,$$

which intersects $E$ at $X^3 + (-X)^3 + Z^3 = 0$, or $Z = 0$. Hence $L \cap E = \{P\}$ and let $Q = [1, -1, 1] \in L \setminus E$. Then there is an invertible affine transformation matrix

$$M = \begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \qquad \implies \qquad M^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & -1 \\ 1 & 1 & 0 \end{pmatrix}.$$

such that the affine transformation $[X,Y,Z]\mapsto M\,[X,Y,Z]^T$ gives

$$(X+Y+Z)^3+(-X-Y)^3=X^3\qquad\implies 3Y^2Z+6XYZ+3YZ^2=X^3-3X^2Z-3XZ^2-Z^3.$$

Thus the affine transformation $[X,Y,Z]\mapsto\left[X,Y,\frac{1}{3}Z\right]$ gives a Weierstrass curve

$$E:Y^2Z+2XYZ+\tfrac{1}{3}YZ^2=X^3-X^2Z-\tfrac{1}{3}XZ^2-\tfrac{1}{27}Z^3.$$

This characterisation allows a smooth Weierstrass curve to act as an alternative definition for an elliptic curve, and will be done for ease of future discussions. For the rest of this subsection, let $E$ and $E'$ be respectively given by the two Weierstrass curves over $F$

$$W:w\,(x,y)=0:y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6,\qquad a_i\in F,$$

$$W':w'\,(x,y)=0:y^2+a_1'xy+a_3'y=x^3+a_2'x^2+a_4'x+a_6',\qquad a_i'\in F,$$

and write them interchangeably as an abuse of notation by

$$(E,\mathcal{O}_E)=E:e\,(x,y)=0\qquad\iff\qquad(W,\mathcal{O})=W:w\,(x,y)=0,$$

$$(E',\mathcal{O}_{E'})=E':e'\,(x,y)=0\qquad\iff\qquad(W',\mathcal{O})=W':w'\,(x,y)=0.$$

With these explicit equations at hand, the abstract notion of isomorphism between elliptic curves can now be made explicit by considering affine transformations of these equations, which is given below.

**Proposition 1.2.3.** $E\cong E'$ iff there is an affine transformation

$$(x,y)\mapsto\left(u^2x+r,u^3y+u^2sx+t\right),\qquad u\in K^*,\qquad r,s,t\in K$$

from $W$ to $W'$.

*Proof.* Omitted, see III.3.1b in [2]. □

**Remark.** This affine transformation also transforms the coefficients and quantities of $W$ and $W'$ by

$$a_1\mapsto\frac{a_1+2s}{u},\qquad a_2\mapsto\frac{a_2-sa_1+3r-s^2}{u^2},\qquad a_3\mapsto\frac{a_3+ra_1+2t}{u^3},$$

$$a_4\mapsto\frac{a_4-sa_3+2ra_2-(t+rs)\,a_1+3r^2-2st}{u^4},\qquad a_6\mapsto\frac{a_6+ra_4-ta_3+r^2a_2-rta_1+r^3-t^2}{u^6},$$

$$b_2\mapsto\frac{b_2+12r}{u^2},\qquad b_4\mapsto\frac{b_4+rb_2+6r^2}{u^4},\qquad b_6\mapsto\frac{b_6+2rb_4+r^2b_2+4r^3}{u^6},$$

$$b_8\mapsto\frac{b_8+3rb_6+3r^2b_4+r^3b_2+3r^4}{u^8},\qquad c_4\mapsto\frac{c_4}{u^4},\qquad c_6\mapsto\frac{c_6}{u^6},\qquad\Delta_W\mapsto\frac{\Delta_W}{u^{12}},\qquad j_W\mapsto j_W$$

which can be tediously verified.

Again, this will be treated as the definition of isomorphism between elliptic curves. Now in the original definition of a Weierstrass curve, it is given by a Weierstrass equation that is somewhat perverse. This *long* Weierstrass equation can in fact be greatly simplified, provided there are small restrictions on the characteristic of the underlying field.

**Proposition 1.2.4.** If $char\,(F)\neq 2$, then

$$E:y^2=x^3+Ax^2+Bx+C,\qquad A,B,C\in F.$$

If $char\,(F)\neq 3$ as well, then

$$E:y^2=x^3+Ax+B,\qquad A,B\in F.$$

*Proof.* Let $char\,(F) \neq 2$, then the affine transformation $(x, y) \mapsto \left(x, y - \frac{1}{2}(a_1x + a_3)\right)$ gives an isomorphism from $E$ to the curve given by the *medium* Weierstrass equation

$$y^2 = x^3 + Ax^2 + Bx + C, \qquad A = \tfrac{1}{4}b_2, \qquad B = \tfrac{1}{2}b_4, \qquad C = \tfrac{1}{4}b_6.$$

Let $char\,(F) \neq 3$ as well, then the affine transformation $(x, y) \mapsto \left(x - \frac{1}{12}b_2, y\right)$ gives an isomorphism from $E$ to the curve given by the *short* Weierstrass equation

$$y^2 = x^3 + Ax + B, \qquad A = -\tfrac{1}{48}c_4, \qquad B = -\tfrac{1}{864}c_6.$$

□

Medium and short Weierstrass equations greatly reduce the tedium when manipulating them, since there is a symmetry to the equation itself, giving two $y$ opposite in sign for each $x$. As there are only two characteristics that do not permit the affine transformation to a short Weierstrass equation, they will be disregarded for ease of future discussions. Hence always assume that $char\,(F) \notin \{2, 3\}$ and write the Weierstrass equations of $W$ and $W'$ as

$$W : w(x, y) = 0 : y^2 = x^3 + Ax + B, \qquad A, B \in F,$$
$$W' : w'(x, y) = 0 : y^2 = x^3 + A'x + B', \qquad A', B' \in F.$$

The following example illustrates the affine transformation to a short Weierstrass equation.

**Example.** Let

$$E : y^2 + 2xy + \tfrac{1}{3}y = x^3 - x^2 - \tfrac{1}{3}x - \tfrac{1}{27}$$

be the Weierstrass curve over $\mathbb{R}$ from the example above. Since $char\,(\mathbb{R}) = 0 \notin \{2, 3\}$, there is an affine transformation $(x, y) \mapsto \left(x, y - x - \frac{1}{6}\right)$ such that

$$\left(y - x - \tfrac{1}{6}\right)^2 + 2x\left(y - x - \tfrac{1}{6}\right) + \tfrac{1}{3}\left(y - x - \tfrac{1}{6}\right) = x^3 - x^2 - \tfrac{1}{3}x - \tfrac{1}{27} \qquad \implies \qquad y^2 = x^3 + \tfrac{1}{108},$$

which is a short Weierstrass equation.

Among the quantities associated with Weierstrass curves, most are used in defining the simplified Weierstrass equations, while the last two, the discriminant $\Delta_W$ and the $j$-invariant $j_W$, encode various properties of the curve itself. As only short Weierstrass equations are considered, these two quantities can be restated in an equivalent form in terms of the new coefficients. The discriminant is redefined as follows.

**Definition** (Discriminant)**.** The **discriminant** of $W$ is

$$\Delta_W = -16\left(4A^3 + 27B^2\right).$$

The discriminant is transformed as $\Delta_W \mapsto \Delta_W/u^{12}$ by the affine transformation in Proposition 1.2.3. It encodes behaviours at the singularities of Weierstrass curves, and whether they exist. The following proposition allows for an easy method of checking the smoothness of a Weierstrass curve.

**Proposition 1.2.5.** $W$ is smooth iff $\Delta_W \neq 0$.

*Proof.* Assume that $W$ is not smooth and $P = (a, b) \in W$ is singular. Then

$$0 = \left.\frac{\partial w}{\partial X}\right|_P = -3a^2 - A, \qquad 0 = \left.\frac{\partial w}{\partial Y}\right|_P = 2b, \qquad 0 = \left.\frac{\partial w}{\partial Z}\right|_P = b^2 - 2Aa - 3B.$$

Since $b = 0$ and $A = -3a^2$, it holds that $0 = 2Aa + 3B = -6a^3 + 3B$, so $B = 2a^3$. Hence $\Delta_W = -16\left(4\left(-3a^2\right)^3 + 27\left(2a^3\right)^2\right) = 0$. Conversely assume that $\Delta_W = -16\left(4A^3 + 27B^2\right) = 0$, such that the discriminant of $x^3 + Ax + B$ is $-\left(4A^3 + 27B^2\right) = 0$. Then there is a repeated root $x = a \in K$, so $P = (a, 0) \in W$ and

$$W : y^2 = (x - a)^2(x - a'), \qquad a' \in K.$$

Then

$$\left.\frac{\partial w}{\partial x}\right|_P = -2(a - a)(a - a') - (a - a)^2 = 0, \qquad \left.\frac{\partial w}{\partial y}\right|_P = 2(0) = 0.$$

Thus $P$ is singular and $W$ is not smooth. □

Hence $W$ is eligible as an elliptic curve iff $\Delta_W \neq 0$, and by the proof above, iff $x^3 + Ax + B$ has distinct factors. The following example illustrates the discriminant.

**Example.** Let $E$ be the Weierstrass curve over $\mathbb{R}$ from the example above. Then

$$\Delta_E = -16\left(4\left(0\right)^3 + 27\left(\tfrac{1}{108}\right)^2\right) = -\tfrac{1}{27} < 0,$$

so $E$ is smooth. Thus $E$ is an elliptic curve over $\mathbb{R}$.

The $j$-invariant, defined only for smooth Weierstrass curves where $\Delta_W \neq 0$, is redefined as follows.

**Definition** ($j$-invariant)**.** The **$j$-invariant** of $W$ is

$$j_W = 1728\left(\frac{4A^3}{4A^3 + 27B^2}\right).$$

The $j$-invariant is transformed as $j_W \mapsto j_W$ by the affine transformation in Proposition 1.2.3. It stays invariant between elliptic curves that are isomorphic, which gives its name. The following proposition allows for an alternative characterisation of an isomorphism.

**Proposition 1.2.6.** $E \cong E'$ iff $j_W = j_{W'}$.

*Proof.* Assume that $E \cong E'$, then the affine transformation maps $j_W$ to $j_W$, so $j_W = j_{W'}$. Conversely assume that $j_W = j_{W'}$, so

$$1728\left(\frac{4A^3}{4A^3 + 27B^2}\right) = 1728\left(\frac{4A'^3}{4A'^3 + 27B'^2}\right) \qquad \Longrightarrow \qquad A^3B'^2 = A'^3B^2.$$

If $A = 0$, then $B \neq 0$ and $A' = 0$. Then there is an affine transformation

$$(x, y) \mapsto \left(\sqrt[3]{\frac{B}{B'}}x, \sqrt{\frac{B}{B'}}y\right) \qquad \Longrightarrow \qquad \frac{B}{B'}y^2 = \frac{B}{B'}x^3 + A'\sqrt[3]{\frac{B}{B'}}x + B',$$

such that $y^2 = x^3 + B' = x^3 + A'x + B'$. If $B = 0$, then $A \neq 0$ and $B' = 0$. Then there is also an affine transformation

$$(x, y) \mapsto \left(\sqrt{\frac{A}{A'}}x, \sqrt[4]{\frac{A}{A'}^3}\, y\right) \qquad \Longrightarrow \qquad \sqrt{\frac{A}{A'}}^3 y^2 = \sqrt{\frac{A}{A'}}^3 x^3 + A'\sqrt{\frac{A}{A'}}x + B',$$

such that $y^2 = x^3 + A'x = x^3 + A'x + B'$. Otherwise $A \neq 0$ and $B \neq 0$, then there is an affine transformation from $W$ to $W'$ equal to the two affine transformations above. Thus $E \cong E'$. □

While $j$-invariant affine transformations preserve elliptic curves, this does not necessarily hold for their set of rational points. The following illustrates the $j$-invariant.

**Example.** Let $E$ be the elliptic curve over $\mathbb{R}$ from the example above. Then

$$j_E = -1728\left(\frac{4\left(0\right)^3}{4\left(0\right)^3 + 27\left(\frac{1}{108}\right)^2}\right) = 0.$$

Hence $E$ is isomorphic to any elliptic curve with zero $j$-invariant. Now let $E' : y^2 = x^3 + B$ for some $B \in \mathbb{R}$ such that $j_{E'} = 0$, then there is an affine transformation

$$(x, y) \mapsto \left(\frac{1}{3\sqrt[3]{2}^2 B}x, \frac{1}{2\sqrt{3}^3 B}y\right).$$

from $E$ to $E'$. Thus $E \cong E'$.

The definition and isomorphism classes of elliptic curves are now fully characterised.

**Remark.** There are alternate characterisations of elliptic curves by other families of curves, which will not be discussed here. One of these is the *Legendre form* of a Weierstrass curve, written as

$$E : y^2 = x\left(x - 1\right)\left(x - \lambda\right), \qquad \lambda \in K \setminus \{0, 1\}.$$

This is merely a transformation, but proves useful when studying elliptic curves over the reals.

## 1.3 Group law

An elliptic curve has an additional group theoretic property that makes it an *algebraic group*. This subsection provides a full definition of the additive group induced by an elliptic curve, as well as an attempt to prove that it is indeed one. The following lemma will be used in the definition of the addition operation.

**Lemma 1.3.1.** Let $P = [a, b, c] \in E$ and $Q = [a', b', c'] \in E$ be points. Then:

1. if $P \neq Q$, there is a unique line joining $P$ and $Q$ given by
$$L : (bc' - b'c) X + (a'c - ac') Y + (ab' - a'b) Z = 0,$$
2. if $P = Q$, there is a unique tangent at $P$ given by
$$L : \left(-3a^2 - Ac^2\right) X + 2bcY + \left(b^2 - 2Aac - 3Bc^2\right) Z = 0,$$
3. there is a unique third point $R \in E$ such that $L$ intersects $E$ at $P$, $Q$, and $R$.

*Proof.* Let $L : l(X, Y, Z) = 0$.

1. If $P \neq Q$, then
$$l(X, Y, Z) = \begin{pmatrix} X & Y & Z \end{pmatrix} \cdot \left( \begin{pmatrix} a & b & c \end{pmatrix} \times \begin{pmatrix} a' & b' & c' \end{pmatrix} \right).$$
2. If $P = Q$, then
$$l(X, Y, Z) = \begin{pmatrix} 1 \\ 1, 0, 0 \end{pmatrix} \left.\frac{\partial e}{\partial X}\right|_P (X - a) + \begin{pmatrix} 1 \\ 0, 1, 0 \end{pmatrix} \left.\frac{\partial e}{\partial Y}\right|_P (Y - b) + \begin{pmatrix} 1 \\ 0, 0, 1 \end{pmatrix} \left.\frac{\partial e}{\partial Z}\right|_P (Z - c).$$
3. Since $\deg(l) = 1$ and $\deg(\gcd(e, l)) = 0$, Bézout's theorem gives that $L$ intersects $E$ at three points up to multiplicity. Assume that $P = [a, b, c] \neq Q = [a', b', c']$. If $I_P(e, l) = 1$ and $I_Q(e, l) = 1$, then there is a unique third point $R \in E$ such that $R \neq P, Q$ and $I_R(e, l) = 1$. Otherwise $I_P(e, l) = 2$ or $I_Q(e, l) = 2$, then there is also a unique third point $R = P$ or $R = Q$ respectively. Otherwise assume that $P = Q = [a, b, c]$. Since $\{l\} = T_P(l) \in T_P(e)$, it holds that $I_P(e, l) > m_P(e) m_P(l) = 1$. If $I_P(e, l) = 2$, then there is a unique third point $R \in E$ such that $R \neq P$ and $I_R(e, l) = 1$. Otherwise $I_P(e, l) = 3$, then there is also a unique third point $R = P$.

□

The following example illustrates the unique lines and tangents above.

**Example.** Let $E : y^2 = x^3 + 2x + 1$ be an elliptic curve over $\mathbb{R}$ with points $P = (0, -1) \in E$ and $Q = (1, 2) \in E$. Then the unique line joining $P$ and $Q$ is $L : y = 3x - 1$, while the tangent at $P$ is $L_P : y = -x - 1$, and the tangent at $Q$ is $L_Q : y = \frac{5}{4}x + \frac{3}{4}$.

Instead of defining the addition operation right away, it is clearer to define an intermediate operation with the above lemma as follows.

**Definition** $(*)$**.** $* : E \times E \to E$ is defined by $P * Q = R$, where $R$ is the unique third point in Lemma 1.3.1.

The addition operation can then be defined immediately in terms of this intermediate operation, which are both symmetric and hence commutative.

**Definition** $(+)$**.** $+ : E \times E \to E$ is defined by $P + Q = (P * Q) * \mathcal{O}$.

This definition is chosen carefully so as to make a group law possible. While it might be slightly convoluted, there is an easy geometrical interpretation. While $P * Q \in E$ is simply the unique third intersection point of two points $P \in E$ and $Q \in E$, reflecting it along the horizontal axis gives $P + Q$. This motivates writing out several explicit formulae relating the affine coordinates of $P$, $Q$ and $P + Q$, which will allow equation manipulations in later sections. The following algorithm summarises the explicit formulae for $+$, which are proven in the appendix.

**Algorithm 1.3.2** (Group law explicit formulae)**.** Input: points $P, Q \in E$. Output: $P + Q$.

$$P + Q = \begin{cases} R & P = (a, b)\,,\ Q = (a', b')\,,\ a \neq a' \\ S & P = Q = (a, b)\,,\ b \neq 0 \\ P & Q = \mathcal{O} \\ \mathcal{O} & P = Q = (a, 0) \end{cases},$$

where

$$R = \left(\frac{(A + aa')(a + a') + 2(B - bb')}{(a - a')^2}, \frac{\left(Ab' - a'^2b\right)(3a + a') + \left(a^2b' - Ab\right)(a + 3a') - 4B(b - b')}{(a - a')^3}\right),$$

$$S = \left(\frac{a^4 - 2Aa^2 - 8Ba + A^2}{4b^2}, \frac{a^6 + 5Aa^4 + 20Ba^3 - 5A^2a^2 - 4ABa - A^3 - 8B^2}{8b^3}\right).$$

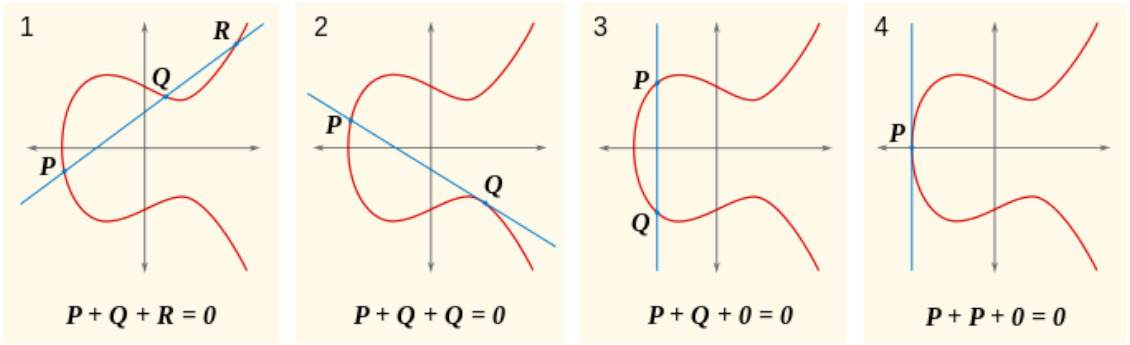
The first case is referred to as the *addition formula*, while the second case is referred to as the *duplication formula*. The last two cases allows the definition of a negation operation used for inverses in the group law. This is referred to as the *negation formula*, where $-\mathcal{O} = \mathcal{O}$ and $-(a, b) = (a, -b)$. Now the group law explicit formulae for characteristic two and three are more complicated and given in full under code listings in the appendix. The following example illustrates an implementation of the algorithm in the appendix.

**Example.** Let $E$ be the elliptic curve over $\mathbb{R}$ and let $L$, $L_P$, $L_Q$ be the lines for the points $P, Q \in E$ from the example above. Then $L$ intersects $E$ at $(3x - 1)^2 = x^3 + 2x + 1$, or $x(x - 1)(x - 8) = 0$. Hence $P * Q = (8, 23)$, so $P + Q = (8, -23)$. Similarly $L_P$ intersects $E$ at $(-x - 1)^2 = x^3 + 2x + 1$, or $x^2(x - 1) = 0$, while $L_Q$ intersects $E$ at $\left(\frac{5}{4}x + \frac{3}{4}\right)^2 = x^3 + 2x + 1$, or $(x - 1)^2(16x + 7) = 0$. Thus $P * P = (1, -2)$ and $Q * Q = (-7/16, 13/64)$, so $P + P = (1, 2)$ and $Q + Q = (-7/16, -13/64)$.

An alternative formulation for $+$ is such that three points $P, Q, R \in E$ are collinear iff

$$P + Q + R = P + (Q + R) = (P + Q) + R = \mathcal{O}.$$

This formulation will help in proving that certain maps obey some property later, but also allows for a pictorial description for $*$. As per the notation in the appendix: the first pane describes $(*)_2$; the second pane describes $(*)_3$; the third pane describes $(*)_1$ and $(*)_5$; the fourth pane describes $(*)_4$; the unillustrated line at infinity describes $(*)_6$.



The group structure of an elliptic curve with respect to $+$ can now be stated in the following theorem.

**Theorem 1.3.3** (Group law)**.** $(E, \mathcal{O}, +)$ is an abelian group.

As full proofs for associativity such as in III.3.4 of [2] require further prerequisites on algebraic curves, particularly on *divisors* and *differentials*, only the sketch of an alternative geometric proof is given, of which the special case of nine pairwise distinct points is assumed.

*Proof.* The unique right identity is $\mathcal{O} \in E$ and unique right inverses are given by the negation formula. Symmetry of $+$ gives the unique identity, unique right inverses, and commutativity. Associativity of $+$ can be checked with various methods, such as by tediously verifying cases of the explicit formulae in [5]. Alternatively, let $P, Q, R \in E$ be points, and let

- $L_1 : l_1(X, Y, Z) = 0$ be the line joining $P$, $Q$, and $P * Q = -(P + Q)$,
- $L_2 : l_2(X, Y, Z) = 0$ be the line joining $Q$, $R$, and $Q * R = -(Q + R)$,
- $L_3 : l_3(X, Y, Z) = 0$ be the line joining $P + Q$, $\mathcal{O}$, and $(P + Q) * \mathcal{O} = -(P + Q)$,
- $L_4 : l_4(X, Y, Z) = 0$ be the line joining $Q + R$, $\mathcal{O}$, and $(Q + R) * \mathcal{O} = -(Q + R)$,
- $L_5 : l_5(X, Y, Z) = 0$ be the line joining $P + Q$, $R$, and $(P + Q) * R = -((P + Q) + R)$, and
- $L_6 : l_6(X, Y, Z) = 0$ be the line joining $P$, $Q + R$, and $P * (Q + R) = -(P + (Q + R))$,

assuming that these points are pairwise distinct except for $-((P + Q) + R)$ and $-(P + (Q + R))$. Now let

$$C_1 : (l_1 l_4 l_5)(X, Y, Z) = 0, \qquad C_2 : (l_2 l_3 l_6)(X, Y, Z) = 0,$$

be cubics such that

$$I = \{\mathcal{O}, P, Q, R, P + Q, Q + R, -(P + Q), -(Q + R)\} \subseteq C_1 \cap C_2.$$

Then Bézout's theorem gives that $E$, $C_1$, and $C_2$ pairwise intersect at nine points up to multiplicity. Hence

$$E \cap C_1 = I \cup \{-((P + Q) + R)\}, \qquad E \cap C_2 = I \cup \{-(P + (Q + R))\}, \qquad C_1 \cap C_2 = I \cup \{S\},$$

for some ninth point $S \in C_1 \cap C_2$. Since $I \subseteq E$, the Cayley-Bacharach theorem gives $S \in E$, so

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

Thus $(P + Q) + R = P + (Q + R)$. □

With an abelian group at hand, some group theoretic properties of an elliptic curve can be explored. In particular, restricting an elliptic curve onto its $F$-rational points retain the group structure.

**Proposition 1.3.4.** $(E(F), \mathcal{O}, +) \leq (E, \mathcal{O}, +)$.

*Proof.* Since $0, 1 \in F$, it holds that $\mathcal{O} \in E(F)$. Let $P, Q \in E(F)$ be points, then the explicit formulae give $-P, P + Q \in E(F)$. Thus $(E(F), \mathcal{O}, +) \leq (E, \mathcal{O}, +)$. □

Additionally, the $n$-torsion points of an elliptic curve also form a group, provided $\mathcal{O}$ is included. The following example illustrates the structure of the 2-torsion subgroup.

**Example.** Let $P = (a, b) \in E[2]$, then $b = -b = 0$. Since $x^3 + Ax + B = 0$ has three distinct solutions, there are three distinct points $P_1 = (a_1, 0)$, $P_2 = (a_2, 0)$, and $P_3 = (a_3, 0)$ in $E[2]$. Thus $(E[2], \mathcal{O}, +) = (\{\mathcal{O}, P_1, P_2, P_3\}, \mathcal{O}, +) \cong \left(\mathbb{Z}_2^2, 0, +\right)$.

Hence $b = 0$ iff $ord(a, b) = 2$.

**Remark.** In fact, the $n$-torsion points of $E$ form a subgroup $E[n]$ of $E$, such that $(E[p], \mathcal{O}, +) \cong \left(\mathbb{Z}_p^2, 0, +\right)$ if $char(F) \nmid p$, and either $(E[p^e], \mathcal{O}, +) \cong (\{0\}, 0, +)$ or $(E[p^e], \mathcal{O}, +) \cong (\mathbb{Z}_{p^e}, 0, +)$ for all $e \in \mathbb{Z}_{>0}$ if $char(F) \mid p$.

## 1.4 Isogenies

Prior to this section, the only maps between elliptic curves that have been defined were affine transformations. Now that the group law is defined, group homomorphisms can also be considered. However, a slightly different approach to this will be taken with the following definition, noting that morphisms of curves are either constant or surjective.

**Definition** (Isogeny)**.** An **isogeny** from $E$ to $E'$ is a surjective morphism $\phi : E \to E'$ such that $\phi(\mathcal{O}) = \mathcal{O}$.

As isomorphisms are defined as invertible morphisms that preserve the point at infinity, they are isogenies as well. Now despite the simple condition, isogenies are actually group homomorphisms, which also preserve the point at infinity. The following proposition then gives an equivalent definition.

**Proposition 1.4.1.** Let $\phi : E \to E'$ be an isogeny. Then $\phi$ is a group homomorphism.

*Proof.* Omitted, see III.4.8 in [2]. □

The following is a typical example of an isogeny.

**Example.** The *multiplication by $n$ map* $[n] : E \to E$ defined by $[n](P) = nP$ is an isogeny such that $Ker([n]) = E[n]$.

Let $\phi : E \to E'$ be an isogeny. While isomorphisms are easily characterised by $j$-invariant affine transformations, the smaller restriction on isogenies allow for a wider range of coordinate transformations that still obey the group homomorphism property. In particular, rational functions that define isogenies can be characterised by the following lemma.

**Lemma 1.4.2.** Let $f \in F(E)$ be a rational function. Then

$$f(x, y) = \frac{f'(x) + f''(x)\, y}{f'''(x)}, \qquad f', f'' \in F[x], \qquad f''' \in F[x] \setminus \{0\}.$$

*Proof.* Let $f = g/h$ for some $g \in F[x, y]$ and some $h \in F[x, y] \setminus \{0\}$. Then $g(x, y) = \sum_{i=0}^{n} g_i(x)\, y^i$ for some $g_i \in F[x]$, some $h_i \in F[x] \setminus \{0\}$, and some $n, m \in \mathbb{Z}_{\geq 0}$, so:

$$\begin{aligned} g(x, y) &= \sum_{i=0}^{n} g_i(x)\, y^i = \sum_{i=0}^{n/2} g_{2i}(x)\, y^{2i} + \sum_{i=0}^{n/2} g_{2i+1}(x)\, y^{2i+1} \\ &= \sum_{i=0}^{n/2} g_{2i}(x) \left(x^3 + Ax + B\right)^i + \sum_{i=0}^{n/2} g_{2i+1}(x) \left(x^3 + Ax + B\right)^i y \\ &= g'(x) + g''(x)\, y, \qquad g', g'' \in F[x]. \end{aligned}$$

Similarly $h(x, y) = h'(x) + h''(x)\, y$ for some $h', h'' \in F[x]$. Thus

$$\begin{aligned} f(x, y) = \frac{g(x, y)}{h(x, y)} &= \frac{g'(x) + g''(x)\, y}{h'(x) + h''(x)\, y} = \frac{(g'(x) + g''(x)\, y)(h'(x) - h''(x)\, y)}{(h'(x) + h''(x)\, y)(h'(x) - h''(x)\, y)} \\ &= \frac{g'(x) h'(x) - g''(x) h''(x)\, y^2 - g'(x) h''(x)\, y + g''(x) h'(x)\, y}{h'(x)^2 - h''(x)^2\, y^2} \\ &= \frac{g'(x) h'(x) - g''(x) h''(x) \left(x^3 + Ax + B\right) - g'(x) h''(x)\, y + g''(x) h'(x)\, y}{h'(x)^2 - h''(x)^2 (x^3 + Ax + B)} \\ &= \frac{f'(x) + f''(x)\, y}{f'''(x)}, \qquad f, f' \in F[x], \qquad f'' \in F[x] \setminus \{0\}. \end{aligned}$$

□

An entire isogeny can now be characterised similarly, noting the group homomorphism property. The following proposition gives the explicit *standard form* of an isogeny, defined in terms of its image.

**Proposition 1.4.3.** Let $P = (a, b) \in E \setminus Ker(\phi)$ be a point. Then

$$\phi(P) = \left(\frac{r(a)}{s(a)}, \frac{u(a)}{v(a)}b\right) \qquad r, u \in F[x], \qquad s, v \in F[x] \setminus \{0\},$$

such that $\gcd(r, s) = \gcd(u, v) = 1$.

*Proof.* Let $\phi = [\phi_x, \phi_y, \phi_z]$ for some $\phi_x, \phi_y, \phi_z \in F(E)$. Since $\phi(P) \neq \mathcal{O}$, it holds that $\phi_z(P) \neq 0$, so

$$\phi(P) = [\phi_x(P), \phi_y(P), \phi_z(P)] = \left(\frac{\phi_x(P)}{\phi_z(P)}, \frac{\phi_y(P)}{\phi_z(P)}\right).$$

Then $\phi_x(P)/\phi_z(P), \phi_y(P)/\phi_z(P) \in F(E)$ are rational functions, so

$$\frac{\phi_x(P)}{\phi_z(P)} = \frac{\psi(a) + \psi'(a)b}{\psi''(a)}, \qquad \frac{\phi_y(P)}{\phi_z(P)} = \frac{\chi(a) + \chi'(a)b}{\chi''(a)}, \qquad \psi, \psi', \chi, \chi' \in F[x], \qquad \psi'', \chi'' \in F[x] \setminus \{0\}.$$

Since $\phi(-P) = -\phi(P)$,

$$\left(\frac{\psi(a) + \psi'(a)(-b)}{\psi''(a)}, \frac{\chi(a) + \chi'(a)(-b)}{\chi''(a)}\right) = \phi(-P) = -\phi(P) = \left(\frac{\psi(a) + \psi'(a)b}{\psi''(a)}, -\frac{\chi(a) + \chi'(a)b}{\chi''(a)}\right).$$

Hence $\psi'(a) = \chi(a) = 0$. Now let $g = \gcd(\psi, \psi'')$ and $g' = \gcd(\chi', \chi'')$. Thus let

$$r = \frac{\psi}{g}, u = \frac{\chi'}{g'} \in F[x], \qquad s = \frac{\psi''}{g}, v = \frac{\chi''}{g'} \in F[x] \setminus \{0\},$$

such that $\gcd(r, s) = \gcd(u, v) = 1$. □

In the above proof, the assumption that a point $P \in E$ is not in the kernel allows for the isogeny to be scaled appropriately. If $P$ is in the kernel, it would be mapped to the point at infinity, which would mean that $\phi_z$, and hence $s$ or $v$, is zero. With this in mind, an abuse of notation allows for the standard form to be written as

$$\phi(x, y) = \left(\frac{r(x)}{s(x)}, \frac{u(x)}{v(x)}y\right), \qquad r, s, u, v \in F[x], \qquad \gcd(r, s) = \gcd(u, v) = 1,$$

remembering that $\phi(\mathcal{O}) = \mathcal{O}$, and $\phi(a, b) = \mathcal{O}$ whenever $s(a) = 0$ or $v(a) = 0$ for any point $(a, b) \in E$. The following example rewrites the multiplication by two map with the familiar duplication formula.

**Example.** By the duplication formula,

$$\begin{aligned}[2](x, y) &= \left(\frac{x^4 - 2Ax^2 - 8Bx + A^2}{4y^2}, \frac{x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2}{8y^3}\right) \\ &= \left(\frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}, \frac{x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2}{8(x^3 + Ax + B)^2}y\right),\end{aligned}$$

which is in standard form. Then $[2](a, b) = \mathcal{O}$ iff $b^2 = a^3 + Aa + B = 0$ for any point $(a, b) \in E$.

There are also two useful notions of an isogeny, the first of which is its degree.

**Definition** (Isogeny degree)**.** The **degree** of $\phi$ is $\deg(\phi) = \max\{\deg(r), \deg(s)\}$.

The degree of the constant morphism, while not an isogeny, is defined to be zero. The degrees of two trivial isogenies are given in the following example.

**Example.** The identity isogeny, or the multiplication by one map $[1]$ has degree $\deg([1]) = \max\{1, 1\} = 1$. Similarly, the multiplication by negative one map $[-1]$ also has degree $\deg([-1]) = 1$.

The second invariant notion of an isogeny is its separability.

**Definition** (Separable isogeny)**.** $\phi$ is **separable** iff $d(r/s)/dx \neq 0$.

**Remark.** The isogeny $\phi$ induces an injection $\phi^* : F(E') \to F(E)$ of function fields. Its separability is equivalently formulated as that of $F(E)/\phi^* F(E')$, which reflects the definition of a separable extension.

The following example of the multiplication by two map illustrates these two notions.

**Example.** $[2]$ has degree $\deg([2]) = \max\{4,3\} = 4$ and is separable since

$$\frac{d}{dx}\left(\frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}\right) = \frac{x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2}{4(x^3 + Ax + B)^2} \neq 0.$$

Separability always holds in $char(F) = 0$, but there are inseparable isogenies in $char(F) = p$ for some prime $p \in \mathbb{Z}_{>0}$. More on separable isogenies will be discussed in a later section. Now since $+$ is a morphism, the set of all isogenies between $E$ and $E'$, together with the constant morphism, forms an abelian group $Hom(E, E')$ under the operation

$$(\phi + \psi)(P) = \phi(P) + \psi(P).$$

Isogenies in the group can also compose to form a ring when $E = E'$ in the following definition.

**Definition** (Endomorphism)**.** $\phi$ is an **endomorphism** of $E$ iff $E = E'$. The **endomorphism ring** $End(E)$ of $E$ is the ring of all endomorphisms of $E$ with respect to $+$ and $\circ$, where

$$(\phi \circ \psi) = \phi(\psi(P)).$$

The following example gives an endomorphism of elliptic curves over fields of non-zero characteristic that is of particular interest.

**Example.** Let $F = \mathbb{F}_p$ for some prime $p \in \mathbb{Z}_{>0}$. Then the *Frobenius endomorphism* $Fr : E \to E$ defined by $Fr(x, y) = (x^p, y^p)$ is an inseparable endomorphism with degree $\deg(Fr) = p$.

The Frobenius endomorphism will be formally defined in a later section. On a final note, endomorphisms with inverses also form a multiplicative subgroup.

**Definition** (Automorphism)**.** $\phi$ is an **automorphism** of $E$ iff it is an endomorphism and an isomorphism. The **automorphism group** $Aut(E)$ is the group of all automorphisms of $E$.

Unlike the endomorphism ring, the automorphism group of an elliptic curve is easily characterised.

**Proposition 1.4.4.**

$$Aut(E) \cong \begin{cases} \mathbb{Z}_6 & j_E = 0 \\ \mathbb{Z}_4 & j_E = 1728 \\ \mathbb{Z}_2 & j_E \notin \{0, 1728\} \end{cases}.$$

*Proof.* Let $\phi \in Aut(E)$. Then $\phi$ induces a $j$-invariant affine transformation

$$(x, y) \mapsto \left(u^2 x + r, u^3 y + u^2 s x + t\right), \qquad u \in K^*, \qquad r, s, t \in K$$

from $W$ to itself. Since $\phi$ is an automorphism, it holds that $r = s = t = 0$, and $A = A/u^4$ and $B = B/u^6$. If $j_E = 0$, then $A = 0$ and $B \neq 0$, so $u^6 = 1$. Hence $u$ is a sixth root of unity and $Aut(E) \cong \mathbb{Z}_6$. If $j_E = 1728$, then $A \neq 0$ and $B = 0$, so $u^4 = 1$. Hence $u$ is a fourth root of unity and $Aut(E) \cong \mathbb{Z}_4$. Otherwise $j_E \notin \{0, 1728\}$, then $A \neq 0$ and $B \neq 0$, so $u^6 = 1$ and $u^4 = 1$. Hence $u^2 = 1$ and $u$ is a second root of unity. Thus $Aut(E) \cong \mathbb{Z}_2$. □

**Remark.** If $char(F) \in \{2, 3\}$, then the above list of cases for $Aut(E)$ with $j_E = 0, 1728$ is not exhaustive. In particular, if $char(F) = 2$, then $Aut(E) \cong \mathbb{Z}_4 \ltimes \mathbb{Z}_3$, otherwise $char(F) = 3$, then $Aut(E) \cong \mathbb{Z}_3 \ltimes Q_8$.

The above definitions are defined for $E(F)$ as well, and are written $Hom_F(E, E')$, $End_F(E)$, and $Aut_F(E)$ respectively.

# 2 Elliptic curves over finite fields

When studying elliptic curves over a field or a family of fields, an important question would be to determine the set of solutions existing in that field. For instance, it is desirable to count the rational solutions in that field, which would have far fetching applications in number theory and cryptography. For finite fields, there is a finite process to compute the rational points that would always work. The following example illustrates a naive approach for this.

**Example.** Let $E : y^2 = x^3 + x + 1$ be an elliptic curve over $\mathbb{F}_5$. Since there are five distinct values for $x \in \mathbb{F}_5 = \{0, 1, 2, 3, 4\}$, computing $x^3 + x + 1$ for each value of $x$ and checking if it is a quadratic residue $y^2$ in $\mathbb{F}_5$ gives the following

- If $x = 0$, then $y^2 = x^3 + x + 1 = 1 = 1^2 = 4^2$, so $y = 1$ or $y = 4$.
- If $x = 1$, then $y^2 = x^3 + x + 1 = 3$ is not a quadratic residue.
- If $x = 2$, then $y^2 = x^3 + x + 1 = 1 = 1^2 = 4^2$, so $y = 1$ or $y = 4$.
- If $x = 3$, then $y^2 = x^3 + x + 1 = 1 = 1^2 = 4^2$, so $y = 1$ or $y = 4$.
- If $x = 4$, then $y^2 = x^3 + x + 1 = 4 = 2^2 = 3^2$, so $y = 2$ or $y = 3$.

Since $\mathcal{O} \in E(\mathbb{F}_5)$, there are exactly nine $\mathbb{F}_5$-rational points

$$E(\mathbb{F}_5) = \{\mathcal{O}, (0,1), (0,4), (2,1), (2,4), (3,1), (3,4), (4,2), (4,3)\}.$$

Hence $E(\mathbb{F}_5) \cong \mathbb{Z}_3^2$ or $E(\mathbb{F}_5) \cong \mathbb{Z}_9$. Now Lagrange's theorem gives that $ord(P) = 3$ or $ord(P) = 9$ for any non-zero point $P \in E(\mathbb{F}_5)$. Let $P = (0,1) \in E(\mathbb{F}_5)$. By the addition and duplication formulae, it holds that $3P = (2,1)$ and $9P = \mathcal{O}$, so it has order $ord(P) = 9$ and is a generator of $E(\mathbb{F}_5)$. Thus $E(\mathbb{F}_5) \cong \mathbb{Z}_9$.

This finite process is straightforward in the sense that it always terminates. However, as it runs with an asymptotic time complexity of $O(q)$ for a finite field $\mathbb{F}_q$, the approach becomes rather intractable for large prime powers $q \in \mathbb{Z}_{>0}$. This section will attempt to develop several techniques to compute $E(\mathbb{F}_q)$, or more specifically $|E(\mathbb{F}_q)|$, which will span the next few subsections. Now let $E$ be an elliptic curve over the perfect field $F = \mathbb{F}_q = \mathbb{F}_{p^e}$ for some prime $p \in \mathbb{Z}_{>0} \setminus \{2, 3\}$ and some $e \in \mathbb{Z}_{>0}$, given by the Weierstrass curve

$$E : y^2 = x^3 + Ax + B, \qquad A, B \in F,$$

with the group of rational points $E(F) = (E(F), \mathcal{O}, +)$.

## 2.1 Hasse's theorem: inseparable isogenies

The following theorem bounds the maximum cardinality of the group of rational points.

**Theorem 2.1.1** (Hasse)**.** $|E(F)| = q - t + 1$ for some *trace* $t \in \mathbb{Z}$ such that $|t| \leq 2\sqrt{q}$.

**Remark.** This is a special case of the Hasse-Weil theorem, which states that $|C(F)| = q - t + 1$ for some $|t| \leq 2g\sqrt{q}$ for any projective algebraic curve $C$ over $F$ of genus $g$.

Proof of Hasse's theorem concerns the properties of separable and inseparable isogenies, which are given by separable and inseparable polynomials. The following lemma allows inseparable polynomials to be written in a reduced form.

**Lemma 2.1.2.** Let $f \in F[x]$ be an inseparable polynomial. Then $f(x) = g(x^p)$ for some $g \in F[x]$.

*Proof.* Let $f(x) = \sum_{i=0}^{n} a_i x^i = \sum_{a_i \neq 0} a_i x^{m_i}$ for some $a_i \in F$ and some $n, m_i \in \mathbb{Z}_{>0}$. Since $f$ is separable, it holds that $0 = df/dx = \sum_{a_i \neq 0} m_i a_i x^{m_i - 1}$. Then $m_i a_i = 0$ for each $a_i \neq 0$, so $p \mid m_i$ and $m_i = pk$ for some $k \in \mathbb{Z}_{\geq 0}$. Thus $f(x) = \sum_{a_i \neq 0} a_i (x^p)^k = g(x^p)$ for some $g \in F[x]$. □

The polynomial $g$ would then be of a smaller degree than $f$, which justifies why it is deemed as reduced. A similar argument allows inseparable isogenies to be reduced, so let $E'$ be another elliptic curve over $F$ given by the Weierstrass curve

$$E' : y^2 = x^3 + A'x + B', \qquad A', B' \in F,$$

and let $\phi : E \to E'$ be an isogeny. The following lemma again allows inseparable isogenies to be written in a reduced form.

**Lemma 2.1.3.** Let $\phi$ be inseparable. Then

$$\phi(x, y) = \left(\frac{r'(x^p)}{s'(x^p)}, \frac{u'(x^p)}{v'(x^p)} y^p\right), \qquad r', s', u', v' \in F[x].$$

*Proof.* Since $\phi$ is inseparable,

$$0 = \frac{d}{dx}\left(\frac{r}{s}\right) = \frac{1}{s^2}\left(\frac{dr}{dx}s - \frac{ds}{dx}r\right) \qquad \implies \qquad \frac{dr}{dx}s = \frac{ds}{dx}r.$$

Since $\gcd(r, s) = 1$, it holds that $r \mid dr/dx$. Since $\deg(dr/dx) < \deg(r)$, it also holds that $dr/dx = 0$, so $r$ is inseparable and $r(x) = r'(x^p)$ for some $r' \in F[x]$. Similarly $s$ is inseparable, so $ds/dx = 0$ and $s(x) = s'(x^p)$ for some $s' \in F[x]$. Now

$$\left(\frac{u}{v}y\right)^2 = \left(\frac{r}{s}\right)^3 + A'\frac{r}{s} + B' \qquad \implies \qquad u^2 s^3 y^2 = v^2 t, \qquad t = r^3 + A'rs^2 + B's^3.$$

Then $dr/dx = 0$ and $ds/dx = 0$ gives $dt/dx = 0$, which gives $d\left(u^2y^2/v^2\right)/dx = d\left(t/s^3\right)/dx = 0$. Hence $u(x)^2 y^2 = y'(x^p)$ and $v(x)^2 = v'(x^p)$ for some $y', v' \in F[x]$ similarly. Now since $y^2 = x^3 + Ax + B$ has distinct factors, let $y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ for some $\alpha_i \in K$. Then each $(x - \alpha_i)$ is a factor of $y'(x^p)$, so $(x^p - \alpha_i^p) = (x - \alpha_i)^p$ is also a factor of $y'(x^p)$ and of $u(x)y^2$. Hence $y'(x^p) = t'(x^p)\left(y^2\right)^p$ for some $t' \in F[x]$. Now any factor $(x - \alpha)$ of $u(x)$ is such that $(x - \alpha)^p = (x^p - \alpha^p)$ is a factor of $t'(x^p)$. Since $\gcd(p, 2) = 1$, it holds that $\left((x - \alpha)^p\right)^2$ is also a factor of $t'(x^p)$, so $t'(x^p) = u'(x^p)^2$ for some $u' \in F[x]$. Thus $u(x)^2 y^2 = u'(x^p)^2 (y^p)^2$ and

$$\phi(x, y) = \left(\frac{r(x)}{s(x)}, \frac{u(x)}{v(x)}y\right) = \left(\frac{r'(x^p)}{s'(x^p)}, \pm\frac{u'(x^p)}{v'(x^p)}y^p\right).$$

□

Now the above lemma might feel slightly arbitrary due to the presence of $x^p$ and $y^p$ in the isogeny. This brings the discussion to a particular endomorphism defined as follows, which would simplify the above expression.

**Definition** (Frobenius endomorphism)**.** The **Frobenius endomorphism** $Fr : E \to E$ is defined by $Fr(x, y) = (x^p, y^p)$ if $e = 1$. The $q$-th power Frobenius endomorphism $Fr_q : E \to E$ is defined by $Fr_q(x, y) = (x^q, y^q)$.

The Frobenius endomorphism is also injective by virtue of the field characteristic, and hence bijective, which allows for an inverse isogeny to be easily defined.

**Remark.** A remarkable equivalent characterisation of a perfect field is that the Frobenius endomorphism of a field with positive characteristic is an automorphism, which induces a similar property for isogenies defined over this field.

The above lemmas for inseparable $\phi$ can now be written in terms of the Frobenius endomorphism $\phi = \phi' \circ Fr$, where

$$\phi'(x, y) = \left(\frac{r'(x)}{s'(x)}, \frac{u'(x)}{v'(x)}y\right), \qquad r', s', u', v' \in F[x],$$

which is a reduced standard form of an isogeny. In fact, any isogeny can be written as the composition of a Frobenius endomorphism. The following proposition summarises the above lemmas nicely.

**Proposition 2.1.4.** $\phi = \phi_s \circ Fr^n$ for some separable isogeny $\phi_s : E \to E'$ and some $n \in \mathbb{Z}_{\geq 0}$.

*Proof.* If $\phi$ is separable, then let $\phi_s = \phi$ and $n = 0$. Otherwise $\phi = \phi_1 \circ Fr$ for some $\phi_1 : E \to E'$. If $\phi_i : E \to E'$ is inseparable, then $\phi_i = \phi_{i+1} \circ Fr^i$ for some $\phi_{i+1} : E \to E'$. Since $\deg(\phi)$ is finite, by induction, there is some $n \in \mathbb{Z}_{\geq 0}$ such that $n \leq \deg(\phi)$ and $\phi_n : E \to E'$ is separable. Thus let $\phi_s = \phi_n$. □

**Remark.** Since $F$ is a perfect field, the isogeny $\phi$ can also be written as $\phi = Fr^n \circ \phi'_s$ for some separable isogeny $\phi'_s : E \to E'$ such that $\deg(\phi_s) = \deg(\phi'_s)$. If $F$ is not a perfect field, the Frobenius endomorphism is not necessarily an automorphism, so $Im(Fr) \subseteq E$ and the domain of $\phi_s$ is only a subset of $E$.

Hence any isogeny can be decomposed as the unique composition of a separable isogeny and a Frobenius endomorphism, so $\phi$ will be written as

$$\phi = \phi_s \circ Fr^n, \qquad \phi_s \in F[E], \qquad n \in \mathbb{Z}_{\geq 0},$$

where $\phi_s$ is a separable isogeny. Two additional notions of degree of an isogeny can then be defined as follows.

**Definition** (Separable degree)**.** The **separable degree** of $\phi$ is $\deg_s(\phi) = \deg(\phi_s)$. The **inseparable degree** of $\phi$ is $\deg_i(\phi) = p^n$.

It is clear that the degree of an isogeny is related to these two degrees by

$$\deg(\phi) = \deg_s(\phi) \deg_i(\phi).$$

If an isogeny is separable, its decomposition to a Frobenius endomorphism is trivial, so its separable degree is equal to its degree and its inseparable degree is one.

**Remark.** An inseparable isogeny does not necessarily have its inseparable degree equal to its degree and its separable degree equal to one. If this is the case, then the isogeny is *purely inseparable*. However, purely inseparable isogenies are not always inseparable, as with the case for degree one isogenies, which are isomorphisms, with all three degree equal to one.

The following example illustrates the two additional notions of degree.

**Example.** $Fr$ has separable degree $\deg_s(Fr) = 1$ and inseparable degree $\deg_i(Fr) = p$, while $[2]$ has separable degree $\deg_s([2]) = \deg([2]) = 4$ and inseparable degree $\deg_i([2]) = 1$.

This digression leads to an important proposition relating the kernel and the separable degree of an isogeny as follows, which is crucial to the proof of Hasse's theorem.

**Proposition 2.1.5.** $|Ker(\phi)| = \deg_s(\phi)$.

*Proof.* Let

$$S_1 = \{(a,0) \in E'\} = E[2], \qquad S_2 = \{(0,b) \in E'\}, \qquad S_3 = \{(a,b) \in E' \mid \deg(r - as) < \deg(\phi_s)\},$$

$$S_4 = \left\{(a,b) \in E' \;\middle|\; \left(\frac{r}{s}\right)(a') = a,\ \frac{d}{dx}\left(\frac{r}{s}\right)(a') = 0,\ (a',b') \in E\right\}, \qquad S = S_1 \cup S_2 \cup S_3 \cup S_4.$$

Then $|S_1| \leq 3$ and $|S_2| \leq 2$ are finite. Since $\deg(\phi_s)$ is finite, it holds that $|S_3| \leq 2\deg(\phi_s)$ is also finite. Since $\phi_s$ is separable, it holds that $d(r/s)/dx \neq 0$, so $|S_4| \leq \deg(r)$ is also finite. Hence $S$ is finite and $E' \setminus S$ is non-empty. Now let $P = (a,b) \in E' \setminus S$ and $P' = (a',b') \in E$ be points, and let $\psi = r - as \in K[x]$ be such that $\deg(\psi) = \deg(\phi_s)$. Then $\phi_s(P') = P$ iff $(r/s)(a') = a$ and $(u/v)(a')\, b' = b$. Since $b \neq 0$ gives $u(a') \neq 0$, this also holds iff $\psi(a') = r(a') - as(a') = 0$ and $b' = (v/u)(a')\, b$. Hence $\left|\phi_s^{-1}(P)\right|$ is the number of distinct roots of $\psi$. Suppose for a contradiction that $a'$ is a repeated root of $\psi$. Then

$$0 = \psi(a') = r(a') - as(a'), \qquad 0 = \frac{d\psi}{dx}(a') = \frac{dr}{dx}(a') - a\frac{ds}{dx}(a'),$$

such that

$$\left(\frac{r}{s}\right)(a') = a, \qquad \frac{dr}{dx}(a')\, s(a') = \frac{ds}{dx}(a')\, r(a') \qquad \implies \qquad \frac{d}{dx}\left(\frac{r}{s}\right)(a') = 0,$$

so $P' \in S_4$, which is a contradiction. Hence $\psi$ splits over $K$ and $\left|\phi_s^{-1}(P)\right| = \deg(\psi)$. Since $\chi : Ker(\phi_s) \to \phi_s^{-1}(P)$ defined by $\chi(Q) = Q + P$ is a bijection, it holds that $|Ker(\phi_s)| = \left|\phi_s^{-1}(P)\right|$. Since $Fr$ is bijective, so are $Fr^n$ and $Fr^n|_{Ker(\phi)} : Ker(\phi) \to Ker(\phi_s)$, so $|Ker(\phi)| = |Ker(\phi_s)|$. Thus

$$|Ker(\phi)| = |Ker(\phi_s)| = \left|\phi_s^{-1}(P)\right| = \deg(\psi) = \deg(\phi_s) = \deg_s(\phi).$$

□

Motivated by the endomorphism ring, composition of isogenies with appropriate domains can be seen as multiplication. In particular, their degrees multiply out naturally in the following lemma.

**Lemma 2.1.6.** Let $E''$ be an elliptic curve over $F$ such that $\psi : E' \to E''$ is an isogeny. Then

$$\deg(\psi \circ \phi) = \deg(\psi)\deg(\phi), \qquad \deg_s(\psi \circ \phi) = \deg_s(\psi)\deg_s(\phi), \qquad \deg_i(\psi \circ \phi) = \deg_i(\psi)\deg_i(\phi).$$

*Proof.* Since $\phi$ and $\psi$ are surjective, so is $\psi \circ \phi$, so the first isomorphism theorem gives

$$\frac{E}{Ker(\phi)} \cong E', \qquad \frac{E'}{Ker(\psi)} \cong E'', \qquad \frac{E}{Ker(\psi \circ \phi)} \cong E'',$$

such that

$$|Ker(\psi \circ \phi)| = \frac{|E|}{|E''|} = \frac{|E'|\,|Ker(\phi)|}{|E'| / |Ker(\psi)|} = |Ker(\psi)|\,|Ker(\phi)|.$$

Hence $\deg_s(\psi \circ \phi) = \deg_s(\psi)\deg_s(\phi)$. Now let $\psi = \psi_s \circ Fr^m$ and $\psi \circ \phi = \chi_s \circ Fr^k$ for some isogenies $\psi_s : E' \to E''$ and $\chi_s : E \to E''$ and some $m, k \in \mathbb{Z}_{\geq 0}$. Then

$$\chi_s \circ Fr^k = \psi_s \circ Fr^m \circ \phi_s \circ Fr^n.$$

Since $\deg_s(Fr) = 1$, it holds that $\deg_s(Fr^m) = 1$, so

$$\deg_s(Fr^m \circ \phi_s) = \deg_s(Fr^m)\deg_s(\phi_s) = \deg_s(\phi_s).$$

Then $Fr^m \circ \phi_s = \chi_s' \circ Fr^m$ for some isogeny $\chi_s' : E \to E'$ such that $\deg(\phi_s) = \deg(\chi_s')$, so

$$\chi_s \circ Fr^k = \psi_s \circ \chi_s' \circ Fr^{n+m}.$$

Since $\psi_s \circ \chi_s'$ is separable, it holds that $k = n + m$. Hence $\deg_i(\psi \circ \phi) = \deg_i(\psi)\deg_i(\phi)$. Thus

$$\deg(\psi \circ \phi) = \deg_s(\psi)\deg_i(\psi)\deg_s(\phi)\deg_i(\phi) = \deg(\psi)\deg(\phi).$$

□

This paves the way to the proof of the following proposition on inseparable isogenies, which is also crucial to the proof of Hasse's theorem. Now let $\psi : E \to E'$ be an isogeny.

**Proposition 2.1.7.** Let $\phi$ and $\psi$ be inseparable, and let $E''$ and $E'''$ be elliptic curves over $F$ such that $\chi : E'' \to E$ and $\chi' : E' \to E'''$ are isogenies. Then $\phi \circ \chi$, $\chi' \circ \phi$, and $\phi - \psi$ are inseparable.

*Proof.* Since $\deg_i(\phi \circ \chi) = \deg_i(\phi)\deg_i(\chi) > 1$ and $\deg_i(\chi' \circ \phi) = \deg_i(\phi)\deg_i(\chi) > 1$, it holds that $\phi \circ \chi$ and $\chi' \circ \phi$ are inseparable. Now let $\phi = \phi_s \circ Fr^n$ and $\psi = \psi_s \circ Fr^m$ for some separable isogenies $\phi_s : E \to E'$ and $\psi_s : E \to E'$ and some $n, m \in \mathbb{Z}_{>0}$. Then

$$\phi - \psi = \phi_s \circ Fr^n - \psi_s \circ Fr^m = \left(\phi_s \circ Fr^{n-1} - \psi_s \circ Fr^{m-1}\right) \circ Fr.$$

Thus $\phi - \psi$ is inseparable. □

Hence adding a separable isogeny with an inseparable isogeny will give a separable isogeny. Returning to the initial motivation, letting $E = E' = E'' = E'''$ in the above results implies that the set of all inseparable endomorphisms of $E$ is an ideal of $End(E)$.

## 2.2 Hasse's theorem: quadratic forms

Now the *degree map* $\deg : Hom(E, E') \to \mathbb{Z}_{\geq 0}$ has a particular property that allows a form of the Cauchy-Schwarz inequality to be defined on it. This property can be defined with the aid of the following notion.

**Definition** (Bilinear pairing)**.** A pairing $b : G \times G \to F$ of an group $G$ is **bilinear** iff $b(x+y, z) = b(x, z) + b(y, z)$ and $b(x, y+z) = b(x, y) + b(x, z)$ for any $x, y, z \in G$.

In other words the pairing is linear in both components. A bilinear pairing can be defined in terms of the degree map, with the set of isogenies $Hom(E, E')$ as the abelian group, which has the following property.

**Definition** (Quadratic form)**.** A **quadratic form** is a map $d : A \to F$ of an abelian group $A$ such that $d(x) = d(-x)$ for any $x \in A$, and the **associated pairing** $b_d : A \times A \to F$ defined by

$$b_d(x, y) = \tfrac{1}{2}(d(x+y) - d(x) - d(y))$$

is bilinear.

The associated bilinear pairing is usually written $\langle \cdot, \cdot \rangle : A \times A \to F$ with context, and inherits all the definitions from linear algebra, such as the notions of being symmetric and positive definite.

**Remark.** Conversely, for any symmetric bilinear pairing $\langle \cdot, \cdot \rangle : A \times A \to F$, the map $d : A \to F$ defined by $d(x) = \langle x, x \rangle$ is a quadratic form, so notions related to symmetric bilinear pairings and quadratic forms are interchangeable, provided $char(F) \neq 2$.

Hence an aim would be to show that the degree map indeed is a positive definite quadratic form, as symmetry follows by definition. This could be done by proving a particular fundamental property that holds for all quadratic forms, which is given in the following theorem. Now denote $-\phi = [-1] \circ \phi$ and

$$\phi + \cdots + \phi = n\phi = [n] \circ \phi, \qquad \psi + \cdots + \psi = m\psi = [m] \circ \psi, \qquad n, m \in \mathbb{Z},$$

to ease the proofs below.

**Theorem 2.2.1** (Parallelogram law)**.** $\deg(\phi + \psi) + \deg(\phi - \psi) = 2\deg(\phi) + 2\deg(\psi)$.

*Proof.* If $\phi = 0$ or $\psi = 0$, then $\deg(\phi + \psi) + \deg(\phi - \psi) = 2\deg(\phi) + 2\deg(\psi)$ holds. If $\phi = \psi$ or $\phi = -\psi$, then

$$\deg(\phi + \psi) + \deg(\phi - \psi) = \deg(2\phi) = \deg([2])\deg(\phi) = 4\deg(\phi) = 2\deg(\phi) + 2\deg(\psi)$$

also holds. Otherwise let

$$\phi(x, y) = (w_1, z_1), \qquad \psi(x, y) = (w_2, z_2), \qquad (\phi + \psi)(x, y) = (w_3, z_3), \qquad (\phi - \psi)(x, y) = (w_4, z_4),$$

for each $w_i = r_i(x)/s_i(x)$ and $z_i = u_i(x)\, y/v_i(x)$ for some homogeneous polynomials $r_i, s_i, u_i, v_i \in F[x]$ such that each $\gcd(r_i, s_i) = \gcd(u_i, v_i) = 1$ and

$$\deg(\phi) = \deg(r_1) = \deg(s_1), \qquad \deg(\psi) = \deg(r_2) = \deg(s_2),$$

$$\deg(\phi + \psi) = \deg(r_3) = \deg(s_3), \qquad \deg(\phi - \psi) = \deg(r_4) = \deg(s_4).$$

By the addition formula,

$$w_3 = \frac{(A + w_1 w_2)(w_1 + w_2) + 2(B - z_1 z_2)}{(w_1 - w_2)^2}, \qquad w_4 = \frac{(A + w_1 w_2)(w_1 + w_2) + 2(B + z_1 z_2)}{(w_1 - w_2)^2}.$$

Adding these two equations gives $(w_3 + w_4)(w_1 - w_2)^2 = 2(A + w_1 w_2)(w_1 + w_2) + 4B$, so

$$\frac{r_3 s_4 + r_4 s_3}{s_3 s_4} = \frac{2(A s_1 s_2 + r_1 r_2)(r_1 s_2 + r_2 s_1) + 4B s_1^2 s_2^2}{(r_1 s_2 - r_2 s_1)^2}.$$

Hence let

$$R = r_3s_4 + r_4s_3, \qquad S = s_3s_4, \qquad U = 2\left(As_1s_2 + r_1r_2\right)\left(r_1s_2 + r_2s_1\right) + 4Bs_1^2s_2^2, \qquad V = \left(r_1s_2 - r_2s_1\right)^2.$$

Similarly multiplying these two equations gives

$$\begin{aligned} w_3w_4\left(w_1 - w_2\right)^4 &= \left(A + w_1w_2\right)^2\left(w_1 + w_2\right)^2 + 4B\left(A + w_1w_2\right)\left(w_1 + w_2\right) + 4B^2 - 4z_1^2z_2^2 \\ &= \left(A^2 + 2Aw_1w_2 + w_1^2w_2^2\right)\left(w_1^2 + 2w_1w_2 + w_2^2\right) + 4B\left(Aw_1 + Aw_2 + w_1^2w_2 + w_1w_2^2\right) \\ &\quad + 4B^2 - 4\left(w_1^3 + Aw_1 + B\right)\left(w_2^3 + Aw_2 + B\right) \\ &= A^2w_1^2 - 2A^2w_1w_2 + A^2w_2^2 - 4Bw_1^3 + 4Bw_1^2w_2 + 4Bw_1w_2^2 - 4Bw_2^3 \\ &\quad - 2Aw_1^3w_2 + 4Aw_1^2w_2^2 - 2Aw_1w_2^3 + w_1^4w_2^2 - 2w_1^3w_2^3 + w_1^2w_2^4 \\ &= A^2\left(w_1 - w_2\right)^2 - 4Bw_1^2\left(w_1 - w_2\right) + 4Bw_2^2\left(w_1 - w_2\right) \\ &\quad - 2Aw_1w_2\left(w_1 - w_2\right)^2 + w_1^2w_2^2\left(w_1 - w_2\right)^2 \\ &= \left(A^2 - 2Aw_1w_2 + w_1^2w_2^2\right)\left(w_1 - w_2\right)^2 - 4B\left(w_1^2 - w_2^2\right)\left(w_1 - w_2\right) \\ &= \left(A - w_1w_2\right)^2\left(w_1 - w_2\right)^2 - 4B\left(w_1 + w_2\right)\left(w_1 - w_2\right)^2, \end{aligned}$$

such that $w_3w_4\left(w_1 - w_2\right)^2 = \left(A - w_1w_2\right)^2 - 4B\left(w_1 + w_2\right)$, so

$$\frac{r_3r_4}{s_3s_4} = \frac{\left(As_1s_2 - r_1r_2\right)^2 - 4B\left(r_1s_2 + r_2s_1\right)s_1s_2}{\left(r_1s_2 - r_2s_1\right)^2}.$$

Hence also let

$$T = r_3r_4, \qquad W = \left(As_1s_2 - r_1r_2\right)^2 - 4B\left(r_1s_2 + r_2s_1\right)s_1s_2,$$

such that

$$\begin{aligned} \deg\left(R\right) = \deg\left(S\right) = \deg\left(T\right) &= \deg\left(\phi + \psi\right) + \deg\left(\phi - \psi\right), \\ \deg\left(U\right) = \deg\left(V\right) = \deg\left(W\right) &= 2\deg\left(\phi\right) + 2\deg\left(\psi\right). \end{aligned}$$

Suppose for a contradiction that $\gcd\left(R, S, T\right) \neq 1$, so $g \mid \gcd\left(R, S, T\right)$ for some irreducible homogeneous polynomial $g \in F\left[x\right]$. If $g \mid r_3$, then $g \nmid s_3$, so $g \mid s_4$ and $g \nmid r_4$ gives $g \nmid r_3s_4 + r_4s_3 = R$. Otherwise $g \nmid r_3$, then $g \mid r_4$, so $g \nmid s_4$ and $g \mid s_3$ also gives $g \nmid r_3s_4 + r_4s_3 = R$, which is a contradiction. Hence $\gcd\left(R, S, T\right) = 1$. Now let $g' = \gcd\left(U, V, W\right)$, so

$$U = g'U', \qquad V = g'V', \qquad W = g'W', \qquad U', V', W' \in F\left[x\right], \qquad \gcd\left(U', V', W'\right) = 1,$$

such that

$$\deg\left(U'\right) = \deg\left(V'\right) = \deg\left(W'\right) = \deg\left(U\right) - \deg\left(g'\right).$$

Combining the two equations from adding and multiplying gives a ratio

$$\left[R, S, T\right] = \left[\frac{R}{S}, 1, \frac{T}{S}\right] = \left[\frac{U}{V}, 1, \frac{W}{V}\right] = \left[U, V, W\right] = \left[g'U', g'V', g'W'\right] = \left[U', V', W'\right],$$

such that $R = U'$, $T = W'$, and $S = V'$. Hence

$$\deg\left(\phi + \psi\right) + \deg\left(\phi - \psi\right) = \deg\left(R\right) = \deg\left(U'\right) = \deg\left(U\right) - \deg\left(g'\right) \leq \deg\left(U\right) = 2\deg\left(\phi\right) + 2\deg\left(\psi\right).$$

Now replacing $\left(\phi, \psi\right) \mapsto \left(\phi + \psi, \psi + \phi\right)$ gives the converse

$$\begin{aligned} 2\deg\left(\phi + \psi\right) + 2\deg\left(\phi - \psi\right) &\geq \deg\left(\phi + \psi + \phi - \psi\right) + \deg\left(\phi + \psi - \phi + \psi\right) \\ &= \deg\left(\left[2\right]\right)\deg\left(\phi\right) + \deg\left(\left[2\right]\right)\deg\left(\psi\right) \\ &= 4\deg\left(\phi\right) + 4\deg\left(\psi\right), \end{aligned}$$

Thus $\deg\left(\phi + \psi\right) + \deg\left(\phi - \psi\right) = 2\deg\left(\phi\right) + 2\deg\left(\psi\right)$. □

An application of the parallelogram law would be a simple inductive proof of the following lemma, which has many other proofs.

**Lemma 2.2.2.** Let $n \in \mathbb{Z}$. Then $\deg([n]) = n^2$.

*Proof.* $\deg([0]) = 0$ and $\deg([1]) = 1$. Assume that $\deg([m]) = m^2$ for any $m \leq n$ for some $n \in \mathbb{Z}_{\geq 0}$. Then

$$\deg([n+1]) = 2\deg([n]) + 2\deg([1]) - \deg([n-1]) = 2n^2 + 2 - (n-1)^2 = n^2 + 2n + 1 = (n+1)^2.$$

Hence $\deg([n]) = n^2$ for any $n \in \mathbb{Z}_{\geq 0}$ by induction. Similarly $\deg([-n]) = \deg([-1])\deg([n]) = \deg([n])$ for any $n \in \mathbb{Z}_{\geq 0}$. Thus $\deg([n]) = n^2$ for any $n \in \mathbb{Z}$. □

In fact, the above lemma can be generalised for arbitrary isogenies, as follows.

**Lemma 2.2.3.** Let $n, m \in \mathbb{Z}$. Then $\deg(n\phi + m\psi) = n^2\deg(\phi) + 2nm\langle\phi, \psi\rangle + m^2\deg(\psi)$.

*Proof.* Since $\langle\phi, \phi\rangle = \frac{1}{2}(\deg(2\phi) - 2\deg(\phi)) = 2\deg(\phi) - \deg(\phi) = \deg(\phi)$, it holds that

$$\deg(n\phi + m\psi) = \langle n\phi + m\psi, n\phi + m\psi\rangle = n^2\deg(\phi) + 2nm\langle\phi, \psi\rangle + m^2\deg(\psi).$$

□

The initial aim can then be proven in the following lemma.

**Lemma 2.2.4.** $\deg : Hom(E, E') \to \mathbb{Z}_{\geq 0}$ is a positive definite quadratic form.

*Proof.* $\deg(-\phi) = \deg([-1])\deg(\phi) = \deg(\phi)$. Let $\chi : E \to E'$ be an isogeny. Since

$$\begin{aligned}\deg(\phi + \psi + \chi) &= 2\deg(\phi + \psi) + 2\deg(\chi) - \deg(\phi + \psi - \chi)\\ &= 2\deg(\phi + \psi) + 2\deg(\chi) - 2\deg(\phi - \chi) - 2\deg(\psi) + \deg(\phi - \psi - \chi)\\ &= 2\deg(\phi + \psi) + 2\deg(\chi) - 2\deg(\phi - \chi) - 2\deg(\psi)\\ &\quad + 2\deg(\psi + \chi) + 2\deg(\phi) - \deg(\phi + \psi + \chi),\end{aligned}$$

it holds that $\deg(\phi + \psi + \chi) = \deg(\phi + \psi) + \deg(\chi) - \deg(\phi - \chi) - \deg(\psi) + \deg(\psi + \chi) + \deg(\phi)$. Hence

$$\begin{aligned}\langle\phi + \psi, \chi\rangle &= \tfrac{1}{2}(\deg(\phi + \psi + \chi) - \deg(\phi + \psi) - \deg(\chi))\\ &= \tfrac{1}{2}(-\deg(\phi - \chi) - \deg(\psi) + \deg(\psi + \chi) + \deg(\phi))\\ &= \tfrac{1}{2}(-2\deg(\phi) - 2\deg(\chi) + \deg(\phi + \chi) - \deg(\psi) + \deg(\psi + \chi) + \deg(\phi))\\ &= \tfrac{1}{2}(\deg(\phi + \chi) - \deg(\phi) - \deg(\chi) + \deg(\psi + \chi) - \deg(\psi) - \deg(\chi)) = \langle\phi, \chi\rangle + \langle\psi, \chi\rangle.\end{aligned}$$

Similarly $\langle\phi, \psi + \chi\rangle = \langle\phi, \psi\rangle + \langle\phi, \chi\rangle$ by symmetry. Thus since $\deg(\phi) > 0$ for any $\phi \neq 0$ and $\deg(0) = 0$, it holds that deg is a positive definite quadratic form. □

Replacing the degree map with any map satisfying the parallelogram law also gives a quadratic form. The following variant of the Cauchy-Schwarz inequality generalises to quadratic forms similarly.

**Theorem 2.2.5** (Cauchy-Schwarz)**.** $\langle\phi, \psi\rangle^2 \leq \deg(\phi)\deg(\psi)$.

*Proof.* Let $n = -\langle\phi, \psi\rangle$ and $m = \deg(\phi)$. Then

$$0 \leq \langle\phi, \psi\rangle^2\deg(\phi) - 2\langle\phi, \psi\rangle^2\deg(\phi) + \deg(\phi)^2\deg(\psi) = \deg(\phi)\left(\deg(\phi)\deg(\psi) - \langle\phi, \psi\rangle^2\right).$$

Thus $\langle\phi, \psi\rangle^2 \leq \deg(\phi)\deg(\psi)$. □

Hasse's theorem can finally be proven.

*Proof of Theorem 2.1.1.* A point $P = [a, b, c] \in E(F)$ iff $a^q = a$, $b^q = b$, and $c^q = c$ by Fermat's little theorem, or $[a^q, b^q, c^q] = [a, b, c]$. This holds iff the $q$-th power Frobenius endomorphism $Fr_q : E \to E$ is such that $Fr_q(P) = P$, or $P \in Ker(Fr_q - [1])$. Hence $E(F) = Ker(Fr_q - [1])$. Since $[1]$ is separable and $Fr_q$ is inseparable with degree $\deg(Fr_q) = \deg_i(Fr_q) = q$, it holds that $Fr_q - [1]$ is separable, so

$$Ker(Fr_q - [1]) = \deg_s(Fr_q - [1]) = \deg(Fr_q - [1]) = \deg(Fr_q) - 2\langle Fr_q, [1]\rangle + \deg([1]) = q - 2\langle Fr_q, [1]\rangle + 1.$$

Then let $t = 2\langle Fr_q, [1]\rangle$, so Cauchy-Schwarz gives $t^2 = 4\langle Fr_q, 1\rangle^2 \leq 4\deg(Fr_q)\deg([1]) = 4q$. Thus $|E(F)| = q - t + 1$ for $|t| \leq 2\sqrt{q}$. □

## 2.3 Riemann hypothesis

Hasse's theorem, or more accurately the Hasse-Weil theorem, is also sometimes referred to as the *Riemann hypothesis* for smooth projective algebraic curves over finite fields. It has an alternative formulation that makes it analogous to the famous classical Riemann hypothesis, an open problem in number theory deemed worthy of being called one of the Millennium Prize Problems by the Clay Mathematics Institute with a monetary prize of a million dollars. The conjecture revolves around zeroes of the following complex function.

**Definition** (Riemann zeta function)**.** The Riemann zeta function $\zeta : \mathbb{C} \to \mathbb{C}$ is defined for any $\Re(s) > 1$ as the power series $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$, and extended to $\mathbb{C}$ by analytic continuation.

Riemann himself proved the analytic continuation, as well as a functional equation satisfied by the Riemann zeta function given by

$$\xi(s) = \xi(1-s), \qquad \xi(s) = \tfrac{1}{2}\sqrt{\pi}^{-s} s(s-1)\,\Gamma\left(\tfrac{1}{2}s\right)\zeta(s).$$

The conjecture is then formulated in [6] as follows.

**Conjecture 2.3.1** (Riemann)**.** Let $s \in \mathbb{C}$ be such that $s \notin -2\mathbb{Z}_{>0}$. If $\zeta(s) = 0$, then $\Re(s) = \frac{1}{2}$.

The connection to this still open problem can be seen via a powerful theorem known as the *Weil conjectures*, proposed by Weil and proven in steps later by himself, Dwork, Deligne, Grothendieck, and many others. The so-called conjectures also involve a related zeta function encoding the number of rational points of a smooth projective algebraic varieties variety, which is defined as follows.

**Definition** (Local zeta function)**.** The **local zeta function** of a projective algebraic variety $V$ over $F$ is the power series

$$Z_V(t) = \exp\left(\sum_{n=1}^{\infty} |V(F_n)| \frac{t^n}{n}\right), \qquad |V(F_n)| = \frac{1}{(n-1)!}\frac{d^n}{dt^n}\ln\left(Z_V(t)\right)\bigg|_{t=0}.$$

where $F_n = \mathbb{F}_{q^n}$.

The following example is a trivial application the local zeta function.

**Example.** Let $V(0)$ be the trivial projective algebraic variety over $F$. Then $|V(F_n)| = 1$ for any $n \in \mathbb{Z}_{>0}$, so

$$Z_V(t) = \exp\left(\sum_{n=1}^{\infty} \frac{t^n}{n}\right) = \exp\left(\ln\left(\frac{1}{1-t}\right)\right) = \frac{1}{1-t}.$$

His three conjectures are then formulated as follows, which are easily satisfied by the above example.

**Theorem 2.3.2** (Weil conjectures)**.** Let $V$ be a smooth projective algebraic variety over $F$ of dimension $n \in \mathbb{Z}_{\geq 0}$.

- Rationality. $Z_V(t) = P(t)/(1-t)(1-q^n t) \in \mathbb{Q}[t]$, where
$$P(t) = \prod_{i=1}^{2n-1} P_i(t)^{(-1)^{i+1}}, \qquad P_i \in \mathbb{Z}[t].$$
- Functional equation. Let $\epsilon \in \mathbb{Z}$ be the *Euler characteristic* of $V$. Then
$$Z_V\left(\frac{1}{q^n t}\right) = \pm\sqrt{q}^{n\epsilon} t^{\epsilon} Z_V(t).$$
- Riemann hypothesis. Let $S_i = \left\{\alpha \in \mathbb{C} \mid |\alpha| = \sqrt{q}^i\right\}$ and $P_i$ be as per above. Then each
$$P_i(t) = \prod_{\alpha \in S_i'} (1 - \alpha t),$$
over some $S_i' \subseteq S_i$ such that $P_i \in \mathbb{Z}(t)$.

*Proof.* Omitted, see [7], [8], and [9]. □

**Remark.** There is a fourth Weil conjecture on *Betti numbers* that states if $V$ is a *reduction modulo* $q$ of a smooth projective algebraic variety $W$ over a number field, then $\deg(P_i)$ is the $i^{th}$ topological Betti number of $W$ for each $P_i$.

In the special case where $V$ is a smooth projective algebraic curve $C$ of genus $g_C$, its dimension is $n = 1$ and its Euler characteristic is $\epsilon = 2 - 2g_C$, which greatly simplifies Theorem 2.3.2. The following is a formulation for the elliptic curve $E$ of genus one.

**Theorem 2.3.3** (Weil conjectures for elliptic curves)**.** $Z_E$ satisfies the following properties.

- Rationality. $Z_E(t) = P(t) / (1-t)(1-qt) \in \mathbb{Q}(t)$ for some $P \in \mathbb{Z}(t)$.
- Functional equation. $Z_E(1/qt) = \pm Z_E(t)$.
- Riemann hypothesis. $P(t) = \prod_\alpha (1-\alpha t)$ for some $\alpha \in \mathbb{C}$ such that $|\alpha| = \sqrt{q}$ and $P \in \mathbb{Z}(t)$.

As full proofs of the Weil conjectures, even just for elliptic curves, requires further prerequisites on algebraic geometry, particularly on the *Tate module* and the *Weil pairing*, only the final part of the proof is given, of which the following lemma will be assumed.

**Lemma 2.3.4.** $|E(F_n)| = 1 + q^n - \alpha^n - \overline{\alpha}^n$ for some $\alpha \in \mathbb{C}$ such that $|\alpha| = \sqrt{q}$.

*Proof.* Omitted, see V.2.3 in [2]. □

Letting $n = 1$ in the above lemma for Theorem 2.3.3 gives $||E(F)| - 1 - q| = |-\alpha - \overline{\alpha}| \leq 2|\alpha| = 2\sqrt{q}$, which proves Hasse's theorem once again. The final part of the proof is as follows.

*Proof of Theorem 2.3.3.* The above lemma on the zeta function gives $\alpha \in \mathbb{C}$ such that $|\alpha| = \sqrt{q}$, and

$$\ln(Z_E(t)) = \sum_{n=1}^{\infty} (1 + q^n - \alpha^n - \overline{\alpha}^n) \frac{t^n}{n} = -\ln(1-t) - \ln(1-qt) + \ln(1-\alpha t) + \ln(1-\overline{\alpha} t).$$

Thus

$$Z_E(t) = \frac{(1-\alpha t)(1-\overline{\alpha} t)}{(1-t)(1-qt)}, \qquad |\alpha| = \sqrt{q},$$

which satisfies rationality and the Riemann hypothesis, and gives the functional equation

$$Z_E\left(\frac{1}{qt}\right) = \frac{\left(1 - \frac{\alpha}{qt}\right)\left(1 - \frac{\overline{\alpha}}{qt}\right)}{\left(1 - \frac{1}{qt}\right)\left(1 - \frac{1}{t}\right)} = \frac{qt^2 - (\alpha + \overline{\alpha})t + \frac{\alpha\overline{\alpha}}{q}}{(qt-1)(t-1)} = \frac{(1-\alpha t)(1-\overline{\alpha} t)}{(1-t)(1-qt)} = Z_E(t).$$

□

By the above proof, the connection to the classical Riemann hypothesis can then be seen as follows. An analogue of the Riemann zeta function can be defined for elliptic curves over $F$ as $\zeta_E(s) = Z_E(q^{-s})$. It then satisfies a similar functional equation,

$$\zeta_E(s) = Z_E\left(q^{-s}\right) = Z_E\left(q^{s-1}\right) = \zeta_E(1-s).$$

If $\zeta_E(s) = 0$, Theorem 2.3.3 also gives

$$\frac{(1-\alpha q^{-s})(1-\overline{\alpha} q^{-s})}{(1-q^{-s})(1-q^{1-s})} = 0, \qquad |\alpha| = \sqrt{q}.$$

Hence $1 = \alpha q^{-s}$ or $1 = \overline{\alpha} q^{-s}$, so $q^{\Re(s)} = |q^s| = \sqrt{q}$. Thus $\Re(s) = \frac{1}{2}$.

**Remark.** The Weil conjectures is a generalisation of Riemann hypothesis, which those for elliptic curves is in turn a special case of. In general, there are many zeta functions analogous to the Riemann zeta function. One such family of zeta functions is for a *finitely generated algebra* $R$ over $\mathbb{Z}$, defined as

$$\zeta_R(s) = \prod_M \frac{1}{1 - |R/M|^{-s}},$$

over all maximal ideals $M \subset R$.

## 2.4 Schoof's algorithm

In light of Hasse's theorem, there were improved algorithms to compute $E(F)$ similar to the naive approach described in a previous subsection. Lagrange's theorem gives that $ord(P) \mid |E(F)|$ for any point $P \in E(F)$, the latter of which is bounded by Hasse's theorem. After obtaining a random point $P \in E(F)$ by inspection or otherwise, simply try all values of $n \in \mathbb{Z}$ such that $q - 2\sqrt{q} + 1 \leq n \leq q + 2\sqrt{q} + 1$ to catch whenever $nP = \mathcal{O}$. If this $n$ is unique, the point $P$ is a generator of $E(F)$ and hence $|E(F)| = ord(P) = n$. Otherwise obtain a different random point $P \in E(F)$ and repeat. This process can be illustrated with a prior example.

**Example.** Let $E : y^2 = x^3 + x + 1$ be an elliptic curve over $\mathbb{F}_5$ and $P = (0, 1) \in E(\mathbb{F}_5)$ be a point. Hasse's theorem gives $|E(\mathbb{F}_5)| = 5 - t + 1$ for some $|t| \leq 2\sqrt{5}$, so $|E(\mathbb{F}_5)| \in \{2, \dots, 10\}$. Then the addition formula gives only $9P = \mathcal{O}$, so $|E(\mathbb{F}_5)| = 9$.

There is then room for algorithms like *baby-step giant-step* that trades a space complexity of $O\left(\sqrt{q}\right)$ for a time complexity of also $O\left(\sqrt{q}\right)$, speeding up the computation further. However, discussions here will be on a different algorithm for computing $|E(F)|$, which also builds upon Hasse's theorem. A high-level description of the *deterministic polynomial time* algorithm is as follows.

**Algorithm 2.4.1** (Schoof's algorithm)**.** Input: an elliptic curve $E$ over $\mathbb{F}_q$. Output: $|E(\mathbb{F}_q)|$.

1. Generate a set $S$ of distinct primes excluding $p$ with product $N \in \mathbb{Z}_{>0}$, such that $N > 4\sqrt{q}$.
2. Compute $t \mod n$ for each $n \in S$.
3. Obtain $t \mod N$ from each $t \mod n$.
4. Reduce $t$ into a value between $-2\sqrt{q}$ and $2\sqrt{q}$.
5. Calculate $|E(F)| = q - t + 1$.

The proof of this algorithm will be done in reverse. The first and last two steps will be made clear later, but several results will be proven for the second and third. In particular, the former generates a system of prime congruences for the latter, which in turn employs a classical theorem in number theory as follows.

**Theorem 2.4.2** (Chinese remainder)**.** Let $n_1, \dots, n_k \in \mathbb{Z}_{>1}$ be pairwise coprime with product $N \in \mathbb{Z}_{>0}$, and let $t_1, \dots, t_k \in \mathbb{Z}$. Then there is a unique $t \in \mathbb{Z}_{\geq 0}$ such that $t < N$ and each $t \equiv t_i \mod n_i$.

*Proof.* Let $k = 2$. Bézout's identity gives $m_1 n_1 + m_2 n_2 = 1$ for some $m_i \in \mathbb{Z}$. Let $t' = t_2 m_1 n_1 + t_1 m_2 n_2$, so

$$t' = (t_2 - t_1) m_1 n_1 + t_1 (m_1 n_1 + m_2 n_2) \equiv t_1 \mod n_1,$$

$$t' = t_2 (m_1 n_1 + m_2 n_2) - (t_2 - t_1) m_2 n_2 \equiv t_2 \mod n_2.$$

If $t'' \in \mathbb{Z}$ is such that $t'' \equiv t_1 \mod n_1$ and $t'' \equiv t_2 \mod n_2$, then $t' \equiv t'' \mod n_1$ and $t' \equiv t'' \mod n_2$, so $n_1 \mid t' - t''$ and $n_2 \mid t' - t''$. Then $N = n_1 n_2 \mid t' - t''$, so $t' \equiv t'' \mod N$ and $t'$ is unique up to congruences. Hence division gives a unique $t \in \mathbb{Z}_{\geq 0}$ such that $t < N$ and $t \equiv t' \mod N$. Now let $k \in \mathbb{Z}_{\geq 2}$ with product $N_k \in \mathbb{Z}_{>0}$ and assume that there is a unique $t' \in \mathbb{Z}_{\geq 0}$ such that $t' < N_k$ and each $t' \equiv t_i \mod n_i$. Since $N_k$ and $n_{k+1}$ are coprime, the case $k = 2$ gives a unique $t \in \mathbb{Z}_{\geq 0}$ such that $t < N_k n_{k+1}$, and $t \equiv t' \mod N_k$ and $t \equiv t_{k+1} \mod n_{k+1}$. Thus the unique $t \in \mathbb{Z}_{\geq 0}$ holds by induction. □

**Remark.** The Chinese remainder theorem can be generalised to ideals $I_i$ of arbitrary commutative unital rings $R$, replacing the coprime condition with $I_n + I_m = R$ for all $n, m \in \mathbb{Z}$ and modulo with respect to $I_i$.

A general process for computing this unique $t \in \mathbb{Z}_{\geq 0}$ can be inferred directly from the proof of the Chinese remainder theorem, using the extended Euclidean algorithm for Bézout's identity, illustrated as follows.

**Example.** Let

$$t \equiv 1 \mod 2, \qquad t \equiv 2 \mod 3, \qquad t \equiv 3 \mod 5$$

be a system of congruences for $t \in \mathbb{Z}_{\geq 0}$. Bézout's identity gives $(-1)(2) + (1)(3) = 1$, so let $t' = 2(-1)(2) + 1(1)(3) = -1$ be such that $t' \equiv 1 \mod 2$ and $t' \equiv 2 \mod 3$. Hence division gives $t'' = 1(6) + (-1) = 5 < 6$ such that $t'' \equiv t' \mod 6$. Similarly Bézout's identity gives $(1)(6) + (-1)(5) = 1$, so let $t''' = 3(1)(6) + 5(-1)(5) = -7$ be such that $t''' \equiv 5 \mod 6$ and $t''' \equiv 3 \mod 5$. Thus division gives $t = 1(30) + (-7) = 23 < 30$ such that $t \equiv t''' \mod 30$ similarly.

For the rest of this section, let $S$ be as in the first step of Schoof's algorithm and $n \in S$ be a prime. Now invoking the Chinese remainder theorem on the system of congruences $t' \equiv t \mod n$ generated by the second step gives a unique $t'' \in \mathbb{Z}_{\geq 0}$ such that $t'' < N$ and $t'' \equiv t' \mod N$, as in the third step. The fourth step then ensures this $t''$ falls within the required bound using careful Euclidean division to give the trace $t \in \mathbb{Z}$, of which the first step has made possible by forcing $S$ to span the entire interval over which it could lie in. The fifth step is merely a simple application of Hasse's theorem. It only remains to understand the second step of Schoof's Algorithm. This uses the properties of a general system of polynomials allowing for recursive operations, given in the following definition.

**Definition** (Division polynomial)**.** The **$n$-th division polynomial** $\psi_n \in F[x, y]$ is defined for $n \in \mathbb{Z}$ by

$$\begin{aligned}
\psi_0(x, y) &= 0, \\
\psi_1(x, y) &= 1, \\
\psi_2(x, y) &= 2y, \\
\psi_3(x, y) &= 3x^4 + 6Ax^2 + 12Bx - A^2, \\
\psi_4(x, y) &= 4y\left(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2\right),
\end{aligned}$$

recursively defined for $n > 4$ by

$$\begin{aligned}
\psi_{2m} &= \tfrac{1}{2y}\psi_m\left(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2\right), \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3,
\end{aligned}$$

and for $n < 0$ by $\psi_{-n} = -\psi_n$, with associated polynomials $\phi_n, \omega_n \in F[x, y]$ defined for $n \in \mathbb{Z}_{\geq 0}$ by

$$\begin{aligned}
\phi_n &= x\psi_n^2 - \psi_{n+1}\psi_{n-1}, \\
\omega_n &= \tfrac{1}{4y}\left(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2\right).
\end{aligned}$$

It holds that $\phi_{-n} = -\phi_n$ and $\omega_{-n} = -\omega_n$, and $\psi_{2m} = 2\omega_n\psi_n$. The following lemma allows certain division polynomials to be written solely in terms of $x$.

**Lemma 2.4.3.** If $n \in \mathbb{Z}$ is even, then

$$\psi_n \in 2y\mathbb{Z}[x, A, B], \qquad \phi_n \in \mathbb{Z}[x, A, B], \qquad \omega_n \in \mathbb{Z}[x, A, B],$$

otherwise $n \in \mathbb{Z}$ is odd, then

$$\psi_n \in \mathbb{Z}[x, A, B], \qquad \phi_n \in \mathbb{Z}[x, A, B], \qquad \omega_n \in y\mathbb{Z}[x, A, B].$$

*Proof.* Let $Z = \mathbb{Z}[x, A, B]$, then $\psi_0, \psi_2, \psi_4 \in 2yZ$ and $\psi_1, \psi_3 \in Z$. Assume that $\psi_n \in 2yZ$ for any even $n \in \mathbb{Z}_{\geq 0}$ and $\psi_n \in Z$ for any odd $n \in \mathbb{Z}_{\geq 0}$ such that $n < 2m$. If $m$ is even, then

$$\psi_m, \psi_{m+2}, \psi_{m-2} \in 2yZ, \qquad \psi_{m-1}, \psi_{m+1} \in Z \qquad \implies \qquad \psi_{2m} \in 2yZ, \qquad \psi_{2m+1} \in Z.$$

Otherwise $m$ is odd, then similarly

$$\psi_{m-1}, \psi_{m+1} \in 2yZ, \qquad \psi_m, \psi_{m+2}, \psi_{m-2} \in Z \qquad \implies \qquad \psi_{2m} \in 2yZ, \qquad \psi_{2m+1} \in Z.$$

Hence $\psi_n \in 2yZ$ for any even $n \in \mathbb{Z}$ and $\psi_n \in Z$ for any odd $n \in \mathbb{Z}$. If $n$ is even, then

$$\psi_n^2 \in y^2Z = Z, \qquad \psi_{n+1}\psi_{n-1} \in Z \qquad \implies \qquad \phi_n \in Z.$$

Otherwise $n$ is odd, then similarly

$$\psi_n^2 \in Z, \qquad \psi_{n+1}\psi_{n+1} \in 4y^2Z = Z \qquad \implies \qquad \phi_n \in Z.$$

Now if $n$ is even, then also

$$\psi_{n+2}, \psi_{n-2} \in 2yZ, \qquad \psi_{n-1}, \psi_{n+1} \in Z \qquad \implies \qquad \omega_n \in Z.$$

Otherwise $n$ is odd, then similarly also

$$\psi_{n-1}, \psi_{n+1} \in 2yZ, \qquad \psi_{n+2}, \psi_{n-2} \in Z \qquad \implies \qquad \omega_n \in yZ.$$

□

The division polynomials $\phi_n(x,y)$, $\psi_n(x,y)^2$, and $\omega_n(x,y)^2$ can then be written as $\phi_n(x)$, $\psi_n(x)^2$, and $\omega_n(x)^2$ respectively as an abuse of notation without ambiguity. Now the familiar expression for $\psi_4$ is that of the multiplication by two map, generalised as follows.

**Proposition 2.4.4.** Let $n \in \mathbb{Z}$. Then

$$[n](x,y) = \left(x - \frac{\psi_{n+1}(x,y)\psi_{n-1}(x,y)}{\psi_n(x)^2}, \frac{\psi_{2n}(x,y)}{2\psi_n(x,y)^4}\right) = \left(\frac{\phi_n(x)}{\psi_n(x)^2}, \frac{\omega_n(x,y)}{\psi_n(x,y)^3}\right).$$

The proof of this proposition is through induction on $n \in \mathbb{Z}_{\geq 0}$ with base cases $n \in \{0,\dots,4\}$, while $n \in \mathbb{Z}_{<0}$ follows directly from the above observation. While it is completely elementary through the group law explicit formulae, it is extremely tedious and computational and hence are omitted altogether.

*Proof.* Omitted, see III.E.3.7 in [2]. □

**Remark.** This proof can be approached via other ways, such as through properties of the *Weierstrass elliptic function* $\wp$ in 9.33 of [10], which will not be discussed. The fact that $\gcd(\phi_n, \psi_n^2) = 1$ and $\deg(\phi_n) = n^2$ also lends itself to another proof that $\deg([n]) = n^2$ for any $n \in \mathbb{Z}$.

Relating this back to the standard form of isogenies, it holds that $\psi_n(a,b) = 0$ iff $[n](P) = \mathcal{O}$ for any point $P = (a,b) \in E$, which is the case whenever $P \in E[n]$. Group operations in $End(E[n])$ can be more easily done since the polynomials involved in the endomorphisms have bounded degrees in the *coordinate ring* $F[x,y]/\langle y^2 - x^3 - Ax - B, \psi_n\rangle$, provided $\psi_n$ is already precomputed. Now arithmetic in $End(E[n])$ is motivated by the second step of Schoof's algorithm, where all congruences are modulo $n$ and endomorphisms are computed modulo $\psi_n$. A *characteristic* equation that all endomorphisms satisfy will be given in the following lemma.

**Lemma 2.4.5.** Let $\phi \in End(E)$ be an endomorphism, and let $d = \deg(\phi)$ and $t = 2\langle \phi, [1]\rangle$. Then $\phi^2 - t\phi + [d] = 0$.

*Proof.* Let $n \in \{-1, 1\}$. Since $\deg \phi + [n] = \deg(\phi) + 2n\langle \phi, [1]\rangle + \deg([n]) = d + nt + 1$, it holds that

$$\begin{aligned}\langle \phi^2, [1]\rangle &= -\tfrac{1}{2}\left(\deg\left(\phi^2 - [1]\right) - \deg\left(\phi^2\right) - \deg(-[1])\right)\\ &= -\tfrac{1}{2}\left(\deg(\phi - [1])\deg(\phi + [1]) - \deg(\phi)^2 - 1\right)\\ &= -\tfrac{1}{2}\left((d + t + 1)(d - t + 1) - d^2 - 1\right) = -\tfrac{1}{2}\left(2d - t^2\right).\end{aligned}$$

Since also

$$\langle \phi^2, \phi\rangle = \tfrac{1}{2}\left(\deg\left(\phi^2 + \phi\right) - \deg\left(\phi^2\right) - \deg(\phi)\right) = \tfrac{1}{2}\deg(\phi)\left(\deg(\phi + [1]) - \deg(\phi) - [1]\right) = d\langle \phi, [1]\rangle = \tfrac{1}{2}dt,$$

it holds that

$$\begin{aligned}\deg\left(\phi^2 - t\phi + [d]\right) &= \deg\left(\phi^2\right) + \deg(t\phi) + \deg([d]) - 2\langle \phi^2, t\phi\rangle + 2\langle \phi^2, [d]\rangle - 2\langle t\phi, [d]\rangle\\ &= \deg(\phi)^2 + t^2\deg(\phi) + d^2 - 2t\langle \phi^2, \phi\rangle + 2d\langle \phi^2, [1]\rangle - 2dt\langle \phi, [1]\rangle\\ &= 2d^2 - 2t\langle \phi^2, \phi\rangle + 2d\langle \phi^2, [1]\rangle\\ &= 2d^2 - 2\left(\tfrac{1}{2}dt^2\right) + 2d\left(-\tfrac{1}{2}\left(2d - t^2\right)\right) = 0.\end{aligned}$$

Thus $\phi^2 - t\phi + [d] = 0$. □

In particular, the $q$-th Frobenius endomorphism satisfies the characteristic equation, so it can be written as $tFr_q = Fr_q^2 + [q]$. While it is possible to compute the right hand side directly and try all values of $t$ until one satisfies the characteristic equation, the polynomials involved in $Fr_q$ and $Fr_q^2$ will have rapidly increasing degrees, which is highly impractical for huge $q$. The second step handles exactly this by reducing the equation in $End(E)$ to one in $End(E[n])$ with affine points, as seen in the following lemma.

**Lemma 2.4.6.** Let $P = (a, b) \in E[n]$ be a point. Then there are unique $t_n \in \mathbb{Z}_{\geq 0}$ and $q_n \in \mathbb{Z}_{>0}$ such that $t_n \equiv t,\ q_n \equiv q \mod n$ with $|t_n|, |q_n| < n$, and

$$t_n(a^q, b^q) = \left(a^{q^2}, b^{q^2}\right) + (a_q, b_q), \qquad q_n P = (a_q, b_q) \in E[n].$$

*Proof.* Since $Fr_q$ is injective, so is $Fr_q^2$, so $Fr_q(P) = (a^q, b^q)$ and $Fr_q^2(P) = \left(a^{q^2}, b^{q^2}\right)$. Hence

$$t(a^q, b^q) = \left(a^{q^2}, b^{q^2}\right) + q(a, b).$$

Now Lagrange's theorem gives that $P \in E[n]$ iff $ord(P) = n$. Since $q$ is prime and $q \neq n$, it holds that $\gcd(q, n) = 1$, so $qP \neq \mathcal{O}$. Then division gives a unique $q_n \in \mathbb{Z}_{>0}$ such that $q_n \equiv q \mod n$ with $|q_n| < n$. Hence $q_n P = qP = (a_q, b_q)$ for some point $(a_q, b_q) \in E[n]$. Similarly division gives a unique $t_n \in \mathbb{Z}_{\geq 0}$ such that $t_n \equiv t \mod n$ and $|t_n| < n$. Since $Fr_q$ has a trivial kernel and $nFr_q(P) = Fr_q(nP) = Fr_q(\mathcal{O}) = \mathcal{O}$, it holds that $ord(Fr_q(P)) = n = ord(P)$, so $t_n Fr_q(P) = tFr_q(P)$ similarly. Thus

$$t_n(a^q, b^q) = \left(a^{q^2}, b^{q^2}\right) + (a_q, b_q).$$

□

Hence it boils down to obtaining a suitable $t_n \in \mathbb{Z}_{\geq 0}$ satisfying

$$t_n(x^q, y^q) = \left(x^{q^2}, y^{q^2}\right) + q_n(x, y),$$

all of which can be computed as per usual, but in the coordinate ring $F[x, y] / \langle y^2 - x^3 - Ax - B, \psi_n \rangle$. The following algorithm illustrates the process of computing this $t_n$, with further details given in [10].

**Algorithm 2.4.7** (Computation of the trace modulo prime)**.** Input: an elliptic curve $E$ over $\mathbb{F}_q$ and a prime $n \in S$. Output: $t_n$. If $n = 2$, then

$$t_n = \begin{cases} 0 & g \neq 1 \\ 1 & g = 1 \end{cases}, \qquad g = \gcd\left(x^q - x, x^3 + Ax + B\right).$$

Otherwise $n > 2$, then compute $\psi_n$ and $q_n$, and reduce $q_n$ into a value between $-n/2$ and $n/2$. Let

$$(x', y') = \left(x^{q^2}, y^{q^2}\right) + q_n(x, y), \qquad (x'', y'') = (x^q, y^q).$$

If $x' = x_i$, where $(x_i, y_i) = i(x'', y'')$ for some $i \in \{1, \ldots, (n-1)/2\}$, then

$$t_n = \begin{cases} i & y' = y_i \\ -i & y' = -y_i \end{cases}.$$

Otherwise if $q_n \equiv r_n^2 \mod n$ for some $r_n \in \{1, \ldots, (n-1)/2\}$, then let $(x_r, y_r) = r_n(x, y)$ and

$$\left(\frac{r(x)}{s(x)}, \frac{u(x)}{v(x)} y\right) = (x'' - x_r, y'' - y_r), \qquad \gcd(r, s) = \gcd(u, v) = 1.$$

If $\gcd(r, \psi_n) = 1$, then

$$t_n = \begin{cases} 2r_n & g' \neq 1 \\ -2r_n & g' = 1 \end{cases}, \qquad g' = \gcd(u, \psi_n)$$

Otherwise $t_n = 0$.

An analysis of Schoof's algorithm shows that it has a time complexity of $O\left(\log^8(q)\right)$, which is asymptotically faster than that of the naive approach. Subsequently, there were refinements that restricted the primes in $S$ into *Elkies primes* and *Atkin primes* rather than arbitrary small primes, and made use of *modular polynomials* rather than division polynomials. Now known as the *Schoof-Elkies-Atkin* algorithm, it has a time complexity of $O\left(\log^6(q)\right)$ and is widely used in practicality when the prime $q$ in question is huge, seen in the *ellcard* command in the *PARI* programming language. In implementations when maximum efficiency is required, a probabilistic version is used, which allows even faster computations of many operations.

## 2.5 Point counting

As per the aim of this section, Schoof's algorithm computes the number of rational points of elliptic curves over finite fields. Although computations are generally done by code due to routine tedium, the following simple example illustrates a possible execution process.

**Example.** Let $E : y^2 = x^3 + 2x + 1$ be an elliptic curve over $\mathbb{F}_{19}$, so let $S = \{2, 3, 5\}$ be such that $N = (2)(3)(5) = 30 > 20 = 4\sqrt{25} > 4\sqrt{19}$.

- Let $n = 2$. Then

$$\begin{aligned} x^{19} &= x(-2x-1)^6 = 7x^7 + 2x^6 + 12x^5 + 8x^4 + 3x^3 + 12x^2 + x \\ &= 7x(-2x-1)^2 + 2(-2x-1)^2 + 12x^2(-2x-1) + 8x(-2x-1) + 3(-2x-1) + 12x^2 + x \\ &= 4x^3 + x^2 + 2x + 18 = 4(-2x-1) + x^2 + 2x + 18 = x^2 + 13x + 14, \end{aligned}$$

  so $\gcd\left(x^{19} - x, x^3 + 2x + 1\right) = \gcd\left(x^2 + 12x + 14, x^3 + 2x + 1\right) = 1$. Hence $t_2 = 1$.

- Let $n = 3$. Then $q_3 = 1 \equiv 19 \mod 3$ such that $-3/2 \leq 1 \leq 3/2$, and $\psi_3(x) = 3x^4 + 12x^2 + 12x + 15$. Since $\psi_3(8) = 3(8)^4 + 12(8)^2 + 12(8) + 15 = 0$, it holds that $(8, b) \in E(\mathbb{F}_{19})[3]$ for some $b \in \mathbb{F}_{19}$. Lagrange's theorem gives $3 \mid |E(\mathbb{F}_{19})|$, so $19 - t + 1 \equiv 0 \mod 3$ and $t \equiv 20 \equiv 2 \mod 3$. Hence $t_3 = 2$.

- Let $n = 5$. Then $q_5 = -1 \equiv 19 \mod 5$ such that $-5/2 \leq 1 \leq 5/2$, and

$$\begin{aligned} \psi_5(x) &= \psi_4(x,y)\psi_2(x,y)^3 - \psi_1(x,y)\psi_3(x,y)^3 \\ &= 4y\left(x^6 + 10x^4 + x^3 + 18x^2 + 11x + 11 + 11\right)(2y)^3 - 1\left(3x^4 + 12x^2 + 12x + 15\right)^3 \\ &= 13\left(x^3 + 2x + 1\right)^2\left(x^6 + 10x^4 + x^3 + 18x^2 + 11x + 3\right) \\ &\quad + 11x^{12} + 18x^{10} + 18x^9 + 9x^8 + 11x^7 + 6x^6 + 12x^5 + 10x^4 + 18x^3 + 12x^2 + 13x + 7 \\ &= 5x^{12} + 10x^{10} + 17x^8 + 5x^7 + x^6 + 9x^5 + 12x^4 + 2x^3 + 5x^2 + 8x + 8, \end{aligned}$$

  so let $(x', y') = \left(x^{361}, y^{361}\right) - (x, y)$ and $(x'', y'') = \left(x^{19}, y^{19}\right)$. It can be tediously verified that $x' \neq x_1$ but $x' = x_2$, where $(x_i, y_i) = i(x'', y'')$, so $t_n \equiv 2 \mod 5$ or $t_n \equiv -2 \mod 5$. Another tedious verification gives $y' = -y_2$, so $t_n \equiv -2 \equiv 3 \mod 5$. Hence $t_5 = 3$.

The Chinese Remainder Theorem from the example above gives $t \equiv 23 \mod 30$ such that $0 \geq 23 < 30 = N$. Thus $t = 23 - 30 = -7$ is such that $|-7| < 8 = 4\sqrt{4} < 4\sqrt{19}$ and $|E(\mathbb{F}_{19})| = 19 - (-7) + 1 = 27$.

While just counting $F$-rational points may have many practical applications, a subtler question would be characterising their group structure. This would be more than just Schoof's algorithm, but machinery from previous subsections can finally combine to give the following proposition.

**Proposition 2.5.1.** $E(F) \cong \mathbb{Z}_{n_1}$ or $E(F) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ for some $n_1, n_2 \in \mathbb{Z}_{>0}$ such that $n_1 \mid n_2$.

*Proof.* The fundamental theorem of finite abelian groups gives

$$E(F) \cong \bigoplus_{i=1}^{m} \mathbb{Z}_{n_i}, \qquad m \in \mathbb{Z}_{\geq 0}, \qquad n_i \in \mathbb{Z}_{>0},$$

such that each $n_i \mid n_{i+1}$. Let $G_i = \{x \in \mathbb{Z}_{n_i} \mid ord(x) \mid n_1\} \leq \mathbb{Z}_{n_i}$ be subgroups. Then each $\phi_i : \mathbb{Z}_{n_1} \to G_i$ defined by $\phi_i(x) = n_i x / n_1$ is an isomorphism, so each $|G_i| = |\mathbb{Z}_{n_1}| = n_1$. Hence

$$n_1^m = \left|\bigoplus_{i=1}^{m} G_i\right| = |E(F)[n_1]| \leq |E[n_1]| = |Ker(n_1)| = \deg_s([n_1]) \leq \deg([n_1]) = n_1^2.$$

Since $q \notin \{2, 3\}$, it holds that $|E(F)| = q - t + 1 \geq q - 2\sqrt{q} + 1 > 1$. Thus $|E(F)| \ncong \{0\}$ and $m \in \{1, 2\}$. □

Both cases can arise from different elliptic curves and finite fields, as seen in the following example.

**Example.** $E(\mathbb{F}_5) \cong \mathbb{Z}_9$ in the above example, while $E' : y^2 = x^3 + x$ over $\mathbb{F}_5$ has $E'(\mathbb{F}_5) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

**Remark.** If $q \in \{2, 3\}$, then $E(F)$ could be trivial, but the only examples with this property are $E_2 : y^2 + y = x^3 + x + 1$ and $E_2' : y^2 + y = x^3 + x^2 + 1$ over $\mathbb{F}_2$ and $E_3 : y^2 = x^3 - x - 1$ over $\mathbb{F}_3$, up to isomorphism.

# 3 Elliptic curves over the rationals

After the discussion of elliptic curves over finite fields, the focus redirects to the field of rational numbers. Again, the question of computing the rational points arises again, with the unfortunate answer that it is not as straightforward as finite fields. Due to the countably infinite nature of the rationals, enumerating all possible rational solutions of all elliptic curves is not possible, so other techniques will be deployed. In particular, there will be an attempt to prove one of the most fundamental theorems of elliptic curves over the rationals, namely that the rational points form a finitely generated group. While finite groups arising from finite fields can be fully characterised by the fundamental theorem of finite abelian groups, finitely generated groups arising from the rationals can be fully characterised by the fundamental theorem of finitely generated abelian groups,

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus \bigoplus_{i=1}^{m} \mathbb{Z}_{n_i}, \qquad r, m \in \mathbb{Z}_{\geq 0}, \qquad n_i \in \mathbb{Z}_{>1},$$

such that each $n_i \mid n_{i+1}$, which is given in full in Appendix A.4. However, there are issues with computing $r \in \mathbb{Z}_{\geq 0}$, which will be discussed later. Now let $E$ be an elliptic curve over the perfect field $\mathbb{Q}$, given by the Weierstrass curve

$$E : y^2 = x^3 + A'x + B', \qquad A' = \frac{p}{q}, B' = \frac{p'}{q'} \in \mathbb{Q},$$

with the group of rational points $E(\mathbb{Q}) = (E(\mathbb{Q}), \mathcal{O}, +)$. Since there is a $j$-invariant affine transformation $(x, y) \mapsto \left(q^{-2}q'^{-2}x, q^{-3}q'^{-3}y\right)$, there is an isomorphism from $E$ to the curve given by the Weierstrass equation

$$\left(\frac{1}{q^3q'^3}y\right)^2 = \left(\frac{1}{q^2q'^2}x\right)^3 + \frac{p}{q}\left(\frac{1}{q^2q'^2}x\right) + \frac{p'}{q'} \qquad \implies \qquad y^2 = x^3 + pq^3q'^4x + p'q^6q'^5.$$

Hence for this section, assume without loss of generality that

$$E : y^2 = x^3 + Ax + B, \qquad A, B \in \mathbb{Z}.$$

## 3.1 Nagell-Lutz theorem

For the following sections, let $\Delta'_E = \frac{1}{16}\Delta_E$ be the *reduced discriminant*. Then the following theorem characterises the affine coordinates of torsion points.

**Theorem 3.1.1** (Nagell-Lutz)**.** Let $P = (a, b) \in E(\mathbb{Q})$ be a non-zero torsion point. Then:

1. $a, b \in \mathbb{Z}$, and
2. $b = 0$ or $b^2 \mid \Delta'_E$.

Proof of the first part of the Nagell-Lutz theorem will be split into several definitions and lemmas, many of which follows from the properties of *p-adic numbers*, which will not be discussed. Now let $p \in \mathbb{Z}_{>0}$ be a prime. A particular valuation in the construction of $p$-adic numbers describing how a prime divides the numerator or denominator of a rational number is given in the following definition.

**Definition** ($p$-adic valuation)**.** The **$p$-adic valuation** is a valuation $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ defined by

$$v_p(x) = \begin{cases} \max\left\{v \in \mathbb{Z}_{\geq 0} \;\middle|\; x = \frac{q}{r}p^v,\ q \in \mathbb{Z},\ r \in \mathbb{Z}_{>0},\ p \nmid r\right\} & x \neq 0 \\ \infty & x = 0 \end{cases}.$$

Hence any $x \in \mathbb{Q}$ will be uniquely written as

$$x = \frac{q}{r}p^v, \qquad q \in \mathbb{Z}, \qquad r \in \mathbb{Z}_{>0},$$

such that $p, q, r$ are pairwise coprime, where $v = v_p(x)$. It is clear that $v_p(q/r)$ is positive whenever $p$ divides $q$ and $v_p(q/r)$ is negative whenever $p$ divides $r$, while $v_p(q/r)$ is zero otherwise. This can be illustrated in the following example.

**Example.**

$$v_5\left(\frac{100}{10}\right)=v_5\left(\frac{2}{1}5^1\right)=1,\qquad v_5\left(\frac{10}{100}\right)=v_5\left(\frac{1}{2}5^{-1}\right)=-1,\qquad v_5\left(1\right)=v_5\left(5^0\right)=0.$$

Three properties given in the following lemma will come in handy when computing $p$-adic valuations of sums and products.

**Lemma 3.1.2.** Let $x,y\in\mathbb{Q}$. Then:

1. $v_p\left(1/x\right)=-v_p\left(x\right)$,
2. $v_p\left(xy\right)=v_p\left(x\right)+v_p\left(y\right)$, and
3. $v_p\left(x+y\right)\geq\min\left\{v_p\left(x\right),v_p\left(y\right)\right\}$, with equality if $v_p\left(x\right)\neq v_p\left(y\right)$.

*Proof.* Let

$$x=\frac{q}{r}p^v,\qquad y=\frac{q'}{r'}p^{v'},\qquad q,q'\in\mathbb{Z},\qquad r,r'\in\mathbb{Z}_{>0},$$

such that $p,q,r$ are pairwise coprime and $p,q',r'$ are pairwise coprime, where $v=v_p\left(x\right)$ and $v'=v_p\left(y\right)$.

1. Since $\gcd\left(r,q\right)=1$,
$$v_p\left(\frac{1}{x}\right)=v_p\left(\frac{r}{q}p^{-v}\right)=-v=-v_p\left(x\right).$$
2. Since $\gcd\left(p,qq'\right)=\gcd\left(p,rr'\right)=1$,
$$v_p\left(xy\right)=v_p\left(\frac{qq'}{rr'}p^{v+v'}\right)=v+v'=v_p\left(x\right)+v_p\left(y\right).$$
3. Assume that $v=v'$. Then
$$v_p\left(x+y\right)=v_p\left(\frac{qr'p^v+q'rp^v}{rr'}\right)=v_p\left(\frac{qr'+q'r}{rr'}p^v\right)\geq v=\min\left\{v,v'\right\}=\min\left\{v_p\left(x\right),v_p\left(y\right)\right\}.$$
Assume otherwise that $v>v'$. Since $\gcd\left(rr'\right)=\gcd\left(p,qr'p^{v-v'}+q'r\right)=1$,
$$v_p\left(x+y\right)=v_p\left(\frac{qr'p^v+q'rp^{v'}}{rr'}\right)=v_p\left(\frac{qr'p^{v-v'}+q'r}{rr'}p^{v'}\right)=v'=\min\left\{v,v'\right\}=\min\left\{v_p\left(x\right),v_p\left(y\right)\right\}.$$
Similarly, if $v<v'$, then $v_p\left(x+y\right)=\min\left\{v_p\left(x\right),v_p\left(y\right)\right\}$.

□

The following example illustrates the above lemma.

**Example.**

$$v_5\left(\frac{25}{5}\right)=v_5\left(5\right)=1=2-1=v_5\left(25\right)-v_5\left(5\right),\qquad v_2\left(8\right)=3>2=\min\left\{v_2\left(4\right),v_2\left(4\right)\right\}.$$

With this trick, a relation between the $p$-adic valuated coordinates of any affine rational point in an elliptic curve can be seen in the following lemma.

**Lemma 3.1.3.** Let $P=(a,b)\in E\left(\mathbb{Q}\right)$ be a point. Then $v_p\left(a\right)<0$ iff $v_p\left(b\right)<0$, for which $v_p\left(a\right)=-2v$ and $v_p\left(b\right)=-3v$ for some $v\in\mathbb{Z}_{>0}$.

*Proof.* Assume that $v_p(a) < 0$. Since $A, B \in \mathbb{Z}$, it holds that $v_p(A), v_p(B) \geq 0$, so

$$2v_p(b) = v_p\left(b^2\right) = v_p\left(a^3 + Aa + B\right) = \min\left\{3v_p(a), v_p(A) + v_p(a), v_p(B)\right\} = 3v_p(a).$$

Hence $2 \mid v_p(a)$ and $3 \mid v_p(b)$, so $v_p(a) = -2v$ and $v_p(b) = -3v$ for some $v \in \mathbb{Z}_{>0}$. Conversely assume that $v_p(a) \geq 0$. Then $2v_p(b) \geq \min\left\{3v_p(a), v_p(A) + v_p(a), v_p(B)\right\} \geq 0$. Thus $v_p(b) \geq 0$. □

Hence for any point $P = (a, b) \in E(\mathbb{Q})$,

$$a = \frac{q}{d^2}, \qquad b = \frac{r}{d^3}, \qquad q, r \in \mathbb{Z}, \qquad d \in \mathbb{Z}_{>0}$$

such that $\gcd(q, d) = \gcd(r, d) = 1$. This fact will be proven explicitly here as it will be used several times in later subsections. Now a change of coordinates will be undertaken to ease discussions, namely

$$t = T = \frac{X}{Y}, \qquad s = S = \frac{Z}{Y}, \qquad [X, Y, Z] \mapsto [T, 1, S] = (t, s),$$

which is an invertible projective transformation

$$E : Y^2Z = X^3 + AXZ^2 + BZ^3 \qquad \iff \qquad E' : S = T^3 + ATS^2 + BS^3 : s = t^3 + Ats^2 + Bs^3.$$

This has the effect that

$$\mathcal{O} \mapsto (0, 0), \qquad (a, b) \mapsto \left(\frac{a}{b}, \frac{1}{b}\right)$$

for any point $(a, b) \in E(\mathbb{Q})$ such that $b \neq 0$, while the three 2-torsion points $(a, 0)$ map to three points at infinity and can be disregarded for now. The modified group law is then given in the following lemma.

**Lemma 3.1.4.** Let $P = (a, b) \in E'(\mathbb{Q})$ and $Q = (a', b') \in E'(\mathbb{Q})$ be points such that $P + Q = (a'', b'') \in E'(\mathbb{Q})$. Then $-P = (-a, -b)$ and

$$a'' = a + a' + \frac{2A\lambda\mu + 3B\lambda^2\mu}{1 + A\lambda^2 + B\lambda^3}, \qquad \lambda = \frac{a^2 + aa' + a'^2 + Ab'^2}{1 - Aa(b + b') - B\left(b^2 + bb' + b'^2\right)}, \qquad \mu = b - \lambda a.$$

*Proof.* Since $(a, b) \mapsto (a/b, 1/b)$, it holds that $-(a, b) = (a, -b) \mapsto (-a/b, -1/b)$. Let $P * Q = -(P + Q) = (-a'', -b'')$. If $a \neq a'$, then the line joining $P$ and $Q$ is

$$L : s = \lambda_1 t + \mu_1, \qquad \lambda_1 = \frac{b - b'}{a - a'}, \qquad \mu_1 = b - \lambda_1 a.$$

Otherwise $a = a'$, then the tangent at $P$ is

$$L : s = \lambda_2 t + \mu_2, \qquad \lambda_2 = \frac{3a^2 + Ab^2}{1 - 2Aab - 3Bb^2}, \qquad \mu_2 = b - \lambda_2 a.$$

Since

$$\begin{aligned} b - b' &= a^3 + Aab^2 + Bb^3 - a'^3 - Aa'b'^2 - Bb'^3 \\ &= a^3 - a'^3 + Aab^2 - Aab'^2 + Aab'^2 - Aa'b'^2 + Bb^3 - Bb'^3 \\ &= (a - a')\left(a^2 + aa' + a'^2\right) + Aa(b - b')(b + b') + Ab'^2(a - a') + B(b - b')\left(b^2 + bb' + b'^2\right), \end{aligned}$$

it holds that

$$(b - b')\left(1 - Aa(b + b') - B\left(b^2 + bb' + b'^2\right)\right) = (a - a')\left(a^2 + aa' + a'^2 + Ab'^2\right),$$

so $(b - b')/(a - a') = \lambda = \lambda_1 = \lambda_2$ and $\mu = \mu_1 = \mu_2$. Now $L : s = \lambda t + \mu$ intersects $E'$ at

$$\left(1 + A\lambda^2 + B\lambda^3\right)t^3 + \left(2A\lambda\mu + 3B\lambda^2\mu\right)t^2 + \left(A\mu^2 + 3B\lambda\mu^2 - \lambda\right)t - \left(\mu - B\mu^3\right) = 0.$$

Thus comparing coefficients gives $-\left(2A\lambda\mu + 3B\lambda^2\mu\right)/\left(1 + A\lambda^2 + B\lambda^3\right) = a + a' - a''$. □

The above proof is brief but can be verified manually. Now let

$$E\left(p^v\right) = \{\mathcal{O}\} \cup \{(a,b) \in E\left(\mathbb{Q}\right) \mid v_p\left(a\right) \leq -2v,\ v_p\left(b\right) \leq -3v\}$$

be a subset of $E\left(\mathbb{Q}\right)$. Rewriting coordinates accordingly gives $v_p\left(a/b\right) \geq v$ and $v_p\left(1/b\right) \geq 3v$, so let

$$E'\left(p^v\right) = \{(0,0)\} \cup \{(a,b) \in E'\left(\mathbb{Q}\right) \mid v_p\left(a\right) \geq v,\ v_p\left(b\right) \geq 3v\}$$

be a subset of $E'\left(\mathbb{Q}\right)$ bijective to $E\left(p^v\right)$. These two sets induce two decreasing sequences of subsets.

**Definition** (Filtration)**.** A **filtration** is a decreasing sequence of subsets $S_i$ such that $S_i \supseteq S_j$ for any $i \leq j$.

A simple rephrasal gives that $E\left(p^v\right)$ and $E'\left(p^v\right)$ *induce* two $p$-adic filtrations

$$E\left(\mathbb{Q}\right) \supseteq E\left(p\right) \supseteq E\left(p^2\right) \supseteq E\left(p^3\right) \supseteq \cdots \supseteq \{\mathcal{O}\}, \qquad E'\left(\mathbb{Q}\right) \supseteq E'\left(p\right) \supseteq E'\left(p^2\right) \supseteq E'\left(p^3\right) \supseteq \cdots \supseteq \{(0,0)\}.$$

The individual subsets in these filtrations are actually subgroups, giving a filtration of subgroups, which will be proven in the following lemma.

**Lemma 3.1.5.** Let $v \in \mathbb{Z}_{>0}$ and $P = (a,b) \in E'\left(p^v\right)$ and $Q = (a',b') \in E'\left(p^v\right)$ be points such that $P + Q = (a'',b'') \in E'\left(\mathbb{Q}\right)$. Then $-P, P + Q \in E'\left(p^v\right)$ and $v_p\left(a + a' + a''\right) \geq 5v$.

*Proof.* Since $-P = (-a,-b)$, it holds that $v_p\left(-a\right) = v_p\left(a\right)$, so $-P \in E'\left(p^v\right)$. Since $A, B \in \mathbb{Z}$, it holds that $v_p\left(A\right), v_p\left(B\right) \geq 0$. Now the group law gives

$$a'' = a + a' + \frac{2A\lambda\mu + 3B\lambda^2\mu}{1 + A\lambda^2 + B\lambda^3}, \qquad \lambda = \frac{a^2 + aa' + a'^2 + Ab'^2}{1 - Aa\left(b + b'\right) - B\left(b^2 + bb' + b'^2\right)}, \qquad \mu = b - \lambda a.$$

Then

$$\begin{aligned} v_p\left(a^2 + aa' + a'^2 + Ab'^2\right) &\geq \min\left\{2v_p\left(a\right), v_p\left(a\right) + v_p\left(a'\right), 2v_p\left(a'\right), v_p\left(A\right) + 2v_p\left(b'\right)\right\} \geq 2v, \\ v_p\left(Aa\left(b + b'\right)\right) &\geq \min\left\{v_p\left(a\right) + v_p\left(a'\right) + v_p\left(b\right), v_p\left(a\right) + v_p\left(a'\right) + v_p\left(b'\right)\right\} \geq 5v, \\ v_p\left(B\left(b^2 + bb' + b'^2\right)\right) &\geq \min\left\{v_p\left(B\right) + 2v_p\left(b\right), v_p\left(B\right) + v_p\left(b\right) + v_p\left(b'\right), v_p\left(B\right) + 2v_p\left(b'\right)\right\} \geq 6v, \end{aligned}$$

so $v_p\left(\lambda\right) \geq 2v - \min\left\{0, 5v, 6v\right\} = 2v$ and $v_p\left(\mu\right) \geq \min\left\{3v, 3v\right\} = 3v$. Hence

$$\begin{aligned} &v_p\left(2A\lambda\mu + 3B\lambda^2\mu\right) \geq \min\left\{v_p\left(2\right) + v_p\left(A\right) + v_p\left(\lambda\right) + v_p\left(\mu\right), v_p\left(3\right) + v_p\left(B\right) + 2v_p\left(\lambda\right) + v_p\left(\mu\right)\right\} \geq 5v, \\ &v_p\left(1 + A\lambda^2 + B\lambda^3\right) = \min\left\{v_p\left(1\right), v_p\left(A\right) + 2v_p\left(\lambda\right), v_p\left(B\right) + 3v_p\left(\lambda\right)\right\} = 0, \end{aligned}$$

so $v_p\left(a''\right) \geq \min\left\{a, a', 5v\right\} \geq v$. Thus $P + Q \in E'\left(p^v\right)$ and $v_p\left(a + a' - a''\right) \geq 5v$. □

Note that the second part of the lemma proves something stronger, that the $x$ coordinates of three collinear points add to give a large $p$-adic valuation. Now let $R = \{x \in \mathbb{Q} \mid v_p\left(x\right) \geq 0\}$ be a unique factorisation domain such that $\left\langle p^v \right\rangle = \{x \in \mathbb{Q} \mid v_p\left(x\right) \geq v\} \subseteq R$ is a principal ideal. This also induces a filtration of subgroups

$$R \geq \left\langle p \right\rangle \geq \left\langle p^2 \right\rangle \geq \left\langle p^3 \right\rangle \geq \ldots \{0\}.$$

Then $v_p\left(a + a' - a''\right) \geq 5v$ from the previous lemma can be rephrased as $a + a' - a'' \in \left\langle p^{5v} \right\rangle$, or even better as $\left\langle p^{5v} \right\rangle + a + a' = \left\langle p^{5v} \right\rangle + a''$. The following lemma attempts to makes use of this fact.

**Lemma 3.1.6.** There is an injective group homomorphism

$$\phi : E\left(p^v\right) / E\left(p^{5v}\right) \to \left\langle p^v \right\rangle / \left\langle p^{5v} \right\rangle, \qquad \phi\left(E\left(p^{5v}\right) + P\right) = \begin{cases} \left\langle p^{5v} \right\rangle + \dfrac{a}{b} & P = (a,b) \\ \left\langle p^{5v} \right\rangle & P = \mathcal{O} \end{cases}.$$

*Proof.* Let $\psi : E\left(p^v\right) \to \left\langle p^v \right\rangle / \left\langle p^{5v} \right\rangle$ be defined by

$$\psi\left(P\right) = \begin{cases} \left\langle p^{5v} \right\rangle + \dfrac{a}{b} & P = (a, b) \\ \left\langle p^{5v} \right\rangle & P = \mathcal{O} \end{cases},$$

and let $P, Q \in E\left(p^v\right)$ be points. If $P = \mathcal{O}$, then

$$\psi\left(P\right) + \psi\left(Q\right) = \left\langle p^{5v} \right\rangle + \left\langle p^{5v} \right\rangle + \frac{a'}{b'} = \left\langle p^{5v} \right\rangle + \frac{a'}{b'} = \psi\left(Q\right) = \psi\left(P + Q\right),$$

or similar for $Q = \mathcal{O}$. If $P = (a, b)$ and $Q = (a, -b)$, then

$$\psi\left(P\right) + \psi\left(Q\right) = \left\langle p^{5v} \right\rangle + \frac{a}{b} + \left\langle p^{5v} \right\rangle - \frac{a}{b} = \left\langle p^{5v} \right\rangle = \psi\left(\mathcal{O}\right) = \psi\left(P + Q\right).$$

Otherwise $P = (a, b)$ and $Q = (a', b')$ such that $P + Q = (a'', b'')$, then

$$\psi\left(P\right) + \psi\left(Q\right) = \left\langle p^{5v} \right\rangle + \frac{a}{b} + \left\langle p^{5v} \right\rangle + \frac{a'}{b'} = \left\langle p^{5v} \right\rangle + \frac{a}{b} + \frac{a'}{b'} = \left\langle p^{5v} \right\rangle + \frac{a''}{b''} = \psi\left(P + Q\right).$$

Hence $\psi$ is a group homomorphism. Now $\mathcal{O} \in Ker\left(\psi\right)$, and $(a, b) \in Ker\left(\psi\right)$ iff $v_p\left(a/b\right) \geq 5v$. This holds iff $(a/b, 1/b) \in E'\left(p^{5v}\right)$ and $(a, b) \in E\left(p^{5v}\right)$, so $Ker\left(\psi\right) = E\left(p^{5v}\right)$. Thus the first isomorphism theorem gives a natural injective group homomorphism

$$\phi : \frac{E\left(p^v\right)}{E\left(p^{5v}\right)} \to Im\left(\psi\right) \subseteq \frac{\left\langle p^v \right\rangle}{\left\langle p^{5v} \right\rangle}.$$

□

Now the subgroup $E\left(p\right)$ can be proven to be *torsion-free* with a proof by contradiction in the following lemma, from which the first part of the Nagell-Lutz theorem can be deduced.

**Lemma 3.1.7.** $E\left(p\right)$ has no non-zero torsion points.

*Proof.* Let $P = (a, b) \in E\left(\mathbb{Q}\right)$ be an $n$-torsion point. Suppose for a contradiction that $P \in E\left(p\right)$, so $v_p\left(a\right) = -2v$ for some $v \in \mathbb{Z}_{>0}$ and $v_p\left(a/b\right) = v$. Then

$$\left\langle p^{5v} \right\rangle = \phi\left(E\left(p^{5v}\right)\right) = \phi\left(E\left(p^{5v}\right) + nP\right) = n\phi\left(E\left(p^{5v}\right) + P\right) = n\left(\left\langle p^{5v} \right\rangle + \frac{a}{b}\right) = \left\langle p^{5v} \right\rangle + n\frac{a}{b},$$

so $n\left(a/b\right) \in \left\langle p^{5v} \right\rangle$. Assume that $p \nmid n$, so $a/b \in \left\langle p^{5v} \right\rangle$ and $v = v_p\left(a/b\right) \geq 5v$, which is a contradiction. Hence $P \notin E\left(p\right)$. Otherwise assume that $p \mid n$, then $n = mp$ for some $m \in \mathbb{Z}_{>0}$. Now let $Q = mP = (a', b') \in E\left(\mathbb{Q}\right)$ be a $p$-torsion point. Since $P \in E\left(p\right)$, it holds that $Q \in E\left(p\right)$, so $v_p\left(a'\right) = -2v'$ for some $v' \in \mathbb{Z}_{>0}$ and $v_p\left(a'/b'\right) = v'$. Then

$$\left\langle p^{5v'} \right\rangle = \phi\left(E\left(p^{5v'}\right)\right) = \phi\left(E\left(p^{5v'}\right) + pQ\right) = p\phi\left(E\left(p^{5v'}\right) + Q\right) = p\left(\left\langle p^{5v'} \right\rangle + \frac{a'}{b'}\right) = \left\langle p^{5v} \right\rangle + p\frac{a'}{b'},$$

so $p\left(a'/b'\right) \in \left\langle p^{5v'} \right\rangle$. Then $5v' \leq v_p\left(p\left(a'/b'\right)\right) = v_p\left(p\right) + v_p\left(a'/b'\right) = 1 + v'$, which is again a contradiction. Hence $Q \notin E\left(p\right)$ and $P \notin E\left(p\right)$. Thus $E\left(p\right)$ has no non-zero torsion points. □

Both parts of the Nagell-Lutz theorem can finally be proven here, the second part a corollary of the first.

*Proof of Theorem 3.1.1.* Let $P = (a, b) \in E\left(\mathbb{Q}\right)$ be a non-zero $n$-torsion point.

1. Since $P \notin E\left(p\right)$ for any prime $p \in \mathbb{Z}_{>0}$, it holds that $v_p\left(a\right) \geq 0$ and $v_p\left(b\right) \geq 0$. Thus $a, b \in \mathbb{Z}$.
2. Assume that $b \neq 0$ and let $2P = (a', b') \in E\left(\mathbb{Q}\right)$. By the duplication formula,

$$a' = \frac{a^4 - 2Aa^2 - 8Ba + A^2}{4b^2}.$$

Since $P$ and $2P$ are torsion points, it holds that $a, b, a', b' \in \mathbb{Z}$, so $b^2 \mid a^4 - 2Aa^2 - 8Ba + A^2$. Thus

$$b^2 \mid \left(a^4 - 2Aa^2 - 8Ba + A^2\right)\left(3a^2 + 4A\right) - \left(a^3 + Aa + B\right)\left(3a^3 - 5Aa - 27B\right) = 4A^3 + 27B^2 = \Delta'_E.$$

□

## 3.2 Torsion computation

An application of the Nagell-Lutz theorem is as follows. Assuming the fundamental theorem of finite abelian groups,

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors}, \qquad r \in \mathbb{Z}_{\geq 0},$$

the Nagell-Lutz theorem can be used to compute the torsion subgroup $E(\mathbb{Q})_{tors}$, since there are only finitely many torsion points $(a, b) \in E(\mathbb{Q})$ such that $b^2 \mid \Delta'_E$. The following example illustrates the full computation of the torsion subgroup of an elliptic curve.

**Example.** Let $E : y^2 = x^3 + 4$ be an elliptic curve over $\mathbb{Q}$ and $P = (a, b) \in E(\mathbb{Q})$ be a torsion point. Then either $b = 0$ or $b^2 \mid 4(0)^3 + 27(4)^2 = 3(12)^2$, so $b \in \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$, of which only $P_1 = (0, 2) \in E(\mathbb{Q})$ and $P_2 = (0, -2) \in E(\mathbb{Q})$. Then

$$2P_1 = \left(\frac{0}{4(4)}, \frac{2^2 - 3(4)}{2(2)}\right) = (0, -2) = P_2,$$

so $ord(P_1) = ord(P_2) = 3$. Thus the torsion subgroup is $E(\mathbb{Q})_{tors} = \{\mathcal{O}, P_1, P_2\} \cong \mathbb{Z}_3$.

The following algorithm summarises the process and code in the appendix.

**Algorithm 3.2.1** (Computation of the torsion subgroup)**.** Input: an elliptic curve $E$ over $\mathbb{Q}$. Output: $E(\mathbb{Q})_{tors}$.

1. Calculate $\Delta'_E$ and get all non-negative $b$ coordinates such that $b^2 \mid \Delta'_E$.
2. Get all $a$ coordinates for each non-negative $b$ coordinate such that $b^2 = a^3 + Aa + B$.
3. Add points $(a, b)$ with itself repeatedly and stop at $\mathcal{O}$ or non-integer coordinates.
4. Negate each point $(a, b)$ to $(a, -b)$ and do the same.
5. Insert $\mathcal{O}$ into the list of all points that add to $\mathcal{O}$.

The torsion subgroups of the following examples of elliptic curves given by the Weierstrass equations $y^2 = x^3 - px$ for $p \in \mathbb{Z}_{>0}$ can be computed similarly. This information will be used in a later subsection.

**Example.** The elliptic curves $E : y^2 = x^3 - x$ has torsion subgroup $E(\mathbb{Q})_{tors} = \{\mathcal{O}, (0, 0), (1, 0), (-1, 0)\} \cong \mathbb{Z}_2^2$, while the elliptic curves $E : y^2 = x^3 - 5x$, $E : y^2 = x^3 - 17x$, $E : y^2 = x^3 - 226x$ all have torsion subgroup $E(\mathbb{Q})_{tors} = \{\mathcal{O}, (0, 0)\} \cong \mathbb{Z}_2$.

The converse to the Nagell-Lutz theorem does not generally hold. It cannot be used to prove that a certain point is a torsion point, but it can be used to show the contrapositive, that a point is not a torsion point, by duplicating it until its coordinates are not integers. The following example illustrates this.

**Example.** Let $E : y^2 = x^3 - 4$ be an elliptic curve over $\mathbb{Q}$ with torsion subgroup $E(\mathbb{Q})_{tors} = \{\mathcal{O}\} \cong \mathbb{Z}_1$. Now let $P = (2, 2) \in E(\mathbb{Q})$ be a point. Then

$$2P = (5, -11), \qquad 4P = \left(\frac{785}{484}, -\frac{5497}{10648}\right).$$

Thus $ord(P)$ is infinite.

These are several examples of different torsion subgroups. In fact, there are even elliptic curves with as large as 12-torsion elements, but there are strangely none with 11-torsion elements. The following difficult theorem was proven to be an exhaustive list of all possible torsion subgroups of all elliptic curves.

**Theorem 3.2.2** (Mazur)**.** $E(\mathbb{Q})$ is isomorphic to one of

$$\mathbb{Z}_n, \qquad n \in \{1, \dots, 10, 12\},$$
$$\mathbb{Z}_2 \times \mathbb{Z}_{2n}, \qquad n \in \{1, \dots, 4\}.$$

*Proof.* Omitted, see [11]. □

As such, the torsion subgroup of an elliptic curve $E(\mathbb{Q})$ can be computed in a finite number of steps. However, computations may still be intensive if $\Delta'_E$ has many squared factors, as the computation involves solving a cubic equation. The next section provides an alternative method for this.

## 3.3 Reduction modulo prime

Another method of computing the torsion subgroup is to reduce the elliptic curve over rationals into one over a finite field, by applying isomorphisms that simplify the Weierstrass equation, then applying a particular group homomorphism. The assumption of integer coefficients in a previous subsection makes the Weierstrass equation *integral*, but a further reduction can be done as follows.

**Definition** (Minimal)**.** A Weierstrass equation is **minimal** iff it is integral and $g \in \{-1, 1\}$ if $g^4 \mid A$ and $g^6 \mid B$.

A minimal Weierstrass equation is unique up to sign. The above definition reflects the minimality of the integer coefficients after $j$-invariant affine transformations, which is illustrated in the following example.

**Example.** Let $E : y^2 = x^3 + n^4x + n^6$ be an elliptic curve over $\mathbb{Q}$ for some $n \in \mathbb{Q}$. Since there is a $j$-invariant affine transformation $(x, y) \mapsto \left(n^2x, n^3y\right)$, there is an isomorphism from $E$ to the curve given by the Weierstrass equation $y^2 = x^3 + x + 1$, which is integral and minimal.

Minimal Weierstrass equations can then be treated as if their coefficients are modulo a prime, which is stated formally as a map in the following definition.

**Definition** (Reduction map)**.** The **reduction modulo** $p$ **map** $r_p : E(\mathbb{Q}) \to E_p(\mathbb{F}_p)$ for some prime $p \in \mathbb{Z}_{>0}$ is defined by

$$E_p : y^2 = x^3 + \tilde{A}x + \tilde{B}, \qquad r_p(P) = \begin{cases} \left(\tilde{a}, \tilde{b}\right) & P = (a, b) \\ \mathcal{O} & P = \mathcal{O} \end{cases},$$

where $\tilde{\cdot} : \mathbb{Z} \to \mathbb{F}_p$ denotes modulo $p$.

There is a minor hiccup with this definition, since $E_p$ might not even define a smooth Weierstrass curve. However, since $0 \neq \Delta_E = p_1 \dots p_n$ for some primes $p_i \in \mathbb{Z}_{>0}$ and $\Delta_{E_p} = 0$ only if any $p_i \mid p$, this issue can be easily fixed by considering only the primes that are not $p_i$, which is given in the following definition.

**Definition** (Good reduction)**.** A prime $p \in \mathbb{Z}_{>0}$ is of **good reduction** iff $p \nmid \Delta_E$.

Hence $r_p$ has a well-defined codomain for infinitely many primes of good reduction, while those of bad reduction will not be considered. Additionally since the discriminant has a coefficient of 16, the prime 2 will always be considered one of bad reduction. Now $r_p$ is also well-defined, which is immediate considering the following lemma.

**Lemma 3.3.1.** Let $P = [a, b, c] \in E(\mathbb{Q})$ be a point. Then $P = [a', b', c']$ for some $a', b', c' \in \mathbb{Z}$ such that $\gcd(a', b', c') = 1$.

*Proof.* If $c = 0$, then $P = \mathcal{O}$, so $\gcd(0, 1, 0) = 1$. Otherwise $c \neq 0$, then $P = (a/c, b/c)$. Then $a/c = q/d^2$ and $b/c = r/d^3$ for some $q, r \in \mathbb{Z}$ and some $d \in \mathbb{Z}_{>0}$ such that $\gcd(q, d) = \gcd(r, d) = 1$. Thus $P = \left(q/d^2, r/d^3\right) = \left[qd, r, d^3\right]$ is such that $\gcd\left(qd, r, d^3\right) = 1$. □

This integral and minimal condition will also be defined as follows.

**Definition** (Normalised)**.** A point $P \in E(\mathbb{Q})$ has **normalised** coordinates iff it satisfies Lemma 3.3.1.

With this representation, there must be one of $a', b', c'$ coprime to $p$ for any prime $p \in \mathbb{Z}_{>0}$ of good reduction, so $r_p(P) = \left[\tilde{a'}, \tilde{b'}, \tilde{c'}\right] \in E_p(\mathbb{F}_p)$ is well-defined. The normalised coordinates of any point is unique up to sign, which is illustrated with the following example.

**Example.** Let $P = (2/5, -1/3) \in E(\mathbb{Q})$ be a point. Then

$$\left(\frac{2}{5}, -\frac{1}{3}\right) = \left[\frac{2}{5}, -\frac{1}{3}, 1\right] = [6, -5, 15], [-6, 5, -15]$$

are its normalised coordinates.

Let $p \in \mathbb{Z}_{>0}$ be a prime of good reduction. Then the following proposition characterises $r_p$.

**Proposition 3.3.2.** $r_p : E(\mathbb{Q}) \to E_p(\mathbb{F}_p)$ is a group homomorphism such that $Ker(r_p) = E(p)$.

*Proof.* Let $P, Q \in E(\mathbb{Q})$ be points with normalised coordinates and

$$L : l(X, Y, Z) = kX + mY + nZ = 0$$

be a line joining $P$ and $Q$ with coefficients in $\mathbb{Q}$ such that $P, Q, -(P+Q) \in E(\mathbb{Q}) \cap L$. Then normalising $[l, m, n]$ similarly gives $[l', m', n']$ for some $l', m', n' \in \mathbb{Z}$ such that $\gcd(l, m, n) = 1$. Hence the line

$$L_p : l_p(X, Y, Z) = \tilde{l}X + \tilde{m}Y + \tilde{n}Z = 0$$

with coefficients in $\mathbb{F}_p$ is well-defined. Now let $P = [a, b, c]$. Then

$$la + mb + nc = 0 \qquad \implies \qquad \tilde{l}\tilde{a} + \tilde{m}\tilde{b} + \tilde{n}\tilde{c} = 0,$$

so $r_p(P) = \left(\tilde{a}, \tilde{b}, \tilde{c}\right) \in E_p(\mathbb{F}_p) \cap L_p$. Similarly $r_p(Q) \in E_p(\mathbb{F}_p) \cap L_p$. Since $r_p(-\mathcal{O}) = r_p(\mathcal{O}) = -r_p(\mathcal{O})$ and

$$r_p(-(a, b)) = r_p((a, -b)) = \left(\tilde{a}, \tilde{-b}\right) = \left(\tilde{a}, -\tilde{b}\right) = -\left(\tilde{a}, \tilde{b}\right) = -r_p((a, b))$$

for any point $(a, b) \in E(\mathbb{Q})$, similarly $-r_p(P+Q) = r_p(-(P+Q)) \in E_p(\mathbb{F}_p) \cap L_p$. Since $\gcd(e_p, l_p) = 1$ where $e_p(x, y)$ is the Weierstrass equation of $E_p$, Bézout's theorem gives that $L_p$ intersects $E_p(\mathbb{F}_p)$ at three points up to multiplicity, so

$$E_p(\mathbb{F}_p) \cap L_p = \{r_p(P), r_p(Q), -r_p(P+Q)\}.$$

Hence $r_p(P) + r_p(Q) = r_p(P+Q)$. Now let $R = (a, b) \in E(\mathbb{Q})$ be a point. Then $a = q/d^2$ and $b = r/d^3$ for some $q, r \in \mathbb{Z}$ and some $d \in \mathbb{Z}_{>0}$ such that $\gcd(q, d) = \gcd(r, d) = 1$. Since $R = \left[qd, r, d^3\right]$ has normalised coordinates, it holds that $r_p(R) = \left[\tilde{q}\tilde{d}, \tilde{r}, \tilde{d}^3\right] \in E_p(\mathbb{F}_p)$. Then $R \in Ker(r_p)$ iff $\tilde{d}^3 = 0$, or $p \mid d$. This holds iff $v_p(a) \leq -2$ and $v_p(b) \leq -3$, or $R \in E(p)$. Thus $Ker(r_p) = E(p)$. □

Restricting $r_p$ into the torsion subgroup of its domain gives it a stronger property as follows.

**Theorem 3.3.3** (Reduction)**.** $E(\mathbb{Q})_{tors} \cong G$ for some $G \leq E_p(\mathbb{F}_p)$.

*Proof.* Since $Ker(r_p) = E(p)$, it holds that $v_p(a) \leq -2$ and $v_p(b) \leq -3$ for any point $P = (a, b) \in Ker(r_p)$, so $a, b \notin \mathbb{Z}$. Then the Nagell-Lutz theorem gives that $ord(P)$ is infinite, so $P \notin E(\mathbb{Q})_{tors}$. Now let $r'_p = r_p|_{E(\mathbb{Q})_{tors}}$ and $G = Im\left(r'_p\right)$, so $Ker\left(r'_p\right) = Ker(r_p) \cap E(\mathbb{Q})_{tors} = \{\mathcal{O}\}$. Thus the first isomorphism theorem gives $G \cong E(\mathbb{Q})_{tors} / Ker\left(r'_p\right) \cong E(\mathbb{Q})_{tors}$. □

Lagrange's theorem then gives $|E(\mathbb{Q})_{tors}| \mid |E_p(\mathbb{F}_p)|$, which enforces a restriction of the possible torsion subgroups. The following reignites a prior example, this time with the reduction theorem.

**Example.** Let $E : y^2 = x^3 + 4$ be an elliptic curve over $\mathbb{Q}$. Then $\Delta_E = -16\left(4(0)^3 + 27(4)^2\right) = -(2)^8(3)^3$, so let $p = 5$ be a prime of good reduction. Then the previous section gives $|E_5(\mathbb{F}_5)| = 6$. Since $|E(\mathbb{Q})_{tors}| \mid |E_5(\mathbb{F}_5)|$, it holds that $|E(\mathbb{Q})_{tors}| \in \{1, 2, 3, 6\}$. Since $ord((0, 2)) = 3$ and there are no points $P \in E(\mathbb{Q})$ such that $ord(P) = 2$, it holds that $E(\mathbb{Q})_{tors} = \{\mathcal{O}, (0, 2), (0, -2)\} \cong \mathbb{Z}_3$.

While this might not seem much of a timesave, the following example begs to differ.

**Example.** Let $E : y^2 = x^3 + 1680$ be an elliptic curve over $\mathbb{Q}$. Then $\Delta'_E = 4(0)^3 + 27(1680)^2 = 3(5040)^2 = (2)^8(3)^5(5)^2(7)^2$ and $\Delta_E = -(2)^{12}(3)^5(5)^2(7)^2$, so $p \geq 11$ are primes of good reduction. Now 5040 is a *colossally abundant number* with exactly 120 positive and negative divisors, so more than 120 values of $b$ such that $b^2 \mid \Delta'_E$ needs to be checked. Instead the previous section computes $|E_{13}(\mathbb{F}_{13})| = 9$ and $|E_{19}(\mathbb{F}_{19})| = 28$. Since $|E(\mathbb{Q})_{tors}| \mid |E_{13}(\mathbb{F}_{13})|$ and $|E(\mathbb{Q})_{tors}| \mid |E_{19}(\mathbb{F}_{19})|$, and $\gcd(9, 28) = 1$, it holds that $|E(\mathbb{Q})_{tors}| = 1$. Thus $E(\mathbb{Q})_{tors} = \{\mathcal{O}\}$.

Counting points over finite fields can generally be done very efficiently, so the reduction theorem allows for an immediate answer. In any case, computation of the torsion subgroup is relatively straightforward.

## 3.4 Mordell's theorem: descent

The following theorem is one of the most fundamental theorems of elliptic curves over the rationals, as stated in a previous subsection.

**Theorem 3.4.1** (Mordell)**.** The *Mordell-Weil group* $E(\mathbb{Q})$ is finitely generated.

**Remark.** This is a special case of the *Mordell-Weil theorem*, which states that $E(K)$ is finitely generated over any number field $K$.

Proof of Mordell's theorem will be split into two distinct steps. The first step of the proof develops some theory of a certain function that describes the size of points. The second step of the proof is a weak variant of the theorem stating that the index of a subgroup is finite. These two steps are then used in a variant of *Fermat's infinite descent*, which can be stated in full generalisation for arbitrary abelian groups as follows.

**Theorem 3.4.2** (Descent)**.** Let $G$ be an abelian group such that the index $[G : 2G]$ is finite, and let $h : G \to \mathbb{R}_{\geq 0}$ be such that:

- the set $\{P \in G \mid h(P) \leq C_1\}$ is finite for any $C_1 \in \mathbb{R}_{\geq 0}$,
- for any $Q \in G$, there is a constant $C_2 \in \mathbb{R}_{\geq 0}$ such that $h(P+Q) \leq 2h(P) + C_2$ for any $P \in G$, and
- there is a constant $C_3 \in \mathbb{R}_{\geq 0}$ such that $h(2P) \geq 4h(P) - C_3$ for any $P \in G$.

Then $G$ is finitely generated.

*Proof.* Let $Q_1, \dots, Q_n \in G$ be representatives such that $2G + Q_i \in G/2G$ are distinct cosets. For any $P \in G$, the upper bound gives each $h(P - Q_i) \leq 2h(P) + C_i$ for some $C_i \in \mathbb{R}_{\geq 0}$, so

$$h(P - Q_i) \leq 2h(P) + C, \qquad i \in \{1, \dots, n\}, \qquad C = \max\{C_i\} \in \mathbb{R}_{\geq 0}.$$

For any $P \in G$, the lower bound also gives

$$h(2P) \geq 4h(P) - C', \qquad C' \in \mathbb{R}_{\geq 0}.$$

Then there is a finite set

$$S = \{P \in G \mid h(P) \leq C + C'\}.$$

Now let $P \in G$. Then $2G + P = 2G + Q_{i_0}$ for some $i_0 \in \{1, \dots, n\}$, so $P = 2P_0 + Q_{i_0}$ for some $P_0 \in G$. By induction, for any $j \in \mathbb{Z}_{>0}$, there is some $i_j \in \{1, \dots, n\}$ such that $2G + P_{j-1} = 2G + Q_{i_j}$, so

$$P_{j-1} = 2P_j + Q_{i_j}, \qquad P = 2^{j+1}P_j + \sum_{k=0}^{j} 2^k Q_{i_k}, \qquad P_j \in G.$$

Now for any $j \in \mathbb{Z}_{>0}$,

$$4h(P_j) \leq h(2P_j) + C' = h\left(P_{j-1} - Q_{i_j}\right) + C' \leq 2h(P_{j-1}) + (C + C'),$$

so that

$$h(P_j) \leq \tfrac{1}{2}h(P_{j-1}) + \tfrac{1}{4}(C + C') = \frac{3}{4}h(P_{j-1}) - \tfrac{1}{4}\left(h(P_{j-1}) - (C + C')\right).$$

If $h(P_{j-1}) > C + C'$ for some $j \in \mathbb{Z}_{>0}$, then $h(P_j) < \frac{3}{4}h(P_{j-1})$, so $h(P_m) \leq C + C'$ for some $m \in \mathbb{Z}_{>0}$ such that $m \geq j$ and $P_m \in S$. Otherwise $h(P_{j-1}) \leq C + C'$ for all $j \in \mathbb{Z}_{>0}$, so let $m = 1$ such that $P_m \in S$ as well. Hence

$$P = 2^{m+1}P_m + \sum_{k=0}^{m} 2^k Q_{i_k} = \sum_{S_i \in S} n_i S_i + \sum_{i=1}^{n} m_i Q_i, \qquad n_i, m_i \in \mathbb{Z}.$$

Thus $G$ is finitely generated by $S \cup \{Q_i\}$. □

Mordell's theorem is simply an application of the general descent procedure.

*Proof of Theorem 3.4.1.* The three properties of the function $h$ will be given in Propositions 3.5.1, 3.5.2, 3.5.3 of the next section. The weak version of the theorem will be given in Theorem 3.6.1 of the section after the next. Applying descent to $G = E(\mathbb{Q})$ with $h$ gives that $E(\mathbb{Q})$ is finitely generated. □

The next subsections will be devoted to proving these claims.

## 3.5 Mordell's theorem: heights

The function $h$ can be defined as follows.

**Definition** (Height)**.** The **height** of a point $P \in E(\mathbb{Q})$ is a function $h(P) : E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ defined by $h(P) = \log_2(H(P))$, where

$$H(P) = \begin{cases} \max\{|p|, |q|\} & P = \left(\frac{p}{q}, y\right), \ \gcd(p, q) = 1 \\ 1 & P = \mathcal{O} \end{cases}.$$

**Remark.** The above definition for heights is chosen due to its simplicity, and is not the *canonical height* in the general literature. The theory of height functions will not be discussed here.

The three intended properties of height function will then be proven, the first of which states that there are a finite number of points less than a given height. This property is trivial and stated as follows.

**Proposition 3.5.1.** The set $S = \{P \in E(\mathbb{Q}) \mid h(P) \leq C_1\}$ is finite for any $C_1 \in \mathbb{R}_{\geq 0}$.

*Proof.* Let $C_1 \in \mathbb{R}_{\geq 0}$ and $P \in E(\mathbb{Q})$ be a point. If $P = \mathcal{O}$, then $P \in S$. Otherwise $P = (p/q, y)$, then $\max\{|p|, |q|\} \leq 2^{C_1}$, so $-2^{C_1} \leq p, q \leq 2^{C_1}$. Thus $|S| \leq \left(2^{C_1+1} + 1\right)^2 + 1$ is finite. □

The second property provides an upper bound for the height of added points. This is relatively easy and is stated in the following proposition.

**Proposition 3.5.2.** Let $Q \in E(\mathbb{Q})$. Then there is a constant $C_2 \in \mathbb{R}_{\geq 0}$ such that $h(P + Q) \leq 2h(P) + C_2$ for any $P \in E(\mathbb{Q})$.

*Proof.* If $P = \mathcal{O}$ or $Q = \mathcal{O}$ or $P + Q = \mathcal{O}$, let $C_2 = 2h(Q)$ such that $h(P + Q) \leq 2h(P) + 2h(Q)$. Otherwise $P = (a, b)$ and $Q = (a', b')$ for $a \neq a'$ or $a = a'$ and $b = b' \neq 0$. Assume that $a = a'$ and $b = b' \neq 0$, then let $C_2 = h(2Q)$ such that $h(P + Q) = h(2Q) \leq 2h(P) + h(2Q)$. Assume otherwise that $a \neq a'$, and let $C_2 = \log_2(\max\{K_3, K_2\})$, where

$$K_1 = \sqrt{1 + |A| + |B|}, \qquad K_2 = 1 + |a'|, \qquad K_3 = (|A| + |a'|) K_2 + 2(|B| + |b'| K_1).$$

Then $a = p/d^2$ and $b = q/d^3$ for some $p, q \in \mathbb{Z}$ and some $d \in \mathbb{Z}_{>0}$ such that $\gcd(p, d) = \gcd(q, d) = 1$, and $q^2 = p^3 + Apd^4 + Bd^6$. Since $H(P) = \max\left\{|p|, |d|^2\right\}$, it holds that $|p|, |d|^2 \leq H(P)$, so $|d| \leq \sqrt{H(P)}$ and

$$|q|\,|d| = \left|\sqrt{p^3 + Apd^4 + Bd^6}\right| |d| \leq \sqrt{|p|^3 |d|^2 + |A|\,|p|\,|d|^6 + |B|\,|d|^8} \leq K_1 H(P)^2.$$

Now let $P + Q = (a'', b'')$. By the addition formula,

$$a'' = \frac{(A + aa')(a + a') + 2(B - bb')}{(a - a')^2} = \frac{\left(Ad^2 + a'p\right)\left(p + a'd^2\right) + 2\left(Bd^4 - b'qd\right)}{\left(p - a'd^2\right)^2}.$$

Thus

$$\begin{aligned} h(P + Q) &\leq \log_2\left(\max\left\{\left|\left(Ad^2 + a'p\right)\left(p + a'd^2\right) + 2\left(Bd^4 - b'qd\right)\right|, \left|\left(p - a'd^2\right)^2\right|\right\}\right) \\ &\leq \log_2\left(\max\left\{\left(|A|\,|d|^2 + |a'|\,|p|\right)\left(|p| + |a'|\,|d|^2\right) + 2\left(|B|\,|d|^4 + |b'|\,|q|\,|d|\right), \left(|p| + |a'|\,|d|^2\right)^2\right\}\right) \\ &\leq \log_2\left(\max\left\{K_3 H(P)^2, K_2 H(P)^2\right\}\right) = \log_2\left(H(P)^2 \max\{K_3, K_2\}\right) = 2h(P) + C_2. \end{aligned}$$

□

The third property provides an lower bound for the height of doubled points. It is more difficult as it involves seemingly arbitrary identities, and is stated in the following proposition.

**Proposition 3.5.3.** There is a constant $C_3 \in \mathbb{R}_{\geq 0}$ such that $h(2P) \geq 4h(P) - C_3$ for any $P \in E(\mathbb{Q})$.

*Proof.* If $P = \mathcal{O}$, let $C_3 = 0$ such that $h(2P) \geq 4h(P)$. If $P = (a, 0)$, let $C_3 = 4h(P)$ such that $h(2P) \geq 0$. Otherwise $P = (a, b)$ for $b \neq 0$. Let $a = p/q$ for some $p \in \mathbb{Z}$ and some $q \in \mathbb{Z}^*$ such that $\gcd(p, q) = 1$, and let

$$\begin{aligned}
p' &= p^4 - 2Ap^2q^2 - 8Bpq^3 + A^2q^4, \\
q' &= 4p^3q + 4Apq^3 + 4Bq^4, \\
\lambda &= 12p^2q + 16Aq^3, \\
\mu &= -3p^3 + 5Apq^2 + 27Bq^3, \\
\lambda' &= \left(16A^3 + 108B^2\right)p^3 - 4A^2Bp^2q + \left(12A^4 + 88AB^2\right)pq^2 + \left(12A^3B + 96B^3\right)q^3, \\
\mu' &= A^2Bp^3 + \left(5A^4 + 32AB^2\right)p^2q + \left(26A^3B + 192B^3\right)pq^2 - \left(3A^5 + 24A^2B^2\right)q^3, \\
K_1 &= 4\max\left\{12, 16|A|\right\}, \\
K_2 &= 4\max\left\{3, 5|A|, 27|B|\right\}, \\
K_3 &= 4\max\left\{16|A|^3 + 108B^2, 4A^2|B|, 12A^4 + 88|A|B^2, 12|A|^3|B| + 96|B|^3\right\}, \\
K_4 &= 4\max\left\{A^2|B|, 5A^4 + 32|A|B^2, 26|A|^3|B| + 192|B|^3, 3|A|^5 + 24A^2B^2\right\}.
\end{aligned}$$

Then it can be tediously verified that $\lambda p' + \mu q' = 4\Delta'_E q^7$ and $\lambda' p' + \mu' q' = 4\Delta'_E p^7$. Since $|p|^2|q|$ and $|p||q|^2$ are between $|p|^3$ and $|q|^3$, it holds that $\max\left\{|p|^3, |p|^2|q|, |p||q|^2, |q|^3\right\} = \max\left\{|p|^3, |q|^3\right\}$. Then it can also be verified that

$$|\lambda| \leq K_1 M, \qquad |\mu| \leq K_2 M, \qquad |\lambda'| \leq K_3 M, \qquad |\mu'| \leq K_4 M,$$

for $M = \max\left\{|p|^3, |q|^3\right\}$, so let $C_3 = \log_2(2\max\{K_1, K_2, K_3, K_4\})$. Since

$$\begin{aligned}
4|\Delta'_E|\max\left\{|p|^3, |q|^3\right\}(\max\{|p|, |q|\})^4 = 4|\Delta'_E|\max\left\{|q|^7, |p|^7\right\} &= \max\left\{\left|4\Delta'_E q^7\right|, \left|4\Delta'_E p^7\right|\right\} \\
&\leq \max\left\{|\lambda||p'| + |\mu||q'|, |\lambda'||p'| + |\mu'||q'|\right\} \\
&\leq 2\max\left\{|\lambda|, |\mu|, |\lambda'|, |\mu'|\right\}\max\left\{|p'|, |q'|\right\} \\
&\leq 2M\max\left\{K_1, K_2, K_3, K_4\right\}\max\left\{|p'|, |q'|\right\},
\end{aligned}$$

it holds that

$$4|\Delta'_E|H(P)^4 = 4|\Delta'_E|(\max\{|p|, |q|\})^4 \leq 2\max\{K_1, K_2, K_3, K_4\}\max\{|p'|, |q'|\}.$$

Now let $2P = (a', b')$. By the duplication formula,

$$a' = \frac{a^4 - 2Aa^2 - 8Ba + A^2}{4b^2} = \frac{a^4 - 2Aa^2 - 8Ba + A^2}{4a^3 + 4Aa + 4B} = \frac{p'}{q'}.$$

Since $g = \gcd(p', q') \mid \gcd\left(4\Delta'_E p^7, 4\Delta'_E q^7\right) = 4\Delta'_E$, it holds that $1 \leq |g| \leq 4|\Delta'_E|$. Thus

$$\begin{aligned}
h(2P) &= \log_2\left(\max\left\{\left|\frac{p'}{g}\right|, \left|\frac{q'}{g}\right|\right\}\right) = \log_2\left(\frac{\max\{|p'|, |q'|\}}{|g|}\right) \\
&\geq \log_2\left(\frac{\max\{|p'|, |q'|\}}{4|\Delta'_E|}\right) \geq \log_2\left(\frac{H(P)^4}{2\max\{K_1, K_2, K_3, K_4\}}\right) \geq 4h(P) - C_3.
\end{aligned}$$

□

The properties of the height function $h$ are now verified.

## 3.6 Mordell's theorem: weak Mordell

The weak version of Mordell's theorem, restricted to $\mathbb{Q}$, states that the index of the normal subgroup $2E(\mathbb{Q}) = \{2P \mid P \in E(\mathbb{Q})\}$ is finite.

**Theorem 3.6.1** (Weak Mordell)**.** $|E(\mathbb{Q}) : 2E(\mathbb{Q})|$ is finite.

As full proofs of the weak theorem, such as in VIII.1 of [2], requires further prerequisites on algebraic number theory, particularly finiteness of the *ideal class group* of number fields, only an alternative proof is given, of which the special case of a rational 2-torsion point $(a_0, 0)$ is assumed. Since there is a $j$-invariant affine transformation $(x, y) \mapsto (x + a_0, y)$, there is an isomorphism from $E$ to the curve given by the Weierstrass equation

$$y^2 = (x + a_0)^3 + A(x + a_0) + B \qquad \implies \qquad y^2 = x^3 + 3a_0x^2 + \left(3a_0^2 + A\right)x.$$

Hence for this subsection and the next, assume without loss of generality that $a_0 = 0$ and

$$T = (a_0, 0) = (0, 0) \in E : y^2 = x^3 + Ax^2 + Bx, \qquad A, B \in \mathbb{Z}.$$

The modified discriminant and group law is then given in the following lemma.

**Lemma 3.6.2.** The following properties hold:

1. $B \neq 0$ and $A^2 - 4B \neq 0$.
2. Let $P = (a, b) \in E(\mathbb{Q})$ and $Q = (a', b') \in E(\mathbb{Q})$ be points such that $a \neq a'$ and $P + Q = (a'', b'') \in E(\mathbb{Q})$. Then $aa'a'' = \mu^2$ for some $\mu \in \mathbb{Q}$.
3. Let $P = (a, b) \in E(\mathbb{Q})$ be a point such that $b \neq 0$. Then

$$2P = \left(\frac{\left(a^2 - B\right)^2}{4b^2}, \frac{\left(a^2 - B\right)\left(a^4 + B^2 + 2Aa^3 + 2ABa + 6Ba^2\right)}{8b^3}\right) \in E(\mathbb{Q}).$$

*Proof.* The negation formula remains unmodified, so $-(a, b) = (a, -b)$ for any point $(a, b) \in E$.

1. Since $E$ is smooth and the discriminant is

$$\Delta_E = 9(4A)(2B)(0) - \tfrac{1}{4}(4A)^2\left((4A)(0) - (2B)^2\right) - 8(2B)^3 - 27(0)^2 = 16B^2\left(A^2 - 4B\right),$$

$16B^2\left(A^2 - 4B\right) \neq 0$. Thus $B \neq 0$ and $A^2 - 4B \neq 0$.

2. The line joining $P$ and $Q$ is

$$L : y = \lambda x + \mu, \qquad \lambda = \frac{b - b'}{a - a'}, \qquad \mu = \frac{ab' - a'b}{a - a'},$$

which intersects $E$ at $x^3 - \left(\lambda^2 - A\right)x^2 + (B - 2\lambda\mu)x - \mu^2 = 0$. Let $P * Q = -(P + Q) = (a'', -b'')$. Thus comparing coefficients gives $\mu^2 = aa'a''$.

3. The tangent at $P$ is

$$L : y = \lambda x + \mu, \qquad \lambda = \frac{3a^2 + 2Aa + B}{2b}, \qquad \mu = \frac{b^2 - Aa^2 - 2Ba}{2b},$$

which intersects $E$ at $x^3 - \left(\lambda^2 - A\right)x^2 + (B - 2\lambda\mu)x - \mu^2 = 0$. Let $P * P = -2P = (a', -b')$, so comparing coefficients gives $\lambda^2 - A = 2a + a'$. Thus

$$2P = \left(\lambda^2 - A - 2a, \mu - \lambda\left(\lambda^2 - A - 2a\right)\right) \in E(\mathbb{Q}).$$

□

The above proof is brief but can be verified manually. Let a related curve be

$$E' : y^2 = x^3 + A'x^2 + B'x, \qquad A' = -2A, \qquad B' = A^2 - 4B,$$

such that $T \in E'$ and $B' \neq 0$. Then $A'^2 - 4B' = (-2A)^2 - 4\left(A^2 - 4B\right) = 16B$, and the group law is similar to that of $E$ but with $A'$ and $B'$ instead of $A$ and $B$. Now let the two maps $\phi : E \to E'$ and $\psi : E' \to E$ be defined by

$$\phi(P) = \begin{cases} \left(\dfrac{b^2}{a^2}, \dfrac{b\left(a^2 - B\right)}{a^2}\right) & P = (a, b) \neq T \\ \mathcal{O} & P \in \{\mathcal{O}, T\} \end{cases}, \qquad \psi(P) = \begin{cases} \left(\dfrac{b^2}{4a^2}, \dfrac{b\left(a^2 - B'\right)}{8a^2}\right) & P = (a, b) \neq T \\ \mathcal{O} & P \in \{\mathcal{O}, T\} \end{cases}.$$

These two maps are related in the obvious way, where one can be seen as the scaling of the other. They also relate the two elliptic curves, as seen in the following lemma.

**Lemma 3.6.3.** $\phi : E \to E'$ and $\psi : E' \to E$ are isogenies such that $\psi \circ \phi = [2]_E$ and $\phi \circ \psi = [2]_{E'}$.

**Remark.** Preserving the point at infinity induces a group homomorphism, but the full property can be tediously verified in III.4 of [3] for each case of the group law.

*Proof.* For any point $P = (a, b) \in E$,

$$\left(\frac{b^2}{a^2}\right)^3 + A'\left(\frac{b^2}{a^2}\right)^2 + B'\frac{b^2}{a^2} = \frac{b^2}{a^4}\left(\frac{\left(b^2 - Aa^2\right)^2 - 4Ba^4}{a^2}\right) = \frac{b^2}{a^4}\left(\frac{\left(a^3 + Ba\right)^2 - 4Ba^4}{a^2}\right) = \left(\frac{b\left(a^2 - B\right)}{a^2}\right)^2,$$

so $\phi(P) \in E'$. Since $\phi(T) = \phi(\mathcal{O}) = \mathcal{O}$, it holds that $\phi$ is a well-defined non-constant morphism, and hence an isogeny. Since $\psi$ can be seen as applying $\chi \circ \phi$ to $E$, where $\chi$ is the $j$-invariant affine transformation $(x, y) \mapsto (x/4, y/8)$, it is also a well-defined non-constant morphism, and hence an isogeny. Now let $P \in E$. If $P = \mathcal{O}$ or $P = (a, 0)$, then $(\psi \circ \phi)(P) = \mathcal{O} = 2P$. Otherwise $P = (a, b)$ such that $a \neq 0$ and $b \neq 0$, then

$$\begin{aligned}(\psi \circ \phi)(P) &= \left(\frac{\left(b\left(a^2 - B\right)/a^2\right)^2}{4\left(b^2/a^2\right)^2}, \frac{\left(b\left(a^2 - B\right)/a^2\right)\left(\left(b^2/a^2\right)^2 - B'\right)}{8\left(b^2/a^2\right)^2}\right) \\ &= \left(\frac{\left(a^2 - B\right)^2}{4b^2}, \frac{\left(a^2 - B\right)\left(b^4 - \left(A^2 - 4B\right)a^4\right)}{8b^3a^2}\right) \\ &= \left(\frac{\left(a^2 - B\right)^2}{4b^2}, \frac{\left(a^2 - B\right)\left(a^4 + B^2 + 2Aa^3 + 2ABa + 6Ba^2\right)}{8b^3}\right) = 2P.\end{aligned}$$

Hence $\psi \circ \phi = [2]_E$. Similarly let $P' \in E'$. If $P' = \mathcal{O}$ or $P' = (a, 0)$, then $(\phi \circ \psi)(P') = \mathcal{O} = 2P'$. Otherwise $P' = (a, b)$ such that $a \neq 0$ and $b \neq 0$, then

$$\begin{aligned}(\phi \circ \psi)(P') &= \left(\frac{\left(b\left(a^2 - B'\right)/8a^2\right)^2}{\left(b^2/4a^2\right)^2}, \frac{\left(b\left(a^2 - B'\right)/8a^2\right)\left(\left(b^2/4a^2\right)^2 - B\right)}{\left(b^2/4a^2\right)^2}\right) \\ &= \left(\frac{\left(a^2 - B'\right)^2}{4b^2}, \frac{\left(a^2 - B'\right)\left(b^4 - 16\left(\left(A'^2 - 4B'\right)/16\right)a^4\right)}{8b^3a^2}\right) \\ &= \left(\frac{\left(a^2 - B'\right)^2}{4b^2}, \frac{\left(a^2 - B'\right)\left(a^4 + B'^2 + 2A'a^3 + 2A'B'a + 6B'a^2\right)}{8b^3}\right) = 2P'.\end{aligned}$$

Thus $\phi \circ \psi = [2]_{E'}$. □

Hence the multiplication by 2 map can be decomposed into two isogenies $\phi$ and $\psi$. As only the image of these isogenies will be used, their standard forms will not be used to prevent confusion.

**Remark.** These two isogenies are *dual isogenies* to each other. Any isogeny of degree $n \in \mathbb{Z}_{>0}$ has a dual isogeny, which composes with it to give two multiplication by $n$ maps in their respective domains.

The image of the isogeny $\psi$ depends on whether $B$ is a perfect square or whether $x$ coordinates are in the normal subgroup $(\mathbb{Q}^*)^2 = \{q^2 \mid q \in \mathbb{Q}^*\}$. In particular, the equation $x^3 + A'x + B' = 0$ with discriminant $16\left(A'^2 - 4B'\right) = 16B$ has two solutions in $\mathbb{Q}^*$ iff $16B \in (\mathbb{Z}^*)^2$, or $B \in (\mathbb{Z}^*)^2$, stated as follows.

**Lemma 3.6.4.** The image $Im(\psi)$ is such that:

- $\mathcal{O} \in Im(\psi)$,
- $T \in Im(\psi)$ iff $B \in (\mathbb{Z}^*)^2$, and
- $(a, b) \neq T \in Im(\psi)$ iff $a \in (\mathbb{Q}^*)^2$.

*Proof.* Since $\psi(\mathcal{O}) = \mathcal{O}$, it holds that $\mathcal{O} \in Im(\psi)$. Now $T \in Im(\psi)$ iff there is a point $P = (a, b) \in E'(\mathbb{Q})$ such that $\psi(P) = T$ and $0 = b^2/4a^2$. This holds iff $a \in \mathbb{Q}^*$ and $b = 0$, or $B \in (\mathbb{Z}^*)^2$. Now assume that $P = (a, b) \neq T \in Im(\psi)$. Then there is a point $Q = (a', b') \in E'(\mathbb{Q})$ such that $\psi(Q) = P$, so $a = b'^2/4a'^2 = (b'/2a)^2 \in (\mathbb{Q}^*)^2$. Conversely assume that $P = (a, b) \neq T \in E(\mathbb{Q})$ and $a \in (\mathbb{Q}^*)^2$. Then $a = c^2$ for some $c \in \mathbb{Q}^*$, so

$$b^2 = c^6 - \frac{A'c^4}{2} + \frac{A'^2 - 4B'}{16}c^2 \qquad \implies \qquad B' = \left(2c^2 - \frac{A'}{2} + \frac{2b}{c}\right)\left(2c^2 - \frac{A'}{2} - \frac{2b}{c}\right).$$

Now let $Q = (a', b')$, where $a' = 2c^2 - A'/2 + 2b/c$ and $b' = 2a'c$, such that $B' = a'(a' - 4b/c)$. Then

$$a'^3 + A'a'^2 + B'a' = a'^3 + A'a'^2 + a'^2\left(a' - \frac{2b}{c}\right) = 2a'^2\left(a' + \frac{A'}{2} - \frac{4b}{c}\right) = 4a'^2c^2 = b'^2,$$

so $Q \in E'(\mathbb{Q})$, and

$$\psi(Q) = \left(\frac{b'^2}{4a'^2}, \frac{b'\left(a'^2 - B'\right)}{8a'^2}\right) = \left(\frac{4a'^2c^2}{4a'^2}, \frac{2a'c\left(a'^2 - a'\left(a' - 4b/c\right)\right)}{8a'^2}\right) = \left(c^2, \frac{c\left(4a'b/c\right)}{4a'}\right) = (a, b) = P.$$

Thus $P \in Im(\psi)$. □

The image of the isogeny $\phi$ can be characterised analogously, and will not be explicitly stated here. Now let another map be defined as

$$\alpha : E(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2, \qquad \alpha(P) = \begin{cases} (\mathbb{Q}^*)^2 a & P = (a, b) \neq T \\ (\mathbb{Q}^*)^2 B & P = T \\ (\mathbb{Q}^*)^2 & P = \mathcal{O} \end{cases}.$$

Then $\psi$ and $\alpha$ induce an *exact sequence* $E'(\mathbb{Q}) \xrightarrow{\psi} E(\mathbb{Q}) \xrightarrow{\alpha} \mathbb{Q}^*/(\mathbb{Q}^*)^2$, which can be stated more concretely in the following lemma.

**Lemma 3.6.5.** $\alpha : E(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ is a group homomorphism such that $Im(\psi) = Ker(\alpha)$.

*Proof.* Let $P, Q \in E(\mathbb{Q})$ be points. If $P = \mathcal{O}$,

$$\alpha(P)\alpha(Q) = (\mathbb{Q}^*)^2\alpha(Q) = \alpha(Q) = \alpha(P + Q),$$

or similar for $Q = \mathcal{O}$. If $P = (a, b)$ and $Q = (a', b')$ such that $a \neq a'$ and $P + Q = (a'', b'') \in E(\mathbb{Q})$, then

$$\alpha(P)\alpha(Q) = (\mathbb{Q}^*)^2 a(\mathbb{Q}^*)^2 a' = (\mathbb{Q}^*)^2 aa' = (\mathbb{Q}^*)^2 \frac{\mu^2}{a''} = (\mathbb{Q}^*)^2 \mu^2 a'' = (\mathbb{Q}^*)^2 a'' = \alpha(P + Q).$$

Otherwise $P = (a, b)$ and $Q = (a, b')$, then

$$\alpha(P)\alpha(Q) = (\mathbb{Q}^*)^2 a(\mathbb{Q}^*)^2 a = (\mathbb{Q}^*)^2 a^2 = (\mathbb{Q}^*)^2 = (\mathbb{Q}^*)^2 \frac{\left(a^2 - B\right)^2}{4b^2} = \alpha(P + Q).$$

Hence $\alpha$ is a group homomorphism. Now $\mathcal{O} \in Ker(\alpha)$, the point $T \in Ker(\alpha)$ iff $B \in (\mathbb{Q}^*)^2$, and a point $(a, b) \neq T \in Ker(\alpha)$ iff $a \in (\mathbb{Q}^*)^2$. Thus $Im(\psi) = Ker(\alpha)$. □

The image of the group homomorphism $\alpha$ can again be characterised, as being contained in a finite subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. Now let $S(B)$ be the set of primes $p \in \mathbb{Z}_{>0}$ such that $p \mid B$, and let

$$G(B) = \left\{ (\mathbb{Q}^*)^2 \left( \prod_{p \in S} p \right) \;\middle|\; S \subseteq S(B) \right\} \cup \left\{ (\mathbb{Q}^*)^2 \left( -\prod_{p \in S} p \right) \;\middle|\; S \subseteq S(B) \right\}.$$

Recalling the fact that for any point $(a, b) \in E(\mathbb{Q})$,

$$a = p/d^2, \qquad b = q/d^3, \qquad p, q \in \mathbb{Z}, \qquad d \in \mathbb{Z}_{>0},$$

such that $\gcd(p, d) = \gcd(q, d) = 1$, the following lemma characterises $\alpha$.

**Lemma 3.6.6.** $G(B)$ is a group such that $|G(B)| = 2^{|S(B)|+1}$ and $Im(\alpha) \leq G(B) \leq \mathbb{Q}^*/(\mathbb{Q}^*)^2$.

*Proof.* Since $\emptyset \subseteq S(B)$, it holds that $(\mathbb{Q}^*)^2 \in G(B)$. Let $a, b \in G(B)$. Then

$$a = (\mathbb{Q}^*)^2 j p_1 \dots p_n p'_1 \dots p'_{n'}, \qquad b = (\mathbb{Q}^*)^2 j' p_1 \dots p_n p''_1 \dots p''_{n''}$$

for some $j, j' \in \{-1, 1\}$ and some distinct primes $p_i, p'_i, p''_i \in S(B)$, so

$$\frac{a}{b} = \frac{(\mathbb{Q}^*)^2 j p_1 \dots p_n p'_1 \dots p'_{n'}}{(\mathbb{Q}^*)^2 j' p_1 \dots p_n p''_1 \dots p''_{n''}} = (\mathbb{Q}^*)^2 \frac{j p'_1 \dots p'_{n'}}{j' p''_1 \dots p''_{n''}} = (\mathbb{Q}^*)^2 j j' p'_1 \dots p'_{n'} p''_1 \dots p''_{n''} \in G(B).$$

Hence $G(B) \leq \mathbb{Q}^*/(\mathbb{Q}^*)^2$ and $|G(B)| = 2^{|S(B)|} + 2^{|S(B)|} = 2^{|S(B)|+1}$. Now let $P \in E(\mathbb{Q})$ be a point. If $P = \mathcal{O}$, then $\alpha(P) = (\mathbb{Q}^*)^2 \in G(B)$. If $P = T$, then $\alpha(P) = (\mathbb{Q}^*)^2 B \in G(B)$. Otherwise $P = (a, b) \neq T$, then $a = r/d^2$ and $b = s/d^3$ for some $r, s \in \mathbb{Z}$ and some $d \in \mathbb{Z}_{>0}$ such that $\gcd(r, d) = \gcd(s, d) = 1$ and $s^2 = r^3 + Ar^2 d^2 + Brd^4 = r\left(r^2 + Ard^2 + Bd^4\right)$. Let $g = \gcd\left(r, r^2 + Ard^2 + Bd^4\right)$, then $r = cg$ and $r^2 + Ard^2 + Bd^4 = c'g$ for some $c, c' \in \mathbb{Z}_{\geq 0}$ such that $\gcd(c, c') = 1$. Since $s^2 = (cg)(c'g) = cc'g^2$, it holds that $(s/g)^2 = cc'$, so $c = kq_1^2 \cdots q_m^2$ for some $k \in \{-1, 1\}$ and some primes $q_i \in \mathbb{Z}_{>0}$. Since $g \mid r$ and $g \mid Bd^4$, it also holds that $g \mid B$, so $g = k' q'_1 \dots q'_{m'}$ for some $k' \in \{-1, 1\}$ and some primes $q'_i \in \mathbb{Z}_{>0}$ such that $q'_i \mid B$, and hence $q'_i \in S(B)$. Hence

$$\alpha(P) = (\mathbb{Q}^*)^2 a = (\mathbb{Q}^*)^2 \frac{r}{d^2} = (\mathbb{Q}^*)^2 \frac{k k' q_1^2 \cdots q_m^2 q'_1 \dots q'_{m'}}{d^2} = (\mathbb{Q}^*)^2 k k' q'_1 \dots q'_{m'} \in G(B).$$

Thus $Im(\alpha) \leq G(B)$. □

A similar group homomorphism $\alpha' : E'(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ can again be characterised analogously, and will not be explicitly stated here. The weak theorem can then be proven here, for the special case of a rational 2-torsion point.

*Proof of Theorem 3.6.1.* The first isomorphism theorem with the preceding lemmas give two inclusions

$$\frac{E(\mathbb{Q})}{Im(\psi)} = \frac{E(\mathbb{Q})}{Ker(\alpha)} \cong Im(\alpha) \leq G(B), \qquad \frac{E'(\mathbb{Q})}{Im(\phi)} = \frac{E'(\mathbb{Q})}{Ker(\alpha')} \cong Im(\alpha') \leq G(B'),$$

which give finite indices

$$n = |E(\mathbb{Q}) : Im(\psi)| \leq |G(B)| = 2^{|S(B)|+1}, \qquad m = |E'(\mathbb{Q}) : Im(\phi)| \leq |G(B')| = 2^{|S(B')|+1}.$$

Let $P_1, \dots, P_n \in E(\mathbb{Q})$ be representative points such that $Im(\psi) + P_i \in E(\mathbb{Q})/Im(\psi)$ are distinct cosets, and let $Q_1, \dots, Q_m \in E'(\mathbb{Q})$ be representative points such that $Im(\phi) + Q_i \in E'(\mathbb{Q})/Im(\phi)$ are distinct cosets. Now let $P \in E(\mathbb{Q})$ be a point. Then $Im(\psi) + P = Im(\psi) + P_j$ for some $j \in \{1, \dots, n\}$, so $P = \psi(Q) + P_j$ for some $Q \in E'(\mathbb{Q})$ and $\psi(Q) \in Im(\psi)$. Similarly $Im(\phi) + Q = Im(\phi) + Q_k$ for some $k \in \{1, \dots, m\}$, so $Q = \phi(P') + Q_k$ for some $P' \in E(\mathbb{Q})$ and $\phi(P') \in Im(\phi)$. Hence

$$P = \psi(Q) + P_j = \psi(\phi(P') + Q_k) + P_j = \psi(\phi(P')) + \psi(Q_k) + P_j \in 2E(\mathbb{Q}) + \psi(Q_k) + P_j,$$

and $\psi(Q_k) + P_j \in E(\mathbb{Q})$ represent all cosets in $E(\mathbb{Q})/2E(\mathbb{Q})$. Thus

$$|E(\mathbb{Q}) : 2E(\mathbb{Q})| \leq nm = 2^{(|S(B)|+1)\left(|S(B')|+1\right)}$$

is finite. □

The proof of Mordell's theorem is now complete.

## 3.7 Rank computation

A direct application of Mordell's theorem would be the fundamental theorem of finite abelian groups,

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus \bigoplus_{i=1}^{m} \mathbb{Z}_{n_i}, \qquad r, m \in \mathbb{Z}_{\geq 0}, \qquad n_i \in \mathbb{Z}_{>1},$$

such that each $n_i \mid n_{i+1}$. Thus for any point $P \in E(\mathbb{Q})$,

$$P = \sum_{i=1}^{r} r_i P_i + \sum_{i=1}^{m} m_i Q_i, \qquad r_i \in \mathbb{Z}, \qquad m_i \in \mathbb{Z}_{n_i}, \qquad P_i, Q_i \in E(\mathbb{Q}).$$

While the torsion subgroup can be easily computed, the rank $r$ is generally difficult to compute, and can only be made slightly easier with Mordell's theorem. Noting that $\bigoplus_i (G_i/H_i) \cong \left(\bigoplus_i G_i\right) / \left(\bigoplus_i H_i\right)$ for any groups $G_i, H_i$, the following proposition gives a direct formula for the rank.

**Proposition 3.7.1.** The rank $r = rk(E(\mathbb{Q}))$ is such that

$$2^r = \tfrac{1}{4} |Im(\alpha)| \, |Im(\alpha')|.$$

*Proof.* The fundamental theorem of finite abelian groups gives

$$\frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \cong \frac{\mathbb{Z}^r \oplus \bigoplus_{i=1}^{m} \mathbb{Z}_{n_i}}{r2\mathbb{Z} \oplus \bigoplus_{i=1}^{m} 2\mathbb{Z}_{n_i}} \cong r\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right) \oplus \bigoplus_{i=1}^{m} \frac{\mathbb{Z}_{n_i}}{2\mathbb{Z}_{n_i}}.$$

Then $\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2$. If $n_i \nmid 2$, then $2^{-1} \in \mathbb{Z}_{n_i}$, so $\mathbb{Z}_{n_i} \cong 2\mathbb{Z}_{n_i}$ and $\mathbb{Z}_{n_i}/2\mathbb{Z}_{n_i} \cong 0$, otherwise $n_i \mid 2$. Now $P \in E(\mathbb{Q})[2]$ iff $2P = 0$, or each $r_i = 0$ and each $2m_i = 0 \mod n_i$, which holds iff $m_i = 0$ or $n_i \mid 2$, so $E(\mathbb{Q})[2] = \bigoplus_{n_i \mid 2} \mathbb{Z}_{n_i}$. Hence

$$\frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \cong \mathbb{Z}_2^r \oplus E(\mathbb{Q})[2] \qquad \implies \qquad |E(\mathbb{Q}) : 2E(\mathbb{Q})| = 2^r |E(\mathbb{Q})[2]|.$$

Now let $\theta : E'(\mathbb{Q}) \to Im(\psi)/2E(\mathbb{Q})$ be a surjective group homomorphism defined by $\theta(P) = 2E(\mathbb{Q}) + \psi(P)$. Then $P \in Ker(\theta)$ iff $\psi(P) \in 2E(\mathbb{Q})$, or $\psi(P) = \psi(\phi(Q))$ for some $Q \in E(\mathbb{Q})$. This holds iff $\psi(P - \phi(Q)) = 0$, or $P - \phi(Q) \in Ker(\psi)$ and $P \in Ker(\psi) + Im(\phi)$. Then the three isomorphism theorems with $Ker(\theta) = Ker(\psi) + Im(\phi)$ give

$$\frac{Im(\psi)}{2E(\mathbb{Q})} \cong \frac{E'(\mathbb{Q})}{Ker(\psi) + Im(\phi)} \cong \frac{\frac{E'(\mathbb{Q})}{Im(\phi)}}{\frac{Ker(\psi) + Im(\phi)}{Im(\phi)}} \cong \frac{\frac{E'(\mathbb{Q})}{Im(\phi)}}{\frac{Ker(\psi)}{Ker(\psi) \cap Im(\phi)}}.$$

Hence

$$|E(\mathbb{Q}) : 2E(\mathbb{Q})| = \frac{|E(\mathbb{Q}) : Im(\psi)| \, |E'(\mathbb{Q}) : Im(\phi)|}{|Ker(\psi) : Ker(\psi) \cap Im(\phi)|} = \frac{|Im(\alpha)| \, |Im(\alpha')|}{|Ker(\psi) : Ker(\psi) \cap Im(\phi)|}.$$

Now $B' \in (\mathbb{Z}^*)^2$ iff $T \in Im(\phi)$ and the equation $x^2 + Ax + B = 0$ with discriminant $16\left(A^2 - 4B^2\right) = 16B'$ has solutions in $\mathbb{Z}^*$. Since $Ker(\psi) = \{\mathcal{O}, T\}$ and $\mathcal{O} \in Im(\phi)$, this holds iff $Ker(\psi) \cap Im(\phi) = \{\mathcal{O}, T\}$. Since $\mathcal{O}, T \in E(\mathbb{Q})[2]$, this also holds iff $(a, 0), (a', 0) \in E(\mathbb{Q})[2]$ for the solutions $a, a' \in \mathbb{Q}^*$ of $x^2 + Ax + B = 0$. Hence

$$E(\mathbb{Q})[2] = \begin{cases} \{\mathcal{O}, T, (a,0), (a',0)\} & B' \in (\mathbb{Z}^*)^2 \\ \{\mathcal{O}, T\} & B' \notin (\mathbb{Z}^*)^2 \end{cases}, \qquad \frac{Ker(\psi)}{Ker(\psi) \cap Im(\phi)} = \begin{cases} \{\mathcal{O}\} & B' \in (\mathbb{Z}^*)^2 \\ \{\mathcal{O}, T\} & B' \notin (\mathbb{Z}^*)^2 \end{cases},$$

so $|Ker(\psi) : Ker(\psi) \cap Im(\phi)| \, |E(\mathbb{Q})[2]| = 4$. Thus

$$2^r = \frac{|Im(\alpha)| \, |Im(\alpha')|}{|Ker(\psi) : Ker(\psi) \cap Im(\phi)| \, |E(\mathbb{Q})[2]|} = \tfrac{1}{4} |Im(\alpha)| \, |Im(\alpha')|.$$

□

Computation of the rank simply reduces to determining images of $\alpha$ and $\alpha'$. This in turn can be rephrased as a question of Diophantine equations.

**Proposition 3.7.2.** The image $Im(\alpha)$ is such that

$$Im(\alpha) = \left\{ (\mathbb{Q}^*)^2 \beta \;\middle|\; \beta, B/\beta \in \mathbb{Z}^*,\ (X,Y,Z) \in \mathbb{Z}^3 \setminus \{(0,0,0)\},\ Y^2 = \beta X^4 + AX^2Z^2 + (B/\beta) Z^4 \right\}.$$

*Proof.* Since $(\mathbb{Q}^*)^2 \in Im(\alpha)$, there is a solution $(X,Y,Z) = (1,1,0)$ for $\beta = 1$. Since $(\mathbb{Q}^*)^2 B \in Im(\alpha)$, there is also a solution $(X,Y,Z) = (0,1,1)$ for $\beta = B$. Let $P = (a,b) \neq T \in E(\mathbb{Q})$ such that $(\mathbb{Q}^*)^2 a \in Im(\alpha)$. Then $a = r/Z_0^2$ and $b = s/Z_0^3$ for some $r, s \in \mathbb{Z}$ and some $Z_0 \in \mathbb{Z}_{>0}$ such that $\gcd(r, Z_0) = \gcd(s, Z_0) = 1$. Now let $r = X_0^2 \beta_0$, where $X_0 = p_1 \dots p_n \in \mathbb{Z}_{>0}$ for some primes $p_i \in \mathbb{Z}_{>0}$ and $\beta_0 = j q_1 \dots q_n$ for some $j \in \{-1, 1\}$ and some distinct primes $q_i \in \mathbb{Z}_{>0}$. Since $(\mathbb{Q}^*)^2 \beta_0 = (\mathbb{Q}^*)^2 X_0^2 \beta_0 / Z_0^2 = (\mathbb{Q}^*)^2 \beta_0 \in G(B)$, each $q_i \mid B$, so $\beta_0 \mid B$ and hence $B/\beta_0 \in \mathbb{Z}^*$. Then

$$\left(\frac{s}{Z_0^3}\right)^2 = \left(\frac{X_0^2\beta_0}{Z_0^2}\right)^3 + A\left(\frac{X_0^2\beta_0}{Z_0^2}\right)^2 + B\frac{X_0^2\beta_0}{Z_0^2} \qquad \Longrightarrow \qquad s^2 = \beta_0^2 X_0^2 \left(\beta_0 X_0^4 + AX_0^2 Z_0^2 + (B/\beta_0) Z_0^4\right),$$

so let $Y_0 = s^2/\beta_0^2 X_0^2 \in \mathbb{Z}$ such that $Y_0^2 = \beta_0 X_0^4 + AX_0^2 Z_0^2 + (B/\beta_0) Z_0^4$. Hence there is a non-zero solution $(X,Y,Z) = (X_0, Y_0, Z_0)$ for $\beta = \beta_0$. Conversely let $(X,Y,Z) = (X_0, Y_0, Z_0)$ be a non-zero solution for some $\beta = \beta_0 \in \mathbb{Z}^*$, so $Y_0^2 = \beta_0 X_0^4 + AX_0^2 Z_0^2 + (B/\beta_0) Z_0^4$. Then $P = \left(\beta_0 X_0^2/Z_0^2, \beta_0 X_0 Y_0/Z_0^3\right)$ is such that

$$\left(\frac{\beta_0 X_0 Y_0}{Z_0^3}\right)^2 = \frac{\beta_0^2 X_0^2 \left(\beta_0 X_0^4 + AX_0^2 Z_0^2 + (B/\beta_0) Z_0^4\right)}{Z_0^6} = \left(\frac{\beta_0 X_0^2}{Z_0^2}\right)^3 + A\left(\frac{\beta_0 X_0^2}{Z_0^2}\right)^2 + B\frac{\beta_0 X_0^2}{Z_0^2},$$

so $P \in E(\mathbb{Q})$ and $\alpha(P) = (\mathbb{Q}^*)^2 \left(\beta_0 X_0^2/Z_0^2\right) = (\mathbb{Q}^*)^2 \beta_0$. Thus any non-zero solution is in $Im(\alpha)$. □

Again, the image of $\alpha'$ is similar to that of $\alpha$ but with $B'$ instead of $B$. The following example illustrates the full computation of the rank of a simple elliptic curve.

**Example.** Let $E : y^2 = x^3 - x$ be an elliptic curve over $\mathbb{Q}$. Then $\beta \in \{\pm 1\}$. Since $\beta = 1$ and $\beta = -1 = B$ have solutions, it holds that $|Im(\alpha)| = 2$. Now $E' : y^2 = x^3 + 4x$ gives $\beta \in \{\pm 1, \pm 2, \pm 4\}$. Since $(\mathbb{Q}^*)^2 (\pm 1) = (\mathbb{Q}^*)^2 (\pm 4)$, the Diophantine equations to consider are:

1. $\beta = 1$ gives $Y^2 = X^4 + 4Z^4$, which has a solution $(X,Y,Z) = (0,2,1)$.
2. $\beta = 2$ gives $Y^2 = 2X^4 + 2Z^4$, which has a solution $(X,Y,Z) = (1,2,1)$.
3. $\beta = -1$ gives $Y^2 = -X^4 - 4Z^4$, which has no solutions by sign disparity.
4. $\beta = -2$ gives $Y^2 = -2X^4 - 2Z^4$, which has no solutions by sign disparity.

Hence $|Im(\alpha')| = 2$ and $2^r = \frac{1}{4}(2)(2) = 1$. Thus $rk(E(\mathbb{Q})) = 0$ and $E(\mathbb{Q}) = E(\mathbb{Q})_{tors} \cong \mathbb{Z}_2$.

The following algorithm summarises the process and code in the appendix.

**Algorithm 3.7.3** (Computation of the rank)**.** Input: an elliptic curve $E$ over $\mathbb{Q}$. Output: $rk(E(\mathbb{Q}))$.

1. Get all positive $\beta$ such that $\beta \mid B$ and free the squares from each $\beta$.
2. Print all Diophantine equations of the form $Y^2 = \beta X^4 + AX^2Z^2 + (B/\beta) Z^4$.
3. Write down the elliptic curve $E' : y^2 = x^3 - 2Ax^2 + \left(A^2 - 4B\right) x$ and do the same.
4. Check if there are non-zero solutions to the systems of Diophantine equations.
5. Compute the rank with the formula $rk(E(\mathbb{Q})) = \log_2 |Im(\alpha)| + \log_2 |Im(\alpha')| - 2$.

Unfortunately, there are no known effective method for the second to last step. In contrast to attempting at a number theoretic algorithm like in [12], only ad-hoc congruences will be used to complete the computations in the following examples of elliptic curves given by the Weierstrass equations $y^2 = x^3 - px$ for $p \in \mathbb{Z}_{>0}$. The following example is an elliptic curve of rank one.

**Example.** Let $E : y^2 = x^3 - 5x$ be an elliptic curve over $\mathbb{Q}$, which gives $\beta \in \{\pm 1, \pm 5\}$. Since $\beta = 1$ and $\beta = -5$ have trivial solutions, the Diophantine equations to consider are $Y^2 = -X^4 + 5Z^4$, which has a solution $(X, Y, Z) = (1, 2, 1)$, and $Y^2 = 5X^4 - Z^4$, which has a solution by symmetry. Hence $|Im(\alpha)| = 4$. Now $E' : y^2 = x^3 + 20x$ gives $\beta \in \{\pm 1, \pm 2, \pm 5, \pm 10\}$. If $\beta < 0$, there are no solutions by sign disparity. Since $\beta = 1$ and $\beta = 5$ have trivial solutions, the Diophantine equations to consider are $Y^2 = 2X^4 + 10Z^4$ and $Y^2 = 10X^4 + 2Z^4$. Since $\gcd(X_0, Y_0) = 1$, if the first has a solution $(X, Y, Z) = (X_0, Y_0, Z_0)$, then $Y_0^2 \equiv 2X_0^4 \equiv 2 \mod 5$ gives no solutions for $Y_0$, so both equations have no solutions. Hence $|Im(\alpha')| = 2$. Thus $rk(E(\mathbb{Q})) = \log_2(4) + \log_2(2) - 2 = 1$ and $E(\mathbb{Q}) \cong \mathbb{Z} \oplus E(\mathbb{Q})_{tors} \cong \mathbb{Z} \times \mathbb{Z}_2$.

The following example is an elliptic curve of rank two.

**Example.** Let $E : y^2 = x^3 - 17x$ be an elliptic curve over $\mathbb{Q}$, which gives $\beta \in \{\pm 1, \pm 17\}$. Since $\beta = 1$ and $\beta = -17$ have trivial solutions, the Diophantine equations to consider are $Y^2 = -X^4 + 17Z^4$, which has a solution $(X, Y, Z) = (1, 4, 1)$, and $Y^2 = 17X^4 - Z^4$, which has a solution by symmetry. Hence $|Im(\alpha)| = 4$. Now $E' : y^2 = x^3 + 68x$ gives $\beta \in \{\pm 1, \pm 2, \pm 17, \pm 34\}$. If $\beta < 0$, there are no solutions by sign disparity. Since $\beta = 1$ and $\beta = 17$ have trivial solutions, the Diophantine equations to consider are $Y^2 = 2X^4 + 34Z^4$, which has a solution $(X, Y, Z) = (1, 6, 1)$, and $Y^2 = 34X^4 + 2Z^4$, which has a solution by symmetry. Hence $|Im(\alpha')| = 4$. Thus $rk(E(\mathbb{Q})) = \log_2(4) + \log_2(4) - 2 = 2$ and $E(\mathbb{Q}) \cong \mathbb{Z}^2 \oplus E(\mathbb{Q})_{tors} \cong \mathbb{Z}^2 \times \mathbb{Z}_2$.

The following example is an elliptic curve of rank three.

**Example.** Let $E : y^2 = x^3 - 226x$ be an elliptic curve over $\mathbb{Q}$, which gives $\beta \in \{\pm 1, \pm 2, \pm 113, \pm 226\}$. Since $\beta = 1$ and $\beta = -226$ have trivial solutions, the Diophantine equations to consider are $Y^2 = -X^4 + 226Z^4$, $Y^2 = 2X^4 - 113Z^4$, $Y^2 = -2X^4 + 113Z^4$, $Y^2 = 113X^4 - 2Z^4$, $Y^2 = -113X^4 + 2Z^4$, and $Y^2 = 226X^4 - Z^4$. The first three have solutions $(X, Y, Z) = (1, 15, 1)$, $(X, Y, Z) = (3, 7, 1)$, and $(X, Y, Z) = (1, 9, 2)$ respectively, while the last three have solutions by symmetry. Hence $|Im(\alpha)| = 8$. Now $E' : y^2 = x^3 + 904x$ gives $\beta \in \{\pm 1, \pm 2, \pm 113, \pm 226\}$. If $\beta < 0$, there are no solutions by sign disparity. Since $\beta = 1$ and $\beta = 226$ have trivial solutions, the Diophantine equations to consider are $Y^2 = 2X^4 + 452Z^4$, which has a solution $(X, Y, Z) = (1, 22, 2)$, and $Y^2 = 113X^4 + 8Z^4$, which has a solution $(X, Y, Z) = (1, 11, 1)$. Hence $|Im(\alpha')| = 4$. Thus $rk(E(\mathbb{Q})) = \log_2(8) + \log_2(4) - 2 = 3$ and $E(\mathbb{Q}) \cong \mathbb{Z}^3 \oplus E(\mathbb{Q})_{tors} \cong \mathbb{Z}^3 \times \mathbb{Z}_2$.

The ranks of elliptic curves above are relatively small in value and easy to compute, but there are elliptic curves with larger rank values. The record as of 2018 in [13] for the elliptic curve with the largest rank was discovered by Elkies in 2006, and is given by the Weierstrass curve

$$E : y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x$$

$$+3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9,$$

which is proven to have rank at least 28. There are also elliptic curves with relatively large ranks known exactly, the largest of which was also discovered by Elkies in 2009, and is given by the Weierstrass curve

$$E : y^2 + xy + y = x^3 - x^2 + 31368015812338065133318565292206590792820353345x$$

$$+30203880269856608733564318842954349862452204168387449355518606256815984 7,$$

which has rank 19. In fact, it is conjectured that the rank of an elliptic curve does not have an upper bound.

**Conjecture 3.7.4.** There are elliptic curves over $\mathbb{Q}$ of arbitrary large rank.

However, while they exist, elliptic curves of rank greater than one are rare. This notion of rarity is measured by the *average rank* of all elliptic curves, of which is conjectured to exist as a quantity.

**Conjecture 3.7.5.** The average rank of all elliptic curves over $\mathbb{Q}$ is $\frac{1}{2}$.

In particular, rank zero constitute a half and rank one constitute the other half, while all higher ranks constitute zero percent, of all elliptic curves. While it has not been definitely proven, Bhargava and Shankar showed in [14] that the average rank of all elliptic curves is at most $7/6$.

## 3.8 Birch and Swinnerton-Dyer conjecture

Ultimately, the rank of an elliptic curve is not completely understood. It was greatly studied for decades, and had lead mathematicians to formalise one of the most influential conjectures in number theory, which is also deemed worthy of being called one of the Millennium Prize Problems. The problem, now commonly known as the *Birch and Swinnerton-Dyer conjecture*, relates the rank with Taylor expansion of a particular complex series. Letting $t_p$ denote the trace in Hasse's theorem applied to $E_p(\mathbb{F}_p)$ for any prime $p \in \mathbb{Z}_{>0}$ of good reduction, the series can be given as follows.

**Definition** (Incomplete Hasse-Weil $L$-series)**.** The **incomplete Hasse-Weil $L$-series** is defined for any $\Re(s) > 3/2$ as the *Euler product*

$$L(E,s) = \prod_p \frac{1}{1 - t_p p^{-s} + p^{1-2s}}$$

over all primes $p \in \mathbb{Z}_{>0}$ of good reduction, and extended to $\mathbb{C}$ by analytic continuation.

This analytic continuation, as well as a functional equation similar to that of the Riemann zeta function, was originally known as the *Hasse-Weil conjecture*, but was subsequently implied by the *modularity theorem*.

**Remark.** The *complete Hasse-Weil $L$-series* is defined over all primes $p \in \mathbb{Z}_{>0}$ as the Euler product

$$L^*(E,s) = \prod_{p \mid \Delta_E} \frac{1}{1 - t_p p^{-s}} \prod_{p \nmid \Delta_E} \frac{1}{1 - t_p p^{-s} + p^{1-2s}} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Now $E$ might be a singular cubic curve, so that $t_p$ can be defined for primes of bad reduction as either $t_p = \pm 1$ or $t_p = 0$, depending on whether $E$ has *split* or *non-split multiplicative* reduction or *additive* reduction, which corresponds to whether $E_p$ has a *node* or a *cusp* respectively.

Due to analyticity in $\mathbb{C}$, it makes sense to consider the Taylor expansion of $L(E,s)$ given by

$$L(E,s) = \sum_{i=0}^{\infty} c_i (s - s_0)^i, \qquad s_0 \in \mathbb{C}, \qquad c_i \in \mathbb{C},$$

as well its *order of vanishing* $ord_{s=s_0}$ or order of zero at $s_0$, a value $i$ such that $c_i \neq 0$ but $c_j = 0$ for any $j < i$. A different notion of rank can then be defined for $E$, as follows.

**Definition** (Analytic rank)**.** The **analytic rank** of $E$ is $rk_{an}(E(\mathbb{Q})) = ord_{s=1} L(E,s)$.

The conjecture then relates both notions of ranks as follows.

**Conjecture 3.8.1** (Birch and Swinnerton-Dyer)**.** $rk(E(\mathbb{Q})) = rk_{an}(E(\mathbb{Q}))$.

**Remark.** There is also a refined version of the conjecture that involves the *Tate-Shafarevich group*, which is omitted for further discussion. Proving this strong version will then indirectly lead to efficient algorithms for rank computation.

A direct consequence of the conjecture is that $E(\mathbb{Q})$ is infinite iff its ranks $rk(E(\mathbb{Q}))$ and $rk_{an}(E(\mathbb{Q}))$ are positive. This holds iff $L(E,s)$ does not have a constant term, or iff $L(E,1)$ computes to give a value of 0. In other words, the finiteness of $E(\mathbb{Q})$ holds iff $L(E,1) \neq 0$. Now the conjecture has been supported with much numerical evidence in [15], and can also be verified by prior examples with the *Sage* programming language as follows.

**Example.** Let $E : y^2 = x^3 - x$ be an elliptic curve over $\mathbb{Q}$. Then $rk(E(\mathbb{Q})) = 0$ and

$$L(E,s) \approx 0.655514388573030 + 0.447208159472739s - 0.233131198781643s^2 + 0.0342258563577268s^3 + \dots,$$

Hence $L(E,1) \approx 0.655514388573030 \neq 0$. Now let $E' : y^2 = x^3 - 5x$ be an elliptic curve over $\mathbb{Q}$. Then $rk(E'(\mathbb{Q})) = 1$ and

$$L(E',s) \approx 0.000000000000000 + 2.22876814774675s - 2.06654309593994s^2 + 0.549852427979257s^3 + \dots.$$

Thus $L(E',1) \approx 0.000000000000000 = 0$.

However, only special cases of the conjecture have been proven to date. The first general result, proven by Coates and Wiles, states that an elliptic curve $E$ with $L(E,1) \neq 0$ and *complex multiplication*, or when $|End(E)|$ is strictly larger than $\mathbb{Z}$, has finite $E(\mathbb{Q})$, and hence $rk(E(\mathbb{Q})) = 0$. A later result, proven by Gross and Zagier with *Heegner points*, states that a *modular* elliptic curve $E$ with $L(E,1) = 0$ and $(d/ds)L(E,1) \neq 0$, or equivalently $rk_{an}(E(\mathbb{Q})) = 1$, has a non-torsion rational point in $E(\mathbb{Q})$, and hence $rk(E(\mathbb{Q})) > 0$. Subsequently, Kolyvagin extended this proof by showing that $rk(E(\mathbb{Q})) = 1$ must hold for this latter case, and that $rk(E(\mathbb{Q})) = 0$ if $L(E,1) \neq 0$ instead. With the modularity theorem proven by Breuil et al, it is now known that any elliptic curve over $\mathbb{Q}$ is modular, hence proving the following special case of the Birch and Swinnerton-Dyer conjecture.

**Theorem 3.8.2** (Breuil, Coates, Conrad, Diamond, Gross, Kolyvagin, Taylor, Wiles, Zagier)**.** $rk(E(\mathbb{Q})) = rk_{an}(E(\mathbb{Q}))$ for $rk_{an}(E(\mathbb{Q})) \in \{0,1\}$.

*Proof.* Omitted, see [16], [17], [18], and [19]. □

The very recent result due to Bhargava and Shankar in [14] also showed that a large proportion of all elliptic curves must have either rank zero or one, but the conjecture still remain unproven for elliptic curves with higher ranks. Now as a Millenium Prize Problem, the Birch and Swinnerton-Dyer conjecture has significant implications in number theory, particularly on finiteness of the Tate-Shafarevich group, but it also proves other more elementary results, one of which concerns integers with the following property.

**Definition** (Congruent number)**.** $n \in \mathbb{Z}_{>0}$ is a **congruent number** iff it is the area of some right triangle with sides in $\mathbb{Q}_{>0}$.

Congruent numbers can be illustrated with the following example.

**Example.** $5 = \frac{1}{2}(3/2)(20/3)$ is a congruent number since it is the area of the right triangle with sides $3/2, 20/3, 41/6 \in \mathbb{Q}_{>0}$, while 10 is not a congruent number.

An open problem is the classification of all congruent numbers, known as the *congruent number problem*, which boils down to obtaining simultaneous solutions for $a^2 + b^2 = c^2$ and $2n = ab$, for some $n \in \mathbb{Z}_{>0}$ and some $a, b, c \in \mathbb{Q}_{>0}$. Considering the non-zero inverse transformations

$$(x,y) = \left(\frac{n(a+c)}{b}, \frac{2n^2(a+c)}{b^2}\right), \qquad (a,b,c) = \left(\frac{\left(x^2-n^2\right)}{y}, \frac{2nx}{y}, \frac{\left(x^2+n^2\right)}{y}\right),$$

the system of equations can be transformed with a bijective correspondence to the Weierstrass equation $y^2 = x^3 - n^2x$. Hence checking whether $n$ is a congruent number is in turn equivalent to determining whether an affine rational point with non-zero coordinates exists in the elliptic curve $E : y^2 = x^3 - n^2x$ over $\mathbb{Q}$. This prompts the following theorem that further classify the conditions for being a congruent number.

**Theorem 3.8.3** (Tunnell)**.** Let $n \in \mathbb{Z}_{>0}$ be a square-free congruent number. If $n$ is odd, then

$$2\left|\left\{(x,y,z) \in \mathbb{Z}^3 \mid n = 2x^2 + y^2 + 32z^2\right\}\right| = \left|\left\{(x,y,z) \in \mathbb{Z}^3 \mid n = 2x^2 + y^2 + 8z^2\right\}\right|.$$

Otherwise $n$ is even, then

$$2\left|\left\{(x,y,z) \in \mathbb{Z}^3 \mid n = 2\left(4x^2 + y^2 + 32z^2\right)\right\}\right| = \left|\left\{(x,y,z) \in \mathbb{Z}^3 \mid n = 2\left(4x^2 + y^2 + 8z^2\right)\right\}\right|.$$

*Proof.* Omitted, see [20]. □

The Birch and Swinnerton-Dyer conjecture, on the other hand, provides the converse to Tunnell's theorem, hence giving a single criterion for any congruent number that can be checked by enumerating the four sets involved. The following example illustrates the process, assuming the conjecture.

**Example.** Since 5 is an odd square-free congruent number, it holds that

$$2\left|\left\{(x,y,z) \in \mathbb{Z}^3 \mid 5 = 2x^2 + y^2 + 32z^2\right\}\right| = 0 = \left|\left\{(x,y,z) \in \mathbb{Z}^3 \mid 5 = 2x^2 + y^2 + 8z^2\right\}\right|.$$

Conversely, since 10 is an even square-free non-congruent number, it holds that

$$2\left|\left\{(x,y,z) \in \mathbb{Z}^3 \mid n = 2\left(4x^2 + y^2 + 32z^2\right)\right\}\right| = 8 \neq 4 = \left|\left\{(x,y,z) \in \mathbb{Z}^3 \mid n = 2\left(4x^2 + y^2 + 8z^2\right)\right\}\right|.$$

As such, the conjecture, if proven even only for elliptic curves given by the Weierstrass equation $y^2 = x^3 - n^2x$, would allow the congruence number problem to be fully resolved.

# 4 Applications

In this section, two elementary applications of elliptic curves are briefly touched on, together with a brief history of their development prior to elliptic curves.

## 4.1 Arithmetic

In arithmetic, the widely known fact that $\mathbb{Z}$ is a unique factorisation domain acts as the modern rephrasing of the fundamental theorem of arithmetic, which states that any integer can be uniquely written as a product of primes up to rearrangement and sign. An classical problem in arithmetic is determining these primes, or more commonly known as integer factorisation, for a given huge integer $N \in \mathbb{Z}_{>0}$ with tens of digits. Clearly no work is required if $N$ is prime, which can be verified for most cases by the following theorem.

**Theorem 4.1.1** (Fermat's little theorem)**.** Let $N$ be prime. Then $a^{N-1} \equiv 1 \mod N$ for any $a \in \mathbb{Z}_{>0}$ such that $N \nmid a$.

*Proof.* Since $N \nmid a$, it holds that $a \not\equiv 0 \mod N$, so $a \in \mathbb{Z}_N^*$. Lagrange's theorem gives $ord(a) \mid |\mathbb{Z}_N^*| = N-1$, so $a^{N-1} = 1$. Thus $a^{N-1} \equiv 1 \mod N$. □

Unfortunately, its converse does not hold, due to the existence of *Carmichael numbers*, which are composite integers that seemingly satisfy Fermat's little theorem, the first of which being relatively small at 561. These integers can be avoided manually due to their relative rarity, but there are indeed more reliable tests to check if $N$ is prime. Now simply assume that $N$ is composite, with an unknown large prime factor $p \in \mathbb{Z}_{>0}$. On first sight, there is a simple naive approach to factorise $N$ involving trial division, applying Euclidean division to every positive integer less than $N$. A clear improvement can be made by only considering $2, 3$ and integers of the form $6m \pm 1$, which is illustrated in the following example with a small value of $N$.

**Example.** Let $N = 420$ be composite. Trial division on $\{2, 3, 5, 7, \dots\}$ gives $420 = 2(210) + 0$ and $210 = 2(105) + 0$, but $105 = 2(52) + 1$. Now $105 = 3(35) + 0$, but $35 = 3(11) + 2$. Then $35 = 7(5) + 0$, but $7 = 1(5) + 2$. Finally $7 = 1(7) + 0$. Thus $L' = \{2, 2, 3, 5, 7\}$ and $N = (2)(2)(3)(5)(7)$.

It is immediately evident that this process of factorising $N$ into $p$ and $N/p$ is laborious, and especially difficult if $N/p$ is also prime and relatively similar in magnitude to $p$, since every integer below $p$ and $N/p$ will be checked for failure. In fact, while multiplying $p$ and $N/p$ to produce $N$ is relatively easy, there are no known efficient *non-quantum* polynomial time algorithms to deterministically do the reverse, of which is exactly the basis of modern cryptography. The fastest methods for integer factorisation involve either *sieves* or elliptic curves, the latter of which discussed here has motivations stemming from the classical *Pollard's* $p-1$ *method*. The following definition, considering a fixed integer $B \in \mathbb{Z}_{>0}$, will be used.

**Definition** ($B$-power smooth)**.** Let $n \in \mathbb{Z}_{>0}$ be such that $n = p_1^{e_1} \dots p_n^{e_n}$ for some $e_i \in \mathbb{Z}_{>0}$ and some primes $p_i \in \mathbb{Z}_{>0}$. Then $n$ is **$B$-power smooth** iff each $p_i^{e_i} \leq B$.

This definition is illustrated in the following example.

**Example.** 420 is 7-smooth, and $2(420)$ is not 7-smooth but is 8-smooth.

$B$ is typically chosen to be fairly large, such that the composite integer $p-1$ is likely to be $B$-power smooth. Now let $l_B = \operatorname{lcm}(2, \dots, B)$, so that any prime below $B$ divides $l_B$, and so $p-1 \mid l_B$. The algorithm again uses Fermat's little theorem to give $a^{l_B} \equiv 1 \mod p$ for any $a \in \mathbb{Z}_{>0}$ such that $p \nmid a$. Hence $p \mid a^{l_B} - 1$, so letting $g_B = \gcd\left(a^{l_B} - 1, N\right)$ gives $p \mid g_B \mid N$. Obtaining $g_B < N$ immediately implies that $g_B$ is a proper divisor of $N$, so the process can be repeated replacing $N$ with $g_B$. The algorithm is summarised as follows.

**Algorithm 4.1.2** (Pollard's $p-1$ method)**.** Input: an integer $N \in \mathbb{Z}_{>0}$. Output: a proper divisor of $N$.

1. Choose a *smoothness bound* $B \in \mathbb{Z}_{>0}$.
2. Calculate $l_B = \operatorname{lcm}(1, \dots, B)$.
3. Compute $g_B = \gcd\left(a^{l_B} - 1, N\right)$ for some $a \in \{2, \dots, N-1\}$.
4. If $g_B = 1$, then choose a larger smoothness bound $B$, else if $g_B = N$, then choose a different $a$.
5. Otherwise $1 < g_B < N$, then return $g_B$.

**Remark.** In practicality, this $B$ typically fixed, and a different algorithm is forcibly switched into if this algorithm fails, which would mean that Pollard's $p-1$ algorithm only serves to simplify the problem.

A simple observation picks out several possible concerns in the algorithm, most obviously being the question if the algorithm even terminates, which must be the case, as the smoothness bound $B$ will eventually be large enough for $l_B$ to exceed $p-1$. Another issue might be the speed of computing $l_B$ and $g_B$, with the latter seemingly depending on the former. This is resolved by the realisation that $l_B$ is arbitrarily defined as such to allow all factors below $B$ to divide $l_B$, so a purely multiplicative $l_B = B!$ can be used. While $g_B$ may require further exponentiation, this is not a concern as modular exponentiation with successive squaring to compute $a^{l_B}$ is fast, and the result of this can be used in the computation instead of $a^{l_B} - 1$. In the highly unlikely chance that $p \mid a$, a fix to this issue could be first doing trial division up to a small integer $n \in \mathbb{Z}_{>0}$ to rule out any possibility that $p < n$, and only considering the cases where $a < n$. With these concerns in mind, Pollard's $p-1$ algorithm can be illustrated with the following example involving a small $N$, which on modern computers can actually be done instantly even with trial division.

**Example.** Let $N = 246082373$. Then $2^{N-1} \equiv 114193013 \neq 1 \mod N$, so Fermat's little theorem gives that $N$ is composite. Now let $B = 7$ and $l_B = \operatorname{lcm}(1, \dots, B) = 420$, and let $a = 2$. Then $a^{l_B} \equiv 60592910 \mod N$, so $\gcd\left(a^{l_B} - 1, N\right) = \gcd(60592909, N) = 1$. Hence choose $B = 9 > 7$ and $l_B = \operatorname{lcm}(1, \dots, B) = 2520$, and let $a = 2$. Then $a^{l_B} \equiv 130940741 \mod N$, so $\gcd\left(a^{l_B} - 1, N\right) = \gcd(130940740, N) = 2521 < N$. Thus $2521 \mid N$ and $N = (2521)(97613)$, which are both prime.

A final serious concern would be overall efficiency of the algorithm that is only reasonable with the initial supposition that $p-1$ is $B$-power smooth, which may not always be the case, inevitably forcing large values of $B$. Despite so, it may still be desirable to check the $B$-power smoothness of $p+1$, or even $p \pm n$ for any small $n \in \mathbb{Z}$, to see if the initially fixed $B$ is sufficient to factorise $N$. In this respect, Pollard's $p-1$ algorithm has no way of allowing for other values of $p \pm n$ due to the restriction given by Fermat's little theorem. Now *Lenstra's elliptic curve factorisation method* takes this flaw into account by considering multiple random elliptic curves over finite fields. While the former considers the multiplicative group $\mathbb{Z}_p^*$ of order $\left|\mathbb{Z}_p^*\right| = p-1$ and checks if $a \in \mathbb{Z}_p^*$ satisfies $a^{l_B} = 1$, the latter considers the elliptic curve $E(\mathbb{F}_p)$ of order $|E(\mathbb{F}_p)| = p-t+1$ and checks if $P \in E(\mathbb{F}_p)$ satisfies $l_B P = \mathcal{O}$. Hasse's theorem gives $|t| \leq 2\sqrt{p}$, allowing $|E(\mathbb{F}_p)|$ to vary wildly within this interval and hence removing the aforementioned defect. The algorithm is stated as follows.

**Algorithm 4.1.3** (Lenstra's elliptic curve factorisation method)**.** Input: an integer $N \in \mathbb{Z}_{>0}$. Output: a proper divisor of $N$.

1. Set $P = (a, b)$ and $B = b^2 - a^3 - Aa$ for some $A, a, b \in \{1, \dots, N-1\}$.
2. If $g = \gcd\left(4A^3 + 27B^2, N\right) = N$, choose a different $A$, else if $1 < g < N$, return $g$, else let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{Q}$, treated as over the ring $\mathbb{Z}_N^*$.
3. Choose a smoothness bound $C$ and calculate $l_C$ as per Pollard's $p-1$ method.
4. Compute $l_C P = \left(q/d^2, r/d^3\right)$ and $g_C = \gcd(d, N)$.
5. If $g_C = 1$, choose a larger $C$ or a different $A$, else if $g_C = N$, choose a smaller $C$, else return $g_C$.

A couple of remarks will be made on Lenstra's elliptic curve factorisation method, which has the first two steps markedly differently from Pollard's $p-1$ method. The last three steps of the former mirror the latter, but it is worth noting that $l_C P = \mathcal{O}$ iff $d = 0$, which holds iff $p \mid d$, or $p \mid g_C = \gcd(d, N) \mid N$. While it is possible to directly obtain a random elliptic curve $E : y^2 = x^3 + Ax + B$ over $\mathbb{F}_p$ by choosing some random $A, B \in \mathbb{Z}$ and treating $A, B$ as elements of $\mathbb{F}_p$, obtaining a point in $E$ afterwards will involve the laborious process of finding a modular square root, and so the above approach is taken. Moreover, to avoid having $P$ be a torsion point and hence resulting in $N \mid d$, a simple fix would be an additional condition to choose $b^2 \nmid 4A^3 + 27\left(A^3 + Aa\right)$ in this reverse approach, which by the contrapositive to the Nagell-Lutz theorem forces $P$ to have infinite order. Again, computation of $l_C$ will be done by successive duplication of points, but a concern arises from possibly having denominators $d \in \mathbb{Z}_N$ being zero. Considering the cases when an inverse does not exist in $\mathbb{Z}_N^*$, or when $\gcd(d, N) > 1$, either $\gcd(d, N) = N$, for which it is sufficient to simply choose a different curve $E$, or $1 < \gcd(d, N) < N$, for which $\gcd(d, N)$ can be returned as a proper divisor of

$N$. In practice, the affine coordinates are computed modulo $N$, catching a division by zero error only when the extended Euclidean algorithm fails to give a modular inverse, then computing $g_C$ separately. With these remarks at hand, Lenstra's elliptic curve factorisation method can be illustrated with the following example involving a small $N$, which again can actually be done instantly with a modern computer.

**Example.** Let $N = 1715761513$. Then $2^{N-1} \equiv 114094409 \neq 1 \mod N$, so Fermat's little theorem gives that $N$ is composite. Let $A = 1$, $a = 2$, and $b = 1$, such that $P = (2, 1)$ and $B = 1^2 - 2^3 - 1\,(2) = -9$. Then $g = \gcd\left(4A^3 + 27B^2, N\right) = 1$, such that $E : y^2 = x^3 + x - 9$ is an elliptic curve over $\mathbb{Q}$. Now let $C = 17$ and $l_C = \operatorname{lcm}(1, \dots, C) = 12252240$. Then $l_C P = (1225303014, 142796033)$, so $(d, N) = 1$. Instead of choosing a larger $C$, choose a different $A \in \{2, \dots, N\}$ and recompute. Then $A = 42$ eventually returns $(d, N) = 26927$. Thus $26927 \mid N$ and $N = (26927)\,(63719)$, which are both prime.

As seen above, if choosing a different $A$ does not work, a larger $C$ could be tried, or even picking a different $P = (a, b)$ if all else fails, a sign of high algorithmic flexibility. While it may involve more sophistication and possibly a larger overhead in maintaining the elliptic curve data structure than Pollard's $p - 1$ method, Lenstra's elliptic curve factorisation method *heuristically* runs at sub-exponential time complexity, due to a high probability that an integer is $B$-power smooth within the interval in Hasse's theorem.

**Remark.** Using Pollard's $p - 1$ algorithm for this example will require $B \geq 13463$, which will take a while.

With the discussion on factorising the composite $N$ completed, the initial question of checking if $N$ is prime makes a comeback. After all, probabilistic factorisation algorithms may never terminate if $N$ was never composite in the first place. Again, there is a trivial method to do this, which involves factoring $N$ by trial division, Fermat's little theorem, or any other factorisation methods and hoping to result in a definite failure. While there were subsequent developments on fast non-deterministic tests, such as *Miller-Rabin*, that do not rely on factorisation but on Fermat's little theorem instead, the remaining discussion here focuses on one of the fastest *primality tests* that involves elliptic curves. In contrast to factorisation, currently doable for tens to hundreds of digits, the primality of integers up to tens of thousands of digits have been proven.

**Remark.** These forms of primality testing hold for arbitrary integers, but there are certain classes of huge integers that have been proven to be primes using specialised methods. For instance, the largest integer ever proven to be a prime is a *Mersenne prime* that has tens of millions of digits.

The said primality test is also an elliptic curve version of another classical primality test, known as the *Pocklington-Lehmer primality test*, which has its basis on the following theorem.

**Theorem 4.1.4** (Pocklington-Lehmer)**.** Let $r \in \mathbb{Z}_{>0}$ be such that $r \mid N - 1$ and $r \geq \sqrt{N}$. Then $N$ is prime if

$$a_q^{N-1} \equiv 1 \mod N, \qquad \gcd\left(a_q^{(N-1)/q} - 1, N\right) = 1, \qquad a_q \in \mathbb{Z}_{>0},$$

for any prime $q \in \mathbb{Z}_{>0}$ such that $q \mid r$.

*Proof.* Let $p \in \mathbb{Z}_{>0}$ be a prime such that $p \mid N$, so $p$ is a prime of good reduction, and let $v = v_q(r)$ be the $q$-adic valuation of $r$. Now let $a \equiv a_q^{(N-1)/q^v} \mod p$ for some $a \in \mathbb{Z}_p^*$. Then $a^{q^v} = a_q^{N-1} \equiv 1 \mod p$ and $a^{q^{v-1}} = a_q^{(N-1)/q} \not\equiv 1 \mod p$. Hence $ord(a) = q^v$. Lagrange's theorem gives $q^v \mid \left|\mathbb{Z}_p^*\right| = p - 1$, so $r \mid p - 1$ and $p > r \geq \sqrt{N}$. Thus $p = N$ and $N$ is prime. □

Again, a simple observation points that integer factorisation is involved in finding $r$, as well as its prime factors $q$. Similar to Pollard's $p - 1$ method, a prior assumption is required for the algorithm to run at a reasonable time, namely that $p - 1$ has many small factors $q$ that allow $r$ to be generated quickly with trial division. It is also worth noting that finding $a_q$ is equivalent to finding a generator of the group $\mathbb{Z}_p^*$, which might be laborious, but often letting $a_q = 2$ works. The test algorithm then simply follows from the theorem, but it is desirable to have a third party mechanism that checks validity of the primality proof, which will also help ensure functional correctness of implementations. In particular, the notion of a *primality certificate*, which is an ordered pair $(r, c)$ as in Theorem 4.1.4, where $c$ is a list of ordered pairs $(q, a_q)$, allows for a verification by simple modular exponentiation. The Pocklington-Lehmer primality test can be illustrated with a much larger value of $N$ in the following example, owing to the fact that $N - 1$ has many small factors.

**Example.** Let $N = 9223372036854775783$. Then $N - 1 = 9223372036854775782$. Trial division for primes less than 400000 gives $r = (2)(3)^4(17)(23)(319279) \mid N - 1$, such that $r = 20223770418 \geq \sqrt{N}$. Then

$$2^{N-1} \equiv 3^{N-1} \equiv 1 \mod N, \qquad \gcd\left(2^{(N-1)/3} - 1, N\right) = \gcd\left(3^{(N-1)/2} - 1, N\right) = 1,$$

$$\gcd\left(2^{(N-1)/17} - 1, N\right) = \gcd\left(2^{(N-1)/23} - 1, N\right) = \gcd\left(2^{(N-1)/319279} - 1, N\right) = 1.$$

Thus $N$ is prime with primality certificate $(r, [(2,3), (3,2), (17,2), (23,2), (319279,2)])$.

As for Lenstra's elliptic curve factorisation method, an elliptic curve analogue attempts to fix the $p-1$ assumption by virtue of Hasse's theorem. By first choosing $A, a, b \in \mathbb{Z}_N^*$, a valid elliptic curve over the ring $\mathbb{Z}_N^*$ is considered, giving the following analogous theorem.

**Theorem 4.1.5** (Goldwasser-Kilian)**.** Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{Q}$ such that $\gcd\left(4A^3 + 27B^2, N\right) = 1$, treated as over the ring $\mathbb{Z}_N^*$, and let $m \in \mathbb{Z}_{>0}$ be such that $m > \left(\sqrt[4]{N} + 1\right)^2$. Then $N$ is prime if

$$mP_q = \mathcal{O}, \qquad \frac{m}{q} P_q \neq \mathcal{O}, \qquad P_q \in E(\mathbb{Q}) \setminus \{\mathcal{O}\},$$

for any distinct prime $q \in \mathbb{Z}_{>0}$ such that $q \mid m$.

*Proof.* Let $p \in \mathbb{Z}_{>0}$ be a prime such that $p \mid N$, and let $v = v_q(m)$ be the $q$-adic valuation of $m$. Now let $r_p : E(\mathbb{Q}) \to E_p(\mathbb{F}_p)$ be the reduction modulo $p$ map, and let $P_q' = (m/q^v) r_p(P_q)$. Then $q^v P_q' = m r_p(P_q) = \mathcal{O}$ and $q^{v-1} P_q' = (m/q) r_p(P_q) \neq \mathcal{O}$. Hence $ord\left(P_q'\right) = q^v$. Lagrange's theorem gives $q^v \mid |E_p(\mathbb{F}_p)|$, so $m \mid |E_p(\mathbb{F}_p)|$. Now Hasse's theorem gives

$$\left(\sqrt[4]{N} + 1\right)^2 < m \leq |E_p(\mathbb{F}_p)| \leq p + 2\sqrt{p} + 1 = \left(\sqrt{p} + 1\right)^2.$$

Hence $p > \sqrt{N}$. Thus $p = N$ and $N$ is prime. □

As for the Pocklington-Lehmer primality test, an appropriate primality certificate, possibly with the form of an ordered triple $(m, A, c)$ as in Theorem 4.1.4, where $c$ is a list of ordered pairs $(q, P_q)$, will act as the output of a successful test. With all previous considerations, the Goldwasser-Kilian primality test can be illustrated with an even larger value of $N$ in the following example.

**Example.** Let $N = 9223372036854775907$. Instead let $A = -2$, $a = 2$, and $b = 0$, such that $P = (2, 0)$ and $B = 0^2 - 2^3 - -2(-2) = -4$. Then $\gcd\left(4A^3 + 27B^2, N\right) = 1$, such that $E : y^2 = x^3 - 2x - 4$ is an elliptic curve over $\mathbb{Q}$. Now let $m = (2)(11)(13)(37)(269)(1327) = 3777382466$ such that $\left(\sqrt[4]{N} + 1\right)^2 < 3037110719 < m$. Then $ord(P) = 2$, so $mP = \mathcal{O}$, and

$$\frac{m}{2} P \neq \mathcal{O}, \qquad \frac{m}{11} P \neq \mathcal{O}, \qquad \frac{m}{13} P \neq \mathcal{O}, \qquad \frac{m}{37} P \neq \mathcal{O}, \qquad \frac{m}{269} P \neq \mathcal{O}, \qquad \frac{m}{1327} P \neq \mathcal{O}.$$

Thus $N$ is prime with primality certificate $(m, -2, [(2, P), (11, P), (13, P), (37, P), (269, P), (1327, P)])$.

The heart of the algorithm lies on finding a suitable elliptic curve $E(\mathbb{Q})$, which in the above example is seemingly conjured from thin air. As for Lenstra's elliptic curve factorisation method, many random values of $A$, $a$, and $b$ are generated, until their corresponding elliptic curve is found to have an order with enough small distinct prime factors to multiply and exceed $\left(\sqrt[4]{N} + 1\right)^2$. This order $E_p(F_p)$ is in turn efficiently computed through the Schoof-Elkies-Atkin algorithm.

**Remark.** Using the Pocklington-Lehmer primality test for this example will require $r \geq 273901883852669$, which is a prime and will take forever, even with a supercomputer.

Most algorithms in this subsection are given in full under code listings in the appendix. Unfortunately, due to the difficulty in implementing Schoof's algorithm, the Goldwasser-Kilian primality test is omitted. Historically, Schoof's algorithm was seen as too cumbersome to implement, such that the theory of complex multiplication was utilised instead to construct an elliptic curve $E$ with an easily computable order $E_p(F_p)$. This became known as the *Atkin-Morain primality test*, which remained the fastest primality proving algorithm to date, despite the later advent of the much faster Schoof-Elkies-Atkin algorithm.

## 4.2 Cryptography

*Cryptography* is the study of computational techniques to allow for secure communication of information across public platforms in the presence of third party eavesdroppers. It is historically based on the computational intractability of certain mathematical problems, such as integer factorisation. As the difficult computations involved in elliptic curve point multiplication became more apparent, they saw great use in modern cryptography, of which a very brief introduction will be provided in this short subsection. With the standard notation of three parties, namely *Alice*, the sender, *Bob*, the receiver, and *Eve*, the eavesdropper, the standard process of secure communication is as follows.

**Algorithm 4.2.1** (Communication across a public domain)**.** Alice sends a message to Bob.

1. Alice intends to send a *plaintext* message $P$ to Bob, without Eve eavesdropping.
2. Alice *encrypts* $P$ with an *encryption key* $E$, which is owned only by Alice.
3. The *ciphertext* message $C = E(P)$ is sent across a public domain, from Alice to Bob.
4. Bob *decrypts* $C$ with a *decryption key* $D$, which is owned only by Bob.
5. Bob recovers $P = D(C)$ from Alice.

In this setup, it is clear that Bob should never leak $D$ to Eve so as to keep $P$ secret, and that $D$ must be the left inverse of $E$. In the case of *symmetric encryption*, the right inverse property also holds, allowing for the roles of $E$ and $D$ to swap. However, Alice and Bob would then need to secretly agree on $E$ and $D$ in advance, which may be infeasible if there are no means for prior contact. *Asymmetric encryption* solves this problem by introducing two pairs of inverse keys for Alice and Bob, such that they would publish their respective encryption keys $E_A$ and $E_B$, while hiding their respective decryption keys $D_A$ and $D_B$. Whenever Alice intends to send $P$ to Bob, Alice would send $C = E_B(P)$ across the public domain, so that only Bob could recover $P = D_B(C)$, or vice versa. The modern *Rivest-Shamir-Adleman cryptosystem*, or more commonly known as the *RSA*, is a asymmetric encryption system that has its basis on the difficulty of integer factorisation, and is given in the following algorithm.

**Algorithm 4.2.2** (Rivest-Shamir-Adleman cryptosystem)**.** Outputs a pair of keys.

1. Choose two distinct huge prime numbers $p, q \in \mathbb{Z}_{>0}$ of similar magnitude and compute $n = pq$.
2. Compute $\lambda(n) = \operatorname{lcm}(p-1, q-1)$ and choose a small $e \in \mathbb{Z}_{>0}$ such that $\gcd(e, \lambda(n)) = 1$.
3. Compute the multiplicative inverse $d$ of $e$ modulo $\lambda(n)$.
4. Return the public encryption key $(n, e)$ and function $E(P) \equiv P^e \mod n$.
5. Return the private decryption key $(n, d)$ and function $D(C) \equiv C^d \mod n$.

The functional correctness of the algorithm trivially follows from Fermat's little theorem, and as such will not be discussed. Now $e$ is typically chosen to be small enough for quick encryption computations, but not too small so as to be insecure. Moreover $P$ is also assumed to have been translated into an integer beforehand with some form of *padded* cipher mechanism. The following example implements the RSA.

**Example.** Let $p = 2147483647$ and $q = 2147483659$ be primes. Then $n = pq = 4611686039902224373$ and $\lambda(n) = \operatorname{lcm}(p-1, q-1) = 768614339267876178$. Now choose a public encryption key $n$ and $e = 65537$ such that $\gcd(e, \lambda(n)) = 1$. Thus the private decryption key is $n$ and $d = 73205833433176421 \equiv e^{-1} \mod l$.

Now the availability of increasingly powerful techniques imposes a minimum bit size of $p$ and $q$ in order to make the RSA even remotely practical. Furthermore, the presence of specialised algorithms, such as Pollard's $p-1$ method, forces a requirement on $p-1$ and $q-1$ to have large factors to prevent unprecedented *attacks* as well. To date, a few hundred bits of $n$ is easily factorisable by a desktop computer within hours, if not seconds, with a suitably powerful algorithm. As such, the RSA generally chooses an $n$ with thousands of bits, which is somewhat cumbersome for massive amounts of data, and would require larger chip sizes and power consumption in the process of encryption. On the other hand, this drawback is less evident in symmetric encryption systems, which are generally faster if $E$ and $D$ were somehow agreed by Alice and Bob in advance. This could be feasibly done without any prior contact with the following *key exchange protocol*.

**Algorithm 4.2.3** (Diffie-Hellman key exchange)**.** Outputs a private symmetric key.

1. Alice and Bob agree on a huge prime $p \in \mathbb{Z}_{>0}$ and a small $g \in \mathbb{Z}_{>0}$ such that $g < p$.
2. Alice chooses $a \in \mathbb{Z}_{>0}$ such that $a < p$ and sends $g_a \equiv g^a \mod p$ to Bob across the public domain.
3. Bob chooses $b \in \mathbb{Z}_{>0}$ such that $b < p$ and sends $g_b \equiv g^b \mod p$ to Alice across the public domain.
4. Alice computes $s \equiv g_b^a \equiv g^{ab} \mod p$ privately.
5. Bob computes $s \equiv g_a^b \equiv g^{ab} \mod p$ privately.

The algorithm simply uses basic properties of modular exponentiation and produces a private symmetric key $s$ between Alice and Bob, which as aforementioned allows secure communication in a public domain. In this process, only $p$, $g$, $g_a$, and $g_b$ is immediately available to Eve, while $a$, $b$, and $s$ are kept secret between Alice and Bob. The following example implements the Diffie-Hellman key exchange.

**Example.** Let $p = 2147483647$ be prime and $g = 65537$. Alice chooses $a = 16777259$ and sends the public key $g_a = 751856369 \equiv g^a \mod p$ to Bob, while Bob chooses $b = 16777289$ and sends the public key $g_b = 1654172966 \equiv g^b \mod p$ to Alice. Thus the private symmetric key is $s = 1288974049 \equiv g^{ab} \mod p$.

Reverse engineering these values as a third party attacker is known as the *discrete logarithm problem*, which is, analogous to integer factorisation, computationally infeasible provided $p$ is chosen to be huge. While there is an impossibly slow, naive approach by simply trying $g^n$ for each $n \in \mathbb{Z}_{>0}$ until $g^n = g^a$ or $g^n = g^b$ is obtained, there are no known algorithms efficient enough to crack the system.

**Remark.** Unfortunately, the non-existence of efficient polynomial time algorithms for integer factorisation and the discrete logarithm problem is unproven. In fact, a *quantum computer* running *Shor's algorithm* would theoretically do both of these in polynomial time.

Rephrasing the Diffie-Hellman key exchange in terms of finite cyclic groups, modulo operations involving $p$ is equivalent to operating under the finite multiplicative cyclic group $\mathbb{Z}_p^*$, while $g$ is simply any generator of $\mathbb{Z}_p^*$. A elliptic curve variant of Diffie-Hellman can then be stated easily as follows.

**Algorithm 4.2.4** (Elliptic curve Diffie-Hellman)**.** Outputs a private symmetric key.

1. Alice and Bob agree on an elliptic curve $E$ over $\mathbb{F}_p$ for some prime $p \in \mathbb{Z}_{>0}$ and a point $P \in E(\mathbb{F}_p)$.
2. Alice chooses $a \in \mathbb{Z}_p^*$ and sends $P_a = aP$ to Bob across the public domain.
3. Bob chooses $b \in \mathbb{Z}_p^*$ and sends $P_b = bP$ to Alice across the public domain.
4. Alice computes $S = a(P_b) = a(bP) = abP$ privately.
5. Bob computes $S = b(P_a) = b(aP) = abP$ privately.

The prior example can then be illustrated with elliptic curve Diffie-Hellman as follows.

**Example.** Let $E : y^2 = x^3 + 65537x + 1$ be an elliptic curve over $\mathbb{F}_p$ where $p = 2147483647$ and $P = (0, 1) \in E(\mathbb{F}_p)$. Alice chooses $a = 16777259$ and sends the public key $P_a = aP = (675295473, 1821381850)$ to Bob, while Bob chooses $b = 16777289$ and sends the public key $P_b = bP = (294235749, 438747352)$ to Alice. Thus the private symmetric key is $S = abP = (1210475635, 471187571)$.

The discrete logarithm problem on certain elliptic curves over finite fields is also significantly harder than that of generic finite fields, and as such a list of recommended elliptic curves for use in key exchanges was published publicly by the National Institute of Standards and Technology. These elliptic curves are used in several other cryptosystems, such as the underlying group of the *ElGamal encryption system*, or in other cryptographic contexts, such as *digital signatures*, but will not be discussed further. Most of these elliptic curve based systems require fewer bits than those based on traditional finite fields. An estimate places a key size of less than $2^9$ bits having an equivalent security to a key size of $2^{12}$ bits for the RSA.

**Remark.** Unfortunately, the discrete logarithm problem for elliptic curves is still susceptible to attacks from a quantum computer. The *supersingular isogeny key exchange* is an analogue of Diffie-Hellman that considers isogenies, and would in theory resist quantum attacks, but has a higher performance overhead.

# A Preliminaries

## A.1 Rings and fields

Let $R$ be a commutative unital ring and $F \subseteq K \subseteq L$ be fields.

**Definition** (Automorphism)**.** An **automorphism** of $R$ is an isomorphism from $R$ to itself, which are elements of the **automorphism group** $Aut(R)$ with respect to composition.

**Example.** $id_R$ is an automorphism of $R$.

**Definition** (Prime ideal)**.** An ideal $I \subset R$ is **prime** iff $ab \in I$ implies $a \in I$ or $b \in I$ for any two elements $a, b \in I$.

**Example.** An irreducible element $r \in R$ in a unique factorisation domain $R$ generates a prime ideal $\langle r \rangle$.

**Definition** (Chain)**.** A **chain** of subsets in $R$ of length $n \in \mathbb{Z}_{\geq 0}$ is a sequence of distinct subsets $S_0 \subset \cdots \subset S_n \subset R$.

**Example.** $\langle 0 \rangle \subset \langle x_1 \rangle \subset \cdots \subset \langle x_1, \dots, x_n \rangle \subset F[x_1, \dots, x_n]$ is a chain of prime ideals of length $n$.

**Definition** (Characteristic)**.** The **characteristic** $char(F)$ of $F$ is the smallest $n \in \mathbb{Z}_{>0}$, if it exists, such that $n \cdot 1 = 1 + \cdots + 1 = 0$. Otherwise $char(F)$ is 0.

**Example.** $char(\mathbb{C}) = char(\mathbb{R}) = char(\mathbb{Q}) = 0$ while $char(\mathbb{F}_{p^e}) = p$ for prime $p \in \mathbb{Z}_{>0}$ and $e \in \mathbb{Z}_{\geq 0}$.

**Definition** (Field extension)**.** $K$ is a **field extension** of $F$, denoted by $K/F$, iff $F$ is a subfield of $K$.

**Example.** $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}$, and $\mathbb{F}_{p^e}/\mathbb{F}_{p^{e'}}$ for prime $p \in \mathbb{Z}_{>0}$ and $e \mid e'$ are field extensions.

**Definition** ($F$-homomorphism)**.** An **$F$-homomorphism** from $K/F$ to another field extension $K'/F$ is a field homomorphism $\phi : K \to K'$ such that $\phi|_F = id|_F$. The definitions of **$F$-isomorphism** and **$F$-automorphism** extend naturally, with $Aut_F(K)$ denoting the **$F$-automorphism group** of $K$.

**Example.** Complex conjugation is an $\mathbb{R}$-automorphism of $\mathbb{C}$.

**Definition** (Finite extension)**.** $K/F$ is **finite** iff the dimension $dim_F K$ of $K$ as a vector space over $F$ is finite.

**Example.** $\mathbb{C}/\mathbb{R}$ is a finite extension with $[\mathbb{C} : \mathbb{R}] = 2$ since $\{1, i\}$ is a basis of $\mathbb{C}$ over $\mathbb{R}$.

**Definition** (Finitely generated)**.** $F(s_1, \dots, s_n)$ is **finitely generated** by $s_1, \dots, s_n \in K$ over $F$ iff $F(S)$ is the smallest subfield of $K$ containing $s_1, \dots, s_n$ and the elements of $F$.

**Example.** $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is finitely generated by $\{\sqrt{2}, \sqrt{3}\}$ over $\mathbb{Q}$, by $\{\sqrt{2}\}$ over $\mathbb{Q}(\sqrt{3})$, and by $\{\sqrt{3}\}$ over $\mathbb{Q}(\sqrt{2})$.

**Definition** (Number field)**.** $K$ is a **number field** iff $K/F$ is finite and $F = \mathbb{Q}$.

**Example.** $\mathbb{Q}\left(\sqrt{d}\right)$ for square-free $d \in \mathbb{Z}$ are number fields with $\left[\mathbb{Q}\left(\sqrt{d}\right) : \mathbb{Q}\right] = 2$.

**Definition** (Algebraic element)**.** $\alpha \in K$ is **algebraic** over $F$ iff it is a root of some non-zero polynomial in $F[x]$. Otherwise $\alpha$ is **transcendental** over $F$.

**Example.** $\pi$ is transcendental over $\mathbb{Q}$ but algebraic over $\mathbb{R}$ since it is the root of $x - \pi$.

**Definition** (Minimal polynomial)**.** The **minimal polynomial** $m_\alpha$ of $\alpha$ over $F$ is the unique monic irreducible polynomial in $F[x]$ with $\alpha$ as a root.

**Example.** The minimal polynomial of $\sqrt{2}$ is $x^2 - 2$ over $\mathbb{Q}$ and is $x - \sqrt{2}$ over $\mathbb{R}$.

**Definition** (Algebraic extension)**.** $K/F$ is **algebraic** iff any element in $K$ is algebraic over $F$. Otherwise $K/F$ is **transcendental**.

**Example.** $\mathbb{C}/\mathbb{Q}$ is not an algebraic extension since $\pi$ is transcendental over $\mathbb{Q}$.

**Definition** (Algebraically closed)**.** $F$ is **algebraically closed** iff any non-constant polynomial in $F[x]$ has a root in $F$.

**Example.** $\mathbb{R}$ is not algebraically closed since $x^2+1 \in \mathbb{R}[x]$ has no roots in $\mathbb{R}$.

**Definition** (Algebraic closure)**.** An **algebraic closure** of $F$ is an algebraically closed algebraic extension of $F$ that is unique up to $F$-isomorphism.

**Example.** $\overline{\mathbb{R}} = \mathbb{C}$ while $\overline{\mathbb{Q}}$ is the field of algebraic numbers.

The existence and uniqueness of algebraic closures can be proven from *Zorn's Lemma*, which is equivalent to the *Axiom of Choice*.

**Proposition A.1.1.** An algebraic closure $\overline{F}$ of $F$ exists and is unique up to $F$-isomorphism.

**Definition** (Splits)**.** A polynomial $f(x) \in F[x]$ of degree $n > 0$ **splits** over $K$ iff $f(x) = c\prod_{i=0}^{n}(x - a_k)$ for some $c \in F$ and $a_k \in K$.

**Example.** $x^2 - 2$ splits over $\mathbb{Q}\left(\sqrt{2}\right)$ but not over $\mathbb{Q}$ since $x^2 - 2 = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right)$ in $\mathbb{Q}\left(\sqrt{2}\right)$.

**Definition** (Normal extension)**.** $K/F$ is **normal** iff $K/F$ is algebraic and any irreducible polynomial in $F[x]$ with a root in $K$ splits over $F$.

**Example.** $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ is a normal extension, while $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$ is not a normal extension since $f(x) = x^3 - 2 = \left(x - \sqrt[3]{2}\right)\left(x^2 + \sqrt[3]{2}x + \sqrt[3]{4}\right)$ has a root $x = \sqrt[3]{2}$ but does not split over $\mathbb{Q}\left(\sqrt[3]{2}\right)$.

**Definition** (Separable polynomial)**.** An polynomial $f \in F[x]$ is **separable** iff $df/dx \neq 0$.

**Example.** $x^2 - 2 \in \mathbb{Q}[x]$ is a separable polynomial since $d\left(x^2 - 2\right)/dx = 2x \neq 0$, while $x^2 - y^2 \in \mathbb{F}_2\left(y^2\right)$ is an inseparable polynomial since $d\left(x^2 - y^2\right)/d\left(y^2\right) = 0$.

**Definition** (Separable extension)**.** $K/F$ is **separable** iff $K/F$ is algebraic and the minimal polynomial of any $\alpha \in K$ is separable.

**Example.** $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ is a separable extension, while $\mathbb{F}_2(y)/\mathbb{F}_2\left(y^2\right)$ is an inseparable extension since the minimal polynomial of $y$ over $F_2\left(y^2\right)$ is $x^2 - y^2$, which is inseparable.

**Definition** (Galois extension)**.** $K/F$ is **Galois** iff $K/F$ is normal and separable.

**Example.** $\mathbb{C}/\mathbb{R}$ and $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ are Galois extensions.

**Definition** (Galois group)**.** $Aut_F(K)$ is the **Galois group** $Gal_F(K)$ of $K$ over $F$ iff $K/F$ is Galois.

**Example.** $Gal_{\mathbb{R}}(\mathbb{C}) = \{id_{\mathbb{R}}, \phi\}$ where $\phi$ is complex conjugation, while $Gal_{\mathbb{Q}}\left(\mathbb{Q}\sqrt{2}\right) = \{id_{\mathbb{Q}}, \phi\}$ where $\phi$ is the $\mathbb{Q}$-automorphism that swaps $\sqrt{2}$ and $-\sqrt{2}$.

**Definition** (Perfect field)**.** $F$ is **perfect** iff the algebraic closure of $F$ is Galois.

**Example.** Examples of perfect fields include any field of characteristic zero including $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, any finite field $\mathbb{F}_{p^e}$, and any algebraically closed field including $\overline{\mathbb{Q}}$. Examples of imperfect fields include the field of rational functions $\mathbb{F}_p(y)$ of any finite field $\mathbb{F}_p$ since $x^p - y \in \mathbb{F}_p(y)$ is irreducible but inseparable.

## A.2 Algebraic varieties

Let $F$ be a perfect field of $char\,(F) \notin \{2,3\}$ with algebraic closure $K = \overline{F}$ and Galois group $Gal_F\,(K)$.

**Definition** (Affine space)**.** An **affine $n$-space** over $F$ is $\mathbb{A}^n = K^n$.

**Definition** (Projective space)**.** A **projective $n$-space** over $F$ is $\mathbb{P}^n = \left(\mathbb{A}^{n+1} \setminus \{(0,\dots,0)\}\right) / \sim$, the set of equivalence classes of **homogeneous coordinates** $[p_0,\dots,p_n]$, where $(x_0,\dots,x_n) \sim (y_0,\dots,y_n)$ iff each $x_i = \lambda y_i$ for some $\lambda \in F^*$.

$\mathbb{P}^n$ can be considered a superset of $n+1$ copies of $\mathbb{A}^n$ by the natural inclusions $\phi_i : \mathbb{A}^n \to \mathbb{P}^n$ for each $i \in \{0,\dots,n\}$ defined by

$$\phi_i\,(x_1,\dots,x_n) = [x_1,\dots,x_i,1,x_{i+1},\dots,x_n]\,,$$

so write $\mathbb{A}^n \subseteq \mathbb{P}^n$. Now let $\mathbb{A}^n$ be an affine $n$-space over $F$ and $\mathbb{P}^n$ be a projective $n$-space over $F$.

**Definition** (Rational point)**.** The set of **$F$-rational points** of $\mathbb{A}^n$ is $\mathbb{A}^n\,(F) = F^n$, and of $\mathbb{P}^n$ is

$$\mathbb{P}^n\,(F) = \{[p_0,\dots,p_n] \in \mathbb{P}^n \mid \forall p_j \neq 0,\ \forall p_i,\ p_i/p_j \in F\}\,.$$

$\mathbb{A}^n$ can be equipped with $Gal_F\,(K)$, such that $\mathbb{A}^n\,(F) = \{a \in \mathbb{A}^n \mid \forall \sigma \in Gal_F\,(K)\,,\ \sigma\,(a) = a\}$. This holds similarly in $\mathbb{P}^n$.

**Example.** $\mathbb{C}^n$ is an affine $n$-space over $\mathbb{R}$, with $\mathbb{C}^n\,(\mathbb{R}) = \mathbb{R}$. $\overline{\mathbb{F}}^n$ is a projective $n$-space over $\mathbb{F}^n$, with $\overline{\mathbb{F}}^n\,(\mathbb{F}^n)$ being the projective plane of order $n$.

**Definition** (Homogeneous)**.** A polynomial $f \in K\,[x_0,\dots,x_n]$ is **homogeneous** of degree $d \in \mathbb{Z}_{\geq 0}$ iff for any $\lambda \in K$, it holds that $f\,(\lambda x_0,\dots,\lambda x_n) = \lambda^d f\,(x_0,\dots,x_n)$. An ideal $I \subseteq K\,[x_0,\dots,x_n]$ is homogeneous iff $I$ is generated by homogeneous polynomials in $K\,[x_0,\dots,x_n]$.

A homogeneous polynomial $f^* \in K\,[x_0,\dots,x_n]$ can be *dehomogenised* into $f \in K\,[x_1,\dots,x_n]$ by

$$f\,(x_1,\dots,x_n) = f^*\,(1,x_1,\dots,x_n)\,,$$

while a non-homogeneous polynomial $g \in K\,[x_1,\dots,x_n]$ can be *homogenised* into $g^* \in K\,[x_0,\dots,x_n]$ by

$$f^*\,(x_0,\dots,x_n) = x_0^d f\,(x_1/x_0,\dots,x_n/x_0)\,.$$

**Example.** $z^3 + wxy + 7w^3 \in \mathbb{C}\,[w,x,y,z]$ is homogeneous, which can be dehomogenised to $z^3 + xy + 7 \in \mathbb{C}\,[x,y,z]$. Conversely $x^3 + 3x^2y + z^7 \in \mathbb{C}\,[x,y,z]$ is non-homogeneous, which can be homogenised to $w^4x^3 + 3w^4x^2y + z^7 \in \mathbb{C}\,[w,x,y,z]$. Thus $\left\langle z^3 + wxy + 7w^3, w^4x^3 + 3w^4x^2y + z^7 \right\rangle \subseteq \mathbb{C}\,[w,x,y,z]$ is a homogeneous ideal.

The following definitions are simplified by considering only prime ideals in *Hilbert's Nullstellensatz*.

**Definition** (Algebraic variety)**.** An **affine algebraic variety** of $\mathbb{A}^n$ over $F$ is

$$A = \{a \in \mathbb{A}^n \mid \forall f \in I,\ f\,(a) = 0\}$$

for some finitely generated prime ideal $I \subseteq F\,[x_1,\dots,x_n]$, denoted by $A\,(I)$ and $I\,(A)$ respectively. The set of $F$-rational points of $A$ is $A\,(F) = A \cap \mathbb{A}^n\,(F)$. A **projective algebraic variety** $P$ of $\mathbb{P}^n$ over $F$ and the set of $F$-rational points of $P$ are defined similarly but with homogeneous prime ideals.

Since $I\,(A)$ can be finitely generated by $f_1,\dots,f_m \in F\,[x_1,\dots,x_n]$, it holds that $A\,(f_1,\dots,f_m)\,(F)$ is the set of solutions in $F$ to the system of equations $f_1\,(x_1,\dots,x_n) = \cdots = f_m\,(x_1,\dots,x_n) = 0$. This holds similarly in $\mathbb{P}^n$.

**Example.** Let $\left\langle x^2 + y^2 - 1 \right\rangle \subseteq \mathbb{R}\,[x,y]$ be a finitely generated prime ideal. Thus $A\left(x^2 + y^2 - 1\right)$ is an affine algebraic variety of $\mathbb{C}^2$ over $\mathbb{R}$ and $A\left(x^2 + y^2 - 1\right)(\mathbb{R})$ is the unit circle $S^1$. Homogenisation gives a finitely generated homogeneous ideal $\left\langle x^2 + y^2 - w^2 \right\rangle \subseteq \mathbb{R}\,[w,x,y]$. Similarly $P\left(x^2 + y^2 - w^2\right)$ is a projective algebraic variety of $\mathbb{C}^2$ over $\mathbb{R}$ and $P\left(x^2 + y^2 - w^2\right)(\mathbb{R})$ is the unit circle $S^1$.

Let $A$ be an affine algebraic variety of $\mathbb{A}^n$ over $F$ and $P$ be a projective algebraic variety of $\mathbb{P}^n$ over $F$.

**Definition** (Dimension)**.** The **dimension** $dim\,(A)$ of $A$ is the length of any longest chain of prime ideals in $F\left[x_1,\dots,x_n\right]/I\,(A)$. The dimension of $P$ is $dim\,(P)=dim\,(A\,(I\,(P)))-1$ for any $A\,(I\,(P))\subseteq\mathbb{A}^n$.

**Example.** Let $A\,(x-y)$ be an affine algebraic variety of $\mathbb{C}^3$ over $\mathbb{R}$. Then a longest chain of prime ideals is $\langle 0\rangle\subset\langle y\rangle\subset\langle y,z\rangle\subset\mathbb{R}\left[x,y,z\right]/\langle x-y\rangle$, which has length two. Thus it has dimension $dim\,(A\,(x-y))=2$. A projective algebraic variety $P\,(x-y)$ of $\mathbb{C}^2$ over $\mathbb{R}$ has dimension $dim\,(P\,(x-y))=dim\,(A\,(x-y))-1=1$.

The dimension of projective algebraic varieties can also be defined from *Krull's Hauptidealsatz*.

**Proposition A.2.1.** $dim\,(P)=n-1$ iff $I\,(P)$ is generated by a homogeneous irreducible polynomial in $F\left[X_0,\dots,X_n\right]$.

**Definition** (Smooth)**.** A point $a\in A$ is **singular** iff the Jacobian $m\times n$ matrix $J$ defined by $J_{ij}=\partial f_i/\partial x_j$ is such that $rk\left(J|_a\right)<n-dim\,(A)$. $A$ is **smooth** if it has no singular points. This holds similarly for $P$.

**Example.** Let $A\,(x-y)$ be an affine algebraic variety of $\mathbb{C}^3$ over $\mathbb{R}$. Then $dim\,(A\,(x-y))=2$, so a point $a=(x,y,z)\in A\,(x-y)$ is singular iff $rk\left(J|_a\right)<3-2=1$, or

$$0=rk\left(J|_a\right)=rk\begin{pmatrix}\left.\dfrac{\partial\,(x-y)}{\partial x}\right|_a & \left.\dfrac{\partial\,(x-y)}{\partial y}\right|_a & \left.\dfrac{\partial\,(x-y)}{\partial z}\right|_a\end{pmatrix}=rk\begin{pmatrix}1 & -1 & 0\end{pmatrix}=1.$$

Thus there are no singular points and $A\,(x-y)$ is smooth.

**Definition** (Function field)**.** The **function field** of $P$ is

$$F\,(P)=\left\{f\,(x_0,\dots,x_n)\,/g\,(x_0,\dots,x_n)\mid f,g\in F\left[x_0,\dots,x_n\right],\ \deg\,(f)=\deg\,(g)\,,\ g\notin I\,(P)\right\}/\sim,$$

the field of equivalence classes of **rational functions** of homogeneous polynomials, where $f/g\sim f'/g'$ iff $fg'-f'g\in I\,(P)$.

**Example.** Let $P\,(xy)$ be a projective algebraic variety of $\mathbb{C}$ over $\mathbb{R}$. Then $x\in\mathbb{R}\left[x,y\right]$ and $y\in\mathbb{R}\left[x,y\right]$ are homogeneous of degree one, and $y\notin I\,(P)$. Thus $x/y\in\mathbb{R}\,(P)$.

Let $P'$ be a projective algebraic variety of $\mathbb{P}^m$ over $F$.

**Definition** (Morphism)**.** A **morphism** from $P$ to $P'$ is an equivalence class of rational functions $\phi=\left[\phi_0,\dots,\phi_m\right]:P\to P'$ for some $\phi_i\in F\,(P)$, such that for any $p\in P$, there is a rational function $g\in F\,(P)$ such that $g\phi_i\,(p)\in P'$ for each $\phi_i$ and $g\phi_i\,(p)\neq 0$ for some $\phi_i$, where $(\phi_0,\dots,\phi_m)\sim(\psi_0,\dots,\psi_m)$ iff each $\phi_i=g'\psi_i$ for some $g'\in F\,(P)$.

**Example.** Let $P\left(x^2+y^2-w^2\right)$ be a projective algebraic variety of $\mathbb{C}^2$ over $\mathbb{R}$ and $P'\,(0)$ be a projective algebraic variety of $\mathbb{C}$ over $\mathbb{R}$, and let $\phi=\left[w+x,y\right]:P\to P'$ be such that $w+x,y\in\mathbb{R}\,(P)$. Let $p=\left[w,x,y\right]\in P$ be a point such that $w+x\neq 0$ or $y\neq 0$. Then $w+x,y\neq 0$ are well-defined at $p$. Now let $p'=\left[w,x,y\right]\in P$ be a point such that $w+x=y=0$. Then $((w-x)\,/y)\,(w+x)=\left(w^2-x^2\right)/y=y^2/y=y$ and $((w-x)\,/y)\,y=w-x\neq 0$ are well-defined at $p'$. Thus $\phi$ is a morphism.

A standard result in algebraic geometry states that images of morphisms are projective algebraic varieties.

**Proposition A.2.2.** Let $\phi:P\to P'$ be a morphism and $dim\,(P)=dim\,(P')=1$. Then $\phi$ is either constant or surjective.

**Definition** (Isomorphism)**.** An **isomorphism** is a morphism $\phi:P\to P'$ such that there is another morphism $\phi':P'\to P$ where $\phi'\circ\phi=id_P$ and $\phi\circ\phi'=id_{P'}$. $P$ and $P'$ are **isomorphic**, denoted by $P\cong P'$, iff there is an isomorphism $\phi:P\to P'$.

**Example.** Let $P\left(x^2+y^2-w^2\right)$ be a projective algebraic variety of $\mathbb{C}^2$ over $\mathbb{R}$ and $P'\,(0)$ be a projective algebraic variety of $\mathbb{C}$ over $\mathbb{R}$ with a morphism $\phi:\left[w+x,y\right]:P\to P'$. Then $\phi'=\left[x^2+y^2,x^2-y^2,2xy\right]:P'\to P$ is also a morphism such that $\phi\circ\phi'=\left[2x^2,2xy\right]=\left[x,y\right]=id_{P'}$ and

$$\phi'\circ\phi=\left[(w+x)^2+y^2,(w+x)^2-y^2,2\,(w+x)\,y\right]=\left[2w\,(w+x)\,,2x\,(w+x)\,,2y\,(w+x)\right]=\left[w,x,y\right]=id_P.$$

Thus $\phi$ is an isomorphism and $P\cong P'$.

## A.3 Algebraic curves

Let $F$ be a perfect field of $char\,(F) \notin \{2,3\}$ with algebraic closure $K = \overline{F}$ and $V$ be a projective algebraic variety of $\mathbb{P}^n$ over $F$.

**Definition** (Projective plane curve)**.** $V$ is a **projective plane curve** iff $dim\,(V) = 1$ and $n = 2$.

Since a projective plane curve $V$ is such that $\dim(V) = 1 = 2 - 1$, it holds that $I(V)$ is generated by some homogeneous irreducible polynomial $f \subseteq F[X,Y,Z]$. For ease of notation $V$ will be written in the form $V : f(X,Y,Z) = 0$, or in its simpler dehomogeneous form $V : f(x,y) = 0$. Now let $C : f(X,Y,Z) = 0$ and $C' : g(X,Y,Z) = 0$ be two projective plane curves over $F$ with a point $P = [a,b,c] \in C \cap C'$.

**Definition** (Multiplicity)**.** The **multiplicity** $m_P(f)$ of $C$ at $P$ is the smallest $m \in \mathbb{Z}_{>0}$ such that

$$\forall i,j,k \in \mathbb{Z}_{\geq 0}, \qquad i+j+k = n, \qquad \left.\frac{\partial^n f}{\partial X^i \partial Y^j \partial Z^k}\right|_P = 0$$

for any $n \in \{0,\dots,m-1\}$ but not $n = m$.

$P$ is singular iff $rk\,(J|_P) < 1$, or $\partial f/\partial X|_P = \partial f/\partial Y|_P = \partial f/\partial Z|_P = 0$, which holds iff $m_P(f) > 1$.

**Example.** Assume $char\,(F) = 0$, and let $f(X,Y,Z) = f(x,y) = \left(x^2+y^2\right)^2 + 3x^2y - y^3$ with $P = [0,0,1] = (0,0)$. Then

$$\left.\frac{\partial f}{\partial x}\right|_P = \left.\frac{\partial f}{\partial y}\right|_P = \left.\frac{\partial^2 f}{\partial x^2}\right|_P = \left.\frac{\partial^2 f}{\partial y^2}\right|_P = \left.\frac{\partial^2 f}{\partial x \partial y}\right|_P = 0, \qquad \left.\frac{\partial^3 f}{\partial y^3}\right|_P = -6 \neq 0.$$

Thus the multiplicity of $C$ at $P$ is $m_P(f) = 3$ and $P$ is singular.

**Definition** (Tangent)**.** The **tangents** $T_P(f)$ of $C$ at $P = [a,b,c]$ with multiplicity $m = m_P(f)$ are the irreducible factors of the polynomial

$$t_P(f)(X,Y,Z) = \sum_{i+j+k=m} \binom{m}{i,j,k} \left.\frac{\partial^m f}{\partial X^i \partial Y^j \partial Z^k}\right|_P (X-a)^i (Y-b)^j (Z-c)^k.$$

**Example.** Let $f(X,Y,Z) = f(x,y) = \left(x^2+y^2\right)^2 + 3x^2y - y^3$ with $P = [0,0,1] = (0,0)$ and $m = m_P(f) = 3$. Then

$$\begin{aligned} t_P(f)(X,Y,Z) = t_P(f)(x,y) &= \binom{3}{0} \left.\frac{\partial^3 f}{\partial x^3}\right|_P x^3 + \binom{3}{1} \left.\frac{\partial^3 f}{\partial x^2 \partial y}\right|_P x^2 y + \binom{3}{2} \left.\frac{\partial^3 f}{\partial x \partial y^2}\right|_P x y^2 + \binom{3}{3} \left.\frac{\partial^3 f}{\partial y^3}\right|_P y^3 \\ &= 18x^2y - 6y^3 = 6y\left(\sqrt{3}x - y\right)\left(\sqrt{3}x + y\right). \end{aligned}$$

Thus the tangents of $C$ at $P$ are $T_P(f) = \left\{y, \sqrt{3}x - y, \sqrt{3}x + y\right\}$.

**Definition** (Ordinary singularity)**.** A singular point $P \in C$ is **ordinary** iff $t_P(f)$ has distinct factors.

**Example.** Let $f(X,Y,Z) = f(x,y) = \left(x^2+y^2\right)^2 + 3x^2y - y^3$ with $P = [0,0,1] = (0,0)$. Then $t_P(f)$ have distinct factors $y$, $\sqrt{3}x - y$, and $\sqrt{3}x + y$. Thus $P$ is ordinary.

**Definition** (Intersection number)**.** The **intersection number** of $C$ and $C'$ at $P$ if $\deg(\gcd(f,g)) = 0$ is $I_P(f,g)$, where $I_P : F[X,Y,Z] \times F[X,Y,Z] \to \mathbb{Z}_{>0}$ is defined for any $f', g' \in F[X,Y,Z]$ by:

- $I_P(f',g') = I_P(g',f')$,
- $I_P(f',g') = I_P(f',g' \circ h)$ for any affine transformation $h$,
- $I_P(f',g') = I_P(f',g' + hf')$ for any $h \in F[X,Y,Z]$,
- $I_P(f',hh') = I_P(f',h) + I_P(f',h')$ for any $h,h' \in F[X,Y,Z]$, and
- $I_P(f',g') \geq m_P(f')\,m_P(g')$, with equality iff $T_P(f') \cap T_P(g') = \emptyset$.

Since $T_P(X) = \{X\}$, $T_P(Y) = \{Y\}$, and $T_P(Z) = \{Z\}$ are all distinct, it holds that $I_P(X,Y) = I_P(X,Z) = I_P(Y,Z) = 1$.

**Example.** Let $f(X,Y,Z) = f(x,y) = \left(x^2+y^2\right)^2 + 3x^2y - y^3$ and $g(X,Y,Z) = g(x,y) = \left(x^2+y^2\right)^3 - 4x^2y^2$ with $P = [0,0,1] = (0,0)$. Then $\gcd(f,g) = 1$, so $\deg(\gcd(f,g)) = 0$. Now let $h(x,y) = 4x^2y + 4y^3 + 5x^2 - 3y^2$, such that

$$g + \left(3y - x^2 - y^2\right) f = y^2 h \qquad \text{and} \qquad f + \left(y^2 - 2x^2y - y^3 - 3x^2\right) y = x^4.$$

Then

$$I_P(f,g) = I_P\left(f, g + \left(3y - x^2 - y^2\right) f\right) = I_P\left(f, y^2 h\right) = I_P\left(f, y^2\right) + I_P(f,h).$$

The first term can be computed as

$$I_P\left(f,y^2\right) = 2I_P(f,y) = 2I_P\left(f + \left(y^2 - 2x^2y - y^3 - 3x^2\right) y, y\right) = 2I_P\left(x^4, y\right) = 8I_P(x,y) = 8.$$

Now $m_P(f) = 3$ and $T_P(f) = \left\{y, \sqrt{3}x - y, \sqrt{3}x + y\right\}$. Since $C'' : h(x) = 0$ is also a projective plane curve, its multiplicity at $P$ can be computed to be $m_P(h) = 2$ and its tangents at $P$ can also be computed to be $T_P(h) = \left\{\sqrt{5}x - \sqrt{3}y, \sqrt{5}x + \sqrt{3}y\right\}$. Hence $I_P(f,h) = m_P(f)\, m_P(h) = (3)(2) = 6$. Thus the intersection number of $C$ and $C'$ at $P$ is $I_P(f,g) = 8 + 6 = 14$.

**Definition** (Flex)**.** $P$ is a **flex** iff $I_P(f,g) > 2$ is odd.

**Example.** Let $f(X,Y,Z) = f(x,y) = y - x^3$ with $P = [0,0,1] = (0,0)$. Then $\partial f/\partial y|_P = 1 \neq 0$, so $m_P(f) = 1$. Since

$$g(X,Y,Z) = g(x,y) = t_P(f)(x,y) = \partial f/\partial x|_P\, x + \partial f/\partial y|_P\, y = y,$$

it holds that $\gcd(f,g) = 1$, so $\deg(\gcd(f,g)) = 0$. Hence

$$I_P(f,g) = I_P(f - y, y) = I_P\left(-x^3, y\right) = 3I_P(-x,y) = 3 > 2.$$

Thus $P$ is a flex.

The following follows from the fundamental theorem of algebra on the *resultant* of $f$ and $g$.

**Theorem A.3.1** (Bézout)**.** $C$ intersects $C'$ at $(\deg(f))(\deg(g))$ points *up to multiplicity*, so

$$\sum_{P \in C \cap C'} I_P(f,g) = (\deg(f))(\deg(g)).$$

The following follows from a *dimension counting* argument.

**Theorem A.3.2** (Cayley-Bacharach)**.** Let $\deg(f) = \deg(g) = 3$ such that $C$ intersects $C'$ at nine points up to multiplicity, and let $C'' : h(X,Y,Z) = 0$ be a cubic projective plane curve over $F$ such that at least eight of these points are in $C''$. Then the ninth point is also in $C''$.

The following definition is the *genus-degree formula*, which is a corollary of the *adjunction formula* and the *Riemann-Roch theorem* for arbitrary curves and surfaces.

**Definition** (Degree)**.** The **degree** of $C$ is $d_C = \deg(f)$.

**Definition** (Genus)**.** The **genus** of $C$ is

$$g_C = \tfrac{1}{2}(d_C - 1)(d_C - 2) - \tfrac{1}{2}\sum_{P \in C} m(m-1),$$

over all ordinary singularities $P \in C$ with multiplicity $m_P(f) = m$.

The genus of $C$ is $g_C = \frac{1}{2}(d_C - 1)(d_C - 2)$ if $C$ is smooth.

**Example.** The line $L : y = x$ is a smooth projective plane curve of degree one and genus zero. The unit circle $S_1 : x^2 + y^2 = 1$ is a smooth projective plane curve of degree two and genus zero. An elliptic curve $E : y^2 = x^3 + Ax + B$ is a smooth projective plane curve of degree three and genus zero.

## A.4 Groups

Let $G$ be an additive abelian group, with multiplication $\cdot : \mathbb{Z} \times G \to G$ defined by

$$nx = \begin{cases} x + \cdots + x & n > 0 \\ 0 & n = 0 \\ (-x) + \cdots + (-x) & n < 0 \end{cases}.$$

**Theorem A.4.1** (Isomorphism theorems)**.** The following theorems hold:

1. Let $H$ be a group and $\phi : G \to H$ be a group homomorphism. Then:
$$Ker(\phi) \trianglelefteq G, \qquad \frac{G}{Ker(\phi)} \cong Im(\phi).$$
2. Let $N \trianglelefteq G$ and $H \leq G$ be subgroups. Then:
$$N \cap H \trianglelefteq H, \qquad \frac{H}{N \cap H} \cong \frac{N + H}{N}.$$
3. Let $N \trianglelefteq G$ and $H \trianglelefteq G$ be subgroups such that $N \leq H$. Then:
$$\frac{H}{N} \trianglelefteq \frac{G}{N}, \qquad \frac{G/N}{H/N} \cong \frac{G}{H}.$$

All subgroups of $G$ are normal, but the above theorems still hold if $G$ is non-abelian.

**Definition** (Torsion element)**.** An **$n$-torsion element** is an element $x \in G$ such that $n = ord(x)$ is finite.

**Example.** $\mathbb{Z} + p/q \in \mathbb{Q}/\mathbb{Z}$ is a torsion element since $ord(x) \mid q$ is finite.

**Definition** (Torsion subgroup)**.** The **$n$-torsion subgroup** $G[n]$ is the group of $m$-torsion elements of $G$ such that $m \mid n$. The **torsion subgroup** $G_{tors}$ of $G$ is the group of $m$-torsion elements of $G$ for any $m \in \mathbb{Z}_{\geq 0}$.

**Example.** $G = \mathbb{R}/\mathbb{Z}$ has torsion subgroup $G_{tors} = \mathbb{Q}/\mathbb{Z}$ since any $n$-torsion element $\mathbb{Z} + x \in G$ is such that $nx \in \mathbb{Z}$ and $x \in \mathbb{Q}$.

**Definition** (Finitely generated)**.** $G$ is **finitely generated** iff there are finitely many elements $x_1, \ldots, x_n \in G$ such that any element $x \in G$ is a sum

$$x = \sum_{i=1}^{n} m_i x_i, \qquad m_i \in \mathbb{Z}.$$

**Example.** $\mathbb{Z}$ and $\mathbb{Z}_n$ are finitely generated abelian groups.

The *direct sum* $\oplus$ of finitely many abelian groups is equivalent to their direct product $\times$, thus $\mathbb{Z}^n = \mathbb{Z} \times \cdots \times \mathbb{Z} = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$. Now let $G$ be finitely generated.

**Theorem A.4.2** (Fundamental theorem of finitely generated abelian groups)**.** There are unique $r, m \in \mathbb{Z}_{\geq 0}$ and $n_1, \ldots, n_m \in \mathbb{Z}_{>1}$ such that

$$G \cong r\mathbb{Z} \oplus \bigoplus_{i=1}^{m} \mathbb{Z}_{n_i},$$

with each $n_i \mid n_{i+1}$.

**Definition** (Rank)**.** The **rank** $rk(G)$ of $G$ is the unique $r \in \mathbb{Z}_{\geq 0}$ in Theorem A.4.2.

**Example.** A finite abelian group $G$ has rank $rk(G) = 0$ since $G_{tors} = G$.

# B Algorithm proofs

## B.1 Transformation of a cubic curve into Weierstrass form

Let

$$E : f(X,Y,Z) = a_1X^3+a_2X^2Y+a_3XY^2+a_4Y^3+a_5X^2Z+a_6XYZ+a_7Y^2Z+a_8XZ^2+a_9YZ^2+a_{10}Z^3 = 0$$

for some $a_i \in F$ be an elliptic curve over a perfect field $F$, and let $P = [a,b,c] \in E$ be an $F$-rational point. Then the unique tangent at $P$ is

$$\begin{aligned} L : \begin{pmatrix} 1 \\ 1,0,0 \end{pmatrix} \left.\frac{\partial f}{\partial X}\right|_P (X-a) + \begin{pmatrix} 1 \\ 0,1,0 \end{pmatrix} \left.\frac{\partial f}{\partial Y}\right|_P (Y-b) + \begin{pmatrix} 1 \\ 0,0,1 \end{pmatrix} \left.\frac{\partial f}{\partial Z}\right|_P (Z-c) = 0 \\ : \left(3a_1a^2 + 2a_2ab + a_3b^2 + 2a_5ac + a_6bc + a_8c^2\right)(X-a) \\ + \left(a_2a^2 + 2a_3ab + 3a_4b^2 + a_6ac + 2a_7bc + a_9c^2\right)(Y-b) \\ + \left(a_5a^2 + a_6ab + a_7b^2 + 2a_8ac + 2a_9bc + 3a_{10}c^2\right)(Z-c) = 0. \end{aligned}$$

If $P$ is not a flex, Bézout's theorem gives that $L$ intersects $E$ at three points up to multiplicity, so $E \cap L = \{P, P'\}$ for some other $F$-rational point $P' \in E$, and repeat inductively with $P'$. This *chord-tangent* method eventually terminates until $P'$ is a flex, so assume without loss of generality that $P$ is a flex. Now let $Q \in L \setminus E$ be a point distinct to $P$ and define a matrix

$$M = \begin{pmatrix} Q & P & R \end{pmatrix}, \qquad R \in \{[1,0,0],[0,1,0],[0,0,1]\}.$$

Since $P$ and $Q$ are linearly independent, at least one of these is invertible. Then transforming $[X,Y,Z] \mapsto M[X,Y,Z]^T$ gives $Q \mapsto [1,0,0]$ and $P \mapsto [0,1,0] = \mathcal{O}$, and the elliptic curve

$$E' : f'(X,Y,Z) = a_1'X^3+a_2'X^2Y+a_3'XY^2+a_4'Y^3+a_5'X^2Z+a_6'XYZ+a_7'Y^2Z+a_8'XZ^2+a_9'YZ^2+a_{10}'Z^3 = 0.$$

for some $a_i' \in F$. Since $\mathcal{O} \in E'$, it holds that $f'(0,1,0) = a_4' = 0$. Now the tangent at $\mathcal{O}$ is

$$L' : \begin{pmatrix} 1 \\ 1,0,0 \end{pmatrix} \left.\frac{\partial f'}{\partial X}\right|_{\mathcal{O}} X + \begin{pmatrix} 1 \\ 0,1,0 \end{pmatrix} \left.\frac{\partial f'}{\partial Y}\right|_{\mathcal{O}} (Y-1) + \begin{pmatrix} 1 \\ 0,0,1 \end{pmatrix} \left.\frac{\partial f'}{\partial Z}\right|_{\mathcal{O}} Z = 0 : a_3'X + a_7'Z = 0.$$

Since $L' : Z = 0$, it holds that $a_3' = 0$ and $a_7' \neq 0$. Then $L'$ intersects $E'$ at

$$a_1'X^3 + a_2'X^2Y + a_5'X^2(0) + a_6'XY(0) + a_7'Y^2(0) + a_8'X(0)^2 + a_9'Y(0)^2 + a_{10}'(0)^3 = X^2(a_1'X + a_2'Y) = 0.$$

Since $\mathcal{O}$ is a flex, it holds that $X = 0$ is repeated three times, so $a_1' \neq 0$ and $a_2' = 0$. Hence

$$\begin{aligned} E' &: a_1'X^3 + a_5'X^2Z + a_6'XYZ + a_7'Y^2Z + a_8'XZ^2 + a_9'YZ^2 + a_{10}'Z^3 = 0 \\ &: X^3 + \frac{a_5'}{a_1'}X^2Z + \frac{a_6'}{a_1'}XYZ + \frac{a_7'}{a_1'}Y^2Z + \frac{a_8'}{a_1'}XZ^2 + \frac{a_9'}{a_1'}YZ^2 + \frac{a_{10}'}{a_1'}Z^3 = 0. \end{aligned}$$

Then rescaling $[X,Y,Z] \mapsto [X,Y,-(a_1'/a_7')Z]$ gives

$$\begin{aligned} E' &: X^3 - \frac{a_5'}{a_7'}X^2Z - \frac{a_6'}{a_7'}XYZ - Y^2Z + \frac{a_8'a_1'}{a_7'^2}XZ^2 + \frac{a_9'a_1'}{a_7'^2}YZ^2 - \frac{a_{10}'a_1'^2}{a_7'^3}Z^3 = 0 \\ &: Y^2Z + \frac{a_5'}{a_7'}X^2Z + \frac{a_6'}{a_7'}XYZ = X^3 + \frac{a_8'a_1'}{a_7'^2}XZ^2 + \frac{a_9'a_1'}{a_7'^2}YZ^2 - \frac{a_{10}'a_1'^2}{a_7'^3}Z^3 = 0. \end{aligned}$$

Thus $E'$ is a Weierstrass equation.

## B.2 Group law explicit formulae

Let $P, Q \in E$ be points such that $R = P * Q \in E$. Since $*$ is symmetric, it is commutative, so only the following six cases need to be considered.

$(*)_1$ Assume that $P = (a, b)$ and $Q = (a, b')$ for $b \neq b'$. Then the line joining $P$ and $Q$ is

$$L : (b - b')\,X + (ab' - ab)\,Z = 0 : X = aZ,$$

which intersects $E$ at

$$Y^2Z = (aZ)^3 + A\,(aZ)\,Z^2 + BZ^3 \qquad \Longrightarrow \qquad Z\left(a^3Z^2 + AaZ^2 + BZ^2 - Y^2\right) = 0.$$

If $Z \neq 0$, then this can be dehomogenised into

$$y^2 = a^3 + Aa + B,$$

which has trivial solutions opposite in sign, so $b' = -b$. Thus $Z = 0$ and $R = \mathcal{O}$.

$(*)_2$ Assume that $P = (a, b)$ and $Q = (a', b')$ for $a \neq a'$, and let

$$\lambda = \frac{b - b'}{a - a'}, \qquad \mu = \frac{ab' - a'b}{a - a'}.$$

Then the line joining $P$ and $Q$ is

$$L : (b - b')\,X + (a' - a)\,Y + (ab' - a'b)\,Z = 0 : Y = \lambda X + \mu Z,$$

which intersects $E$ at

$$(\lambda X + \mu Z)^2\,Z = X^3 + AXZ^2 + BZ^3 \qquad \Longrightarrow \qquad X^3 - \lambda^2X^2Z + (A - 2\lambda\mu)\,XZ^2 - \left(\mu^2 - B\right)Z^3 = 0.$$

Since $Z = 0$ gives $Y = 0$, it holds that $Z \neq 0$, and this can be dehomogenised into

$$x^3 - \lambda^2x^2 + (A - 2\lambda\mu)\,x - \left(\mu^2 - B\right) = 0.$$

Let $R = (a'', b'')$. Since

$$0 = (x - a)\,(x - a')\,(x - a'') = x^3 - (a + a' + a'')\,x^2 + (aa' + a'' + a'a'')\,x - aa'a'',$$

comparing coefficients gives

$$\lambda^2 = a + a' + a'', \qquad A - 2\lambda\mu = aa' + aa'' + a'a'', \qquad \mu^2 - B = aa'a''.$$

Thus $R = \left(\lambda^2 - a - a', \lambda\left(\lambda^2 - a - a'\right) + \mu\right)$.

$(*)_3$ Assume that $P = Q = (a, b)$ for $b \neq 0$, and let

$$\lambda = \frac{3a^2 + A}{2b}, \qquad \mu = \frac{2Aa + 3B - b^2}{2b}.$$

Then the tangent at $P$ is

$$L : \left(-3a^2 - A\right)X + 2bY + \left(b^2 - 2Aa - 3B\right)Z = 0 : Y = \lambda X + \mu Z,$$

which intersects $E$ by $(*)_2$ at

$$x^3 - \lambda^2x^2 + (A - 2\lambda\mu)\,x - \left(\mu^2 - B\right) = 0.$$

Let $R = (a', b')$. Since

$$0 = (x - a)^2\,(x - a') = x^3 - (2a + a')\,x^2 + \left(2aa' + a^2\right)x - a^2a',$$

comparing coefficients gives

$$\lambda^2 = 2a + a', \qquad A - 2\lambda\mu = 2aa' + a^2, \qquad \mu^2 - B = a^2a'.$$

Thus $R = \left(\lambda^2 - 2a, \lambda\left(\lambda^2 - 2a\right) + \mu\right)$.

$(*)_4$ Assume that $P = Q = (a, 0)$. Then since $a\left(3a^2 + A\right) = 3\left(a^3\right) + Aa = 3\left(-Aa - B\right) + Aa = -2Aa - 3B$, the tangent at $P$ is

$$L : \left(-3a^2 - A\right) X + \left(-2Aa - 3B\right) Z = 0 : X = aZ,$$

which intersects $E$ at $(a, 0)$, $(a, -0) = (a, 0)$, and $\mathcal{O}$ by $(*)_1$. Thus $R = \mathcal{O}$.

$(*)_5$ Assume that $P = (a, b)$ and $Q = \mathcal{O}$. Then the line joining $P$ and $Q$ is

$$L : -X + aZ = 0 : X = aZ,$$

which intersects $E$ at $(a, b)$, $(a, -b)$, and $\mathcal{O}$ by $(*)_1$. Thus $R = (a, -b)$.

$(*)_6$ Assume that $P = Q = \mathcal{O}$. Then the tangent at $P$ is

$$L : Z = 0.$$

Thus $R = \mathcal{O}$.

Similarly since $+$ is symmetric, it is commutative, so only the following four cases need to be considered. If $P = (a, b)$ and $Q = (a', b')$ for $a \neq a'$, then $(*)_2$ and $(*)_5$ give

$$\begin{aligned} P + Q &= \left(\lambda^2 - a - a', -\left(\lambda\left(\lambda^2 - a - a'\right) + \mu\right)\right), \qquad \lambda = \frac{b - b'}{a - a'}, \qquad \mu = \frac{ab' - a'b}{a - a'} \\ &= \left(\frac{\left(A + aa'\right)\left(a + a'\right) + 2\left(B - bb'\right)}{\left(a - a'\right)^2}, \frac{a'b - ab' - \left(\frac{\left(A + aa'\right)\left(a + a'\right) + 2\left(B - bb'\right)}{\left(a - a'\right)^2}\right)\left(b - b'\right)}{a - a'}\right) \\ &= \left(\frac{\left(A + aa'\right)\left(a + a'\right) + 2\left(B - bb'\right)}{\left(a - a'\right)^2}, \frac{\left(Ab' - a'^2b\right)\left(3a + a'\right) + \left(a^2b' - Ab\right)\left(a + 3a'\right) - 4B\left(b - b'\right)}{\left(a - a'\right)^3}\right). \end{aligned}$$

If $P = Q = (a, b)$ for $b \neq 0$, then $(*)_3$ and $(*)_5$ give

$$\begin{aligned} P + Q &= \left(\lambda^2 - 2a, -\left(\lambda\left(\lambda^2 - 2a\right) + \mu\right)\right), \qquad \lambda = \frac{3a^2 + A}{2b}, \qquad \mu = \frac{2Aa + 3B - b^2}{2b} \\ &= \left(\frac{a^4 - 2Aa^2 - 8Ba + A^2}{4b^2}, \frac{b^2 - 2Aa - 3B - \left(\frac{a^4 - 2Aa^2 - 8Ba + A^2}{4b^2}\right)\left(3a^2 + A\right)}{2b}\right) \\ &= \left(\frac{a^4 - 2Aa^2 - 8Ba + A^2}{4b^2}, \frac{a^6 + 5Aa^4 + 20Ba^3 - 5A^2a^2 - 4ABa - A^3 - 8B^2}{8b^3}\right). \end{aligned}$$

If $P = (a, b)$ and $Q = \mathcal{O}$, then $(*)_5$ gives

$$P + Q = ((a, b) * \mathcal{O}) * \mathcal{O} = (a, -b) * \mathcal{O} = (a, b) = P.$$

Otherwise $P + Q = \mathcal{O}$ or $P = Q = \mathcal{O}$, then $(*)_1$, $(*)_4$, and $(*)_6$ give

$$P + Q = (P * Q) * \mathcal{O} = \mathcal{O} * \mathcal{O} = \mathcal{O}.$$

Thus the explicit formulae hold.

# C Code listings

## C.1 Fields.hs

This module includes basic types and instances for fields and prime subfields in Section 2.

```
{-# LANGUAGE GeneralizedNewtypeDeriving #-}
{-# LANGUAGE ScopedTypeVariables #-}

module Fields (C, Field (..), Fp, Prime (..), Q, R, Val (..), modInv) where

import Data.Complex (Complex (..))
import Data.Ratio (denominator, numerator)

---------------------------------------------------------------------------

-- Fields

-- Value information
data Val = None | NumDen Integer Integer | ReIm Double Double

-- Field type class
class (Eq f, Fractional f, Show f) => Field f where
  {-# MINIMAL char, val #-}
  char :: f -> Integer
  val :: f -> Val

---------------------------------------------------------------------------

-- Characteristic zero

-- Rational numbers Q
newtype Q = Q Rational deriving (Eq, Fractional, Num, Ord)
instance Show Q where
  show q = show n ++ if d == 1 then "" else "/" ++ show d
    where
      NumDen n d = val q
instance Field Q where
  char = const 0
  val (Q q) = NumDen (numerator q) (denominator q)

-- Real numbers R
newtype R = R Double deriving (Eq, Fractional, Num, Ord)
instance Show R where
  show (R r) = if r == fromIntegral r' then show r' else show r
    where
      r' = floor r
instance Field R where
  char = const 0
  val = const None

-- Complex numbers C
newtype C = C (Complex Double) deriving (Eq, Fractional, Num)
instance Show C where
  show (C (r :+ i))
    | signum i == -1 = "(" ++ show (R r) ++ "-" ++ show (R (abs i)) ++ "i)"
    | signum i == 1 = "(" ++ show (R r) ++ "+" ++ show (R i) ++ "i)"
```

```
    | otherwise = show (R r)
instance Field C where
  char = const 0
  val (C (r :+ i)) = ReIm r i
```

---

```
-- Characteristic prime

-- Prime numbers
class (Enum p, Show p) => Prime p where
  prime :: p -> Integer
  prime _ = read . tail . show $ (toEnum 0 :: p)

-- Prime subfields Fp
newtype Fp p = Fp Integer

-- Fp field instance
instance Prime p => Field (Fp p) where
  char = const $ prime (undefined :: p)
  val = const None

-- Fp standard instances
instance Prime p => Bounded (Fp p) where
  minBound = 0
  maxBound = -1
instance Prime p => Enum (Fp p) where
  toEnum = fromIntegral
  fromEnum (Fp n) = fromInteger n
instance Eq (Fp p) where
  Fp n == Fp n' = fromInteger n == fromInteger n'
instance Prime p => Fractional (Fp p) where
  fromRational n = fromInteger (numerator n) / fromInteger (denominator n)
  recip (Fp n) = case modInv n $ prime (undefined :: p) of
    Right m -> fromIntegral m
    Left m -> error $ show m
instance Prime p => Integral (Fp p) where
  quotRem (Fp n) (Fp n') = (fromInteger q, fromInteger r)
    where
      (q, r) = quotRem n n'
  toInteger (Fp n) = fromInteger n
instance Prime p => Num (Fp p) where
  Fp n + Fp n' = fromInteger $ n + n'
  Fp n * Fp n' = fromInteger $ n * n'
  abs n = n
  signum n = if n == 0 then 0 else 1
  fromInteger n = Fp . mod n $ prime (undefined :: p)
  negate (Fp n) = fromInteger $ (-n)
instance Ord (Fp p) where
  Fp n <= Fp n' = n <= n'
instance Prime p => Real (Fp p) where
  toRational (Fp n) = fromInteger n
instance Show (Fp p) where
  show (Fp n) = show n
```

```
-- Extended Euclidean algorithm
extGCD :: Integral a => a -> a -> ((a, a), a)
extGCD 0 y = ((0, 1), y)
extGCD x y = ((t - s * q, s), g)
  where
    (q, r) = quotRem y x
    ((s, t), g) = extGCD r x

-- Modular inverse
modInv :: Integral a => a -> a -> Either a a
modInv x p = if g == 1 then return (mod y p) else Left g
  where
    ((y, _), g) = extGCD x p
```

## C.2 WeierstrassEquations.hs

This module includes data for Weierstrass curves in Section 1.2, as well as related quantities and transformations.

```
{-# LANGUAGE GADTs #-}
{-# LANGUAGE StandaloneDeriving #-}

module WeierstrassEquations (EC (..), discriminant, isSmooth, jInvariant,
  isIsomorphic, lW, l2m, mW, m2s, sW) where

import Fields
```

---

```
-- Elliptic curves

-- Weierstrass curve data
data EC f where
  EC :: Field f => f -> f -> f -> f -> f -> EC f
deriving instance Eq (EC f)
instance Show (EC f) where
  show (EC a_1 a_2 a_3 a_4 a_6) = "y^2" ++ show' a_1 "xy" ++ show' a_3 "y"
    ++ " = " ++ "x^3" ++ show' a_2 "x^2" ++ show' a_4 "x" ++ show' a_6 ""
    where
      show' n s
        | signum n == 1 = " + " ++ show n ++ s
        | signum n == -1 = " - " ++ show (abs n) ++ s
        | otherwise = ""

-- Quantities
a_1, a_2, a_3, a_4, a_6, b_2, b_4, b_6, b_8, c_4, c_6 :: EC f -> f
a_1 (EC a_1 _ _ _ _) = a_1
a_2 (EC _ a_2 _ _ _) = a_2
a_3 (EC _ _ a_3 _ _) = a_3
a_4 (EC _ _ _ a_4 _) = a_4
a_6 (EC _ _ _ _ a_6) = a_6
b_2 e@(EC _ _ _ _ _) = a_1 e ^ 2 + 4 * a_2 e
b_4 e@(EC _ _ _ _ _) = a_1 e * a_3 e + 2 * a_4 e
b_6 e@(EC _ _ _ _ _) = a_3 e ^ 2 + 4 * a_6 e
b_8 e@(EC _ _ _ _ _) = a_1 e ^ 2 * a_6 e + 4 * a_2 e * a_6 e
  - a_1 e * a_3 e * a_4 e + a_2 e * a_3 e ^ 2 - a_4 e ^ 2
c_4 e@(EC _ _ _ _ _) = b_2 e ^ 2 - 24 * b_4 e
c_6 e@(EC _ _ _ _ _) = 36 * b_2 e * b_4 e - b_2 e ^ 3 - 216 * b_6 e
```

---

```
-- Smoothness and isomorphism

-- Discriminant
discriminant :: EC f -> f
discriminant e@(EC _ _ _ _ _) = 9 * b_2 e * b_4 e * b_6 e
  - b_2 e ^ 2 * b_8 e - 8 * b_4 e ^ 3 - 27 * b_6 e ^ 2

-- Check if elliptic curve is smooth by discriminant
isSmooth :: EC f -> Bool
isSmooth e@(EC _ _ _ _ _) = discriminant e /= 0
```

```
-- Verify that elliptic curve is smooth by discriminant
assertSmooth :: EC f -> Either String (EC f)
assertSmooth e = if isSmooth e then return e else
  Left $ "Curve " ++ show e ++ " is not smooth"

-- J-invariant
jInvariant :: EC f -> f
jInvariant e@(EC _ _ _ _ _) = c_4 e ^ 3 / discriminant e

-- Check if elliptic curves are isomorphic by j-invariant
isIsomorphic :: EC f -> EC f -> Bool
isIsomorphic e@(EC _ _ _ _ _) e'@(EC _ _ _ _ _) =
  jInvariant e == jInvariant e'

-- Verify that elliptic curves are isomorphic by j-invariant
assertIsomorphic :: EC f -> EC f -> Either String (EC f)
assertIsomorphic e e' = if isIsomorphic e e' then return e' else
  Left $ "Curves " ++ show e ++ " and " ++ show e' ++ " are not isomorphic"
```

---

```
-- Affine transformations

-- Elliptic curve from long Weierstrass equation
lW :: Field f => f -> f -> f -> f -> f -> Either String (EC f)
lW = ((((assertSmooth .) .) .) .) . EC

-- Convert long to medium Weierstrass equation
l2m :: Field f => EC f -> Either String (EC f)
l2m e = mW (b_2 e / 4) (b_4 e / 2) (b_6 e / 4) >>= assertIsomorphic e

-- Elliptic curve from medium Weierstrass equation
mW :: Field f => f -> f -> f -> Either String (EC f)
mW = ((assertSmooth .) .) . flip (EC 0) 0

-- Convert medium to short Weierstrass equation
m2s :: Field f => EC f -> Either String (EC f)
m2s e = sW (-c_4 e / 48) (-c_6 e / 864) >>= assertIsomorphic e

-- Elliptic curve from short Weierstrass equation
sW :: Field f => f -> f -> Either String (EC f)
sW = (assertSmooth .) . EC 0 0 0
```

## C.3 GroupLaw.hs

This module includes data for the group law in Section 1.3, as well as those of points.

```
{-# LANGUAGE GADTs #-}
{-# LANGUAGE StandaloneDeriving #-}

module GroupLaw (GroupLaw (..), OrdP, P (..), computeOrder, isDefined,
  enumPoints) where

import Fields
import WeierstrassEquations

import Data.Group (Abelian, Group (..))
import Data.Maybe (catMaybes)

-----------------------------------------------------------------------------

-- Points

-- Point data
data P f where
  A :: Field f => EC f -> f -> f -> P f
  O :: P f
deriving instance Eq (P f)
instance Show (P f) where
  show O = "O"
  show (A _ x y) = "(" ++ show x ++ "," ++ show y ++ ")"

-- Check if point is defined in elliptic curve
isDefined :: P f -> Bool
isDefined (A (EC a_1 a_2 a_3 a_4 a_6) x y) = y ^ 2 + a_1 * x * y + a_3 * y
  == x ^ 3 + a_2 * x ^ 2 + a_4 * x + a_6
isDefined _ = True

-- Verify that point is defined in elliptic curve
assertDefined :: P f -> P f
assertDefined p = if isDefined p then p else
  error $ "Point " ++ show p ++ " is not in curve"

-----------------------------------------------------------------------------

-- Group instances

-- Elliptic curve is a monoid
instance Field f => Monoid (P f) where
  mempty = O
  mappend p p' = case (assertDefined p, assertDefined p') of
    (O, A _ _ _) -> p'
    (A _ _ _, O) -> p
    (A e @ (EC a_1 a_2 a_3 a_4 a_6) x y, A e' x' y')
      | e /= e' -> error "Curves are different"
      | x /= x' -> A e (x'' l_a) (y'' l_a m_a)
      | y + y' + a_1 * x' + a_3 /= 0 -> A e (x'' l_d) (y'' l_d m_d)
      | otherwise -> O
      where
        l_a = (y - y') / n_a
```

```
        m_a = (x * y' - x' * y) / n_a
        n_a = x - x'
        l_d = (3 * x ^ 2 + 2 * a_2 * x + a_4 - a_1 * y) / n_d
        m_d = (-x ^ 3 + a_4 * x + 2 * a_6 - a_3 * y) / n_d
        n_d = 2 * y + a_1 * x + a_3
        x'' l = l ^ 2 + a_1 * l - a_2 - x - x'
        y'' l m = - l * x'' l - a_1 * x'' l - m - a_3
    _ -> O

-- Elliptic curve is a group
instance Field f => Group (P f) where
  invert p = case assertDefined p of
    A e @ (EC a_1 _ a_3 _ _) x y -> A e x $ -y - a_1 * x - a_3
    _ -> O

-- Elliptic curve is an abelian group
instance Field f => Abelian (P f)

-- Elliptic curve has a group law
class Abelian p => GroupLaw p where
  o :: p
  o = mempty
  neg :: p -> p
  neg = invert
  add :: p -> p -> p
  add = mappend
  dup :: p -> p
  dup = mconcat . replicate 2
  mul :: Integral n => n -> p -> p
  mul 0 _ = o
  mul n p
    | n < 0 = neg $ mul (-n) p
    | otherwise = (if even n then id else add p) . dup $ mul (quot n 2) p

-- Elliptic curve over field has a group law
instance Field f => GroupLaw (P f)
```

---

```
-- Orders

-- Group of points with order data
data OrdP f where
  OrdP :: Field f => P f -> Int -> OrdP f
deriving instance Eq (OrdP f)
instance Show (OrdP f) where
  show (OrdP p n) = "ord(" ++ show p ++ ") = " ++ show n

-- Compute order of point
computeOrder :: Field f => P f -> Maybe (OrdP f)
computeOrder p = orderPoint' p $ OrdP p 1
  where
    orderPoint' O pq = return pq
    orderPoint' p' @ (A _ x y) (OrdP p'' n) = case (val x, val y) of
      (NumDen _ d', NumDen _ d'')
```

```
        | d' > 1 || d'' > 1 -> Nothing
      _ -> orderPoint' (add p' p'') $ OrdP p'' (succ n)

-- Enumerate points with naive approach
enumPoints :: Prime p => EC (Fp p) -> [OrdP (Fp p)]
enumPoints e = catMaybes orders
  where
    values = [minBound .. maxBound]
    points = filter isDefined [A e x y | x <- values, y <- values]
    orders = map computeOrder $ o : points
```

## C.4 Rationals.hs

This module includes the algorithms in Section 3.2 and Section 3.7.

```
module Rationals (computeRank, computeTors, getRankEqns) where

import Fields
import WeierstrassEquations
import GroupLaw

import Data.List (nub, union)
import Data.Maybe (catMaybes)
```

---

```
-- Auxiliary functions

-- Type synonym
type Z = Integer

-- Throw errors
throw :: Either String a -> a
throw = either error id
```

---

```
-- Torsion computation

-- Elliptic curve E : y^2 = x^3 + Ax + B over Z
data ET = ET Z Z

-- Construct elliptic curve over Q with Z coefficients
eQ :: ET -> EC Q
eQ (ET a b) = throw $ sW (fromInteger a) (fromInteger b)

-- Construct elliptic curve E : y^2 = x^3 + Ax + B over Z
eT :: EC Q -> ET
eT e = ET n'' n'''
  where
    EC _ _ _ a b = throw $ l2m e >>= m2s
    (NumDen n d, NumDen n' d') = (val a, val b)
    (a', b') = (n * d ^ 3 * d' ^ 4, n' * d ^ 6 * d' ^ 5)
    EC _ _ _ a'' b'' = throw $ sW (fromInteger a') (fromInteger b') :: EC Q
    (NumDen n'' _, NumDen n''' _) = (val a'', val b'')

-- Get all non-negative y coordinates such that y^2 | Delta
getYs :: ET -> [Z]
getYs (ET a b) = 0 : filter divisible [1 .. squareRoot delta]
  where
    delta = 4 * a ^ 3 + 27 * b ^ 2
    squareRoot = ceiling . sqrt . fromInteger
    divisible = (== 0) . mod delta . (^ 2)

-- Get all points for each non-negative y coordinate
getPoints :: ET -> Z -> [P Q]
getPoints e @ (ET a b) y = filter isDefined $ map project allXs
  where
```

```
    bY2 = abs $ b - y ^ 2
    maxX = if bY2 == 0 then abs a else bY2
    positiveXs = filter ((== 0) . mod bY2) [1 .. maxX]
    allXs = 0 : union positiveXs (map negate positiveXs)
    project = flip (A $ eQ e) (fromInteger y) . fromInteger

-- Compute torsion subgroup
computeTors :: EC Q -> [OrdP Q]
computeTors e = catMaybes $ map computeOrder allPoints
  where
    e' = eT e
    positivePoints = concatMap (getPoints e') (getYs e')
    allPoints = o : union positivePoints (map neg positivePoints)
```

---

```
-- Rank computation

-- Elliptic curve E : y^2 = x^3 + Ax^2 + Bx over Z
data ER = ER Z Z

-- Diophantine equation data
data D = D Z Z Z
instance Show D where
  show (D a_ b_ beta) = "Y^2 =" ++ show' beta "X^4"
    ++ show' a_ "X^2Z^2" ++ show' (quot b_ beta) "Z^4"
    where
      show' n s
        | n < 0 = " - " ++ show (abs n) ++ s
        | n > 0 = " + " ++ show n ++ s
        | otherwise = ""

-- Construct elliptic curve E : y^2 = x^3 + Ax^2 + Bx over Z
eR :: EC Q -> ER
eR e = case throw (l2m e) of
  EC _ _ a b 0 -> ER n'' n'''
    where
      (NumDen n d, NumDen n' d') = (val a, val b)
      (a', b') = (n * d * d' ^ 2, n' * d ^ 4 * d' ^ 3)
      EC _ _ a'' b'' 0 = throw $
        mW (fromInteger a') (fromInteger b') 0 :: EC Q
      (NumDen n'' _, NumDen n''' _) = (val a'', val b'')
  _ -> error $ "Curve " ++ show (l2m e) ++ " does not contain (0, 0)"

-- Free squares in integer
freeSquares :: Z -> Z
freeSquares = freeSquares' 2
  where
    freeSquares' n m
      | n' > m = m
      | mod m n' == 0 = freeSquares' n $ quot m n'
      | otherwise = freeSquares' (succ n) m
      where
        n' = n^2
```

```
-- Get diophantine equations for image
getImageEqns :: ER -> [D]
getImageEqns (ER a b) = map (D (fromInteger a) (fromInteger b)) allBs
  where
    positiveBs = filter ((== 0) . mod (abs b)) [1 .. abs b]
    squarefreeBs = nub $ map freeSquares positiveBs
    allBs = squarefreeBs ++ map negate squarefreeBs

-- Get diophantine equations for both images
getRankEqns :: EC Q -> ([D], [D])
getRankEqns e = (getImageEqns e', getImageEqns e'')
  where
    e' @ (ER a b) = eR e
    e'' = eR . throw $
      mW (fromInteger (-2 * a)) (fromInteger (a ^ 2 - 4 * b)) 0

-- Compute rank with number of solutions to diophantine equations
computeRank :: Z -> Z -> Z
computeRank e e' = floor . logBase 2 $ fromInteger (e * e') / 4
```

## C.5 Applications.hs

This module includes the algorithms in Section 4.1 and Section 4.2.

```
{-# LANGUAGE GADTs #-}
{-# LANGUAGE ScopedTypeVariables #-}

module Applications (Divisor (..), Key (..), Keys (..), division, dh, ecdh,
  fermat, lenstra, modExp, pocklington, pollard, rsa, trial) where

import Fields
import WeierstrassEquations
import GroupLaw

import Control.Exception (SomeException, evaluate, try)
import System.IO.Unsafe (unsafePerformIO)

-----------------------------------------------------------------------------

-- Auxiliary functions

-- Probable primes
primes :: [Integer]
primes = 2 : 3 : concatMap ((<*>) [pred, succ] . return) [6, 12 ..]

-- Modular exponentiation
modExp :: (Integral a, Integral b) => a -> b -> a -> a
modExp _ 0 _ = 1
modExp 0 _ _ = 0
modExp x e p
  | odd e = mod (x * m) p
  | otherwise = m
  where
    m = modExp (mod (x * x) p) (quot e 2) p

-----------------------------------------------------------------------------

-- Integer factorisation

-- Integer factorisation divisor data
newtype Divisor = Divisor (Either String Integer)
instance Show Divisor where
  show (Divisor (Left s)) = s
  show (Divisor (Right n)) = show n ++ " is a divisor"

-- Naive integer factorisation
division :: Integer -> [Integer]
division = division' primes
  where
    division' ts' @ (t : ts) n
      | n <= 1 = []
      | r == 0 = t : division' ts' q
      | otherwise = division' ts n
      where
        (q, r) = quotRem n t

-- Pollard's p - 1 method with given smoothness bound b
```

```
pollard :: Integer -> Integer -> Divisor
pollard n b = Divisor $ pollard' 2
  where
    l = foldr lcm 1 [2 .. b]
    pollard' a = case gcd n . pred $ modExp a l n of
      1 -> Left "Choose a larger smoothness bound"
      g -> if g < n then return g else pollard' (succ a)

-- Lenstra's elliptic curve factorisation method
-- with given (x, y) coordinates and smoothness bound c
lenstra :: Prime p => Fp p -> Fp p -> Fp p -> Integer -> Divisor
lenstra (_ :: Fp p) x y c = Divisor $ lenstra' (succ minBound :: Fp p)
  where
    n = char (undefined :: Fp p)
    l = foldr lcm 1 [2 .. c]
    lenstra' a = case gcd n d of
      1 -> unsafe (mul l p) (lenstra' a')
        where
          e = either error id $ sW a b
          p = A e x y
      g -> if g < n then return g else lenstra' a'
      where
        a' = succ a
        b = y ^ 2 - x ^ 3 - a * x
        d = 4 * fromIntegral a ^ 3 + 27 * fromIntegral b ^ 2

-- Haskell-specific IO hack, not safe for work
unsafe :: Monad m => P (Fp p) -> m Integer -> m Integer
unsafe x y = unsafePerformIO $ try' x >>= return' y
  where
    try' :: P (Fp p) -> IO (Either SomeException (P (Fp p)))
    try' = try . evaluate
    read' = reads :: ReadS Integer
    gcd' = return . return . fst . head . read' . show
    return' = either gcd' . const . return
```

---

```
-- Primality testing

-- Primality certificate data
data Certificate = Threshold | Composite Integer | Definite Integer
                 | Certified Integer (Integer, [Integer]) [(Integer, Integer)]
instance Show Certificate where
  show Threshold = "Choose a larger trial division threshold"
  show (Composite n) = show n ++ " is composite"
  show (Definite n) = show n ++ " is definitely prime"
  show (Certified n (d, fs) cs) = "N = " ++ show n
    ++ " is certified prime\nr = " ++ show d ++ " divides N - 1 and r = Pi "
    ++ show fs ++ "\n" ++ concatMap (uncurry show') cs
    where
      show' p a = show a ++ "^(N - 1) = 1 mod N and gcd(" ++ show a
        ++ "^((N - 1)/" ++ show p ++ ") - 1, N) = 1 mod N \n"

-- Naive primality test
```

```
trial :: Integer -> Bool
trial n = n > 1 && all indivisible primes'
  where
    squareRoot = floor . sqrt . fromInteger
    primes' = takeWhile (<= squareRoot n) primes
    indivisible = (/= 0) . mod n

-- Fermat's little theorem
fermat :: Integer -> Integer -> Bool
fermat n t = if n < 4 then trial n else
  n > 1 && all one [2 .. mod (t - 1) (n - 3) + 2]
  where
    one p = modExp p (pred n) n == 1

-- Pocklington-Lehmer primality test with a trial division threshold t
pocklington :: Integer -> Integer -> Certificate
pocklington n b
  | n <= b || n <= 2 = if trial n then Definite n else Composite n
  | otherwise = pocklington' 1 primes $ pred n
  where
    pocklington' d ps' @ (p : ps) n'
      | p > b = Threshold
      | d >= floor (sqrt $ fromInteger n) = Certified n (d, []) []
      | r == 0 = case generate 2 of
        Just a -> case pocklington' (p * d) ps' q of
          Certified m (d', fs) cs @ ((p', _) : _)
            | p == p' -> Certified m (d', p : fs) cs
          Certified m (d', fs) cs -> Certified m (d', p : fs) $ (p, a) : cs
          c -> c
        _ -> Composite n
      | otherwise = pocklington' d ps n'
      where
        (q, r) = quotRem n' p
        generate a
          | a >= n = Nothing
          | modExp a' p n == 1 && gcd (pred a') n == 1 = Just a
          | otherwise = generate $ succ a
          where
            a' = modExp a (quot (pred n) p) n
```

---

```
-- Cryptography

-- Public and private key data
data Keys = Keys Key Key | Locked
instance Show Keys where
  show (Keys e d) = "Public encryption key is " ++ show e
    ++ "\nPrivate decryption key is " ++ show d
  show _ = "One of p or q is not prime"

-- Encryption or decryption key data
data Key = Key Integer Integer
instance Show Key where
  show (Key n k) = "(" ++ show n ++ ", " ++ show k ++ ")"
```

```
-- Rivest-Shamir-Adleman cryptosystem with primes p and q
rsa :: Integer -> Integer -> Keys
rsa p q = case modInv e l of
  Right d -> Keys (Key n e) (Key n d)
  _ -> Locked
  where
    n = p * q
    l = lcm (pred p) (pred q)
    e = head $ filter ((== 1) . gcd l) [2 ..]

-- Key exchange data
data Exchange a where
  Exchange :: Show a => a -> a -> a -> Exchange a
instance Show (Exchange a) where
  show (Exchange a b s) = "First key is " ++ show a ++ "\nSecond key is "
    ++ show b ++ "\nPrivate symmetric key is " ++ show s

-- Diffie-Hellman key exchange
dh :: Key -> Integer -> Integer -> Exchange Integer
dh (Key p g) a b = Exchange (modExp g a p) (modExp g b p) (modExp g (a * b) p)

-- Elliptic curve Diffie-Hellman
ecdh :: Prime p => P (Fp p) -> Integer -> Integer -> Exchange (P (Fp p))
ecdh p a b = Exchange (mul a p) (mul b p) (mul (a * b) p)
```

## C.6 Test.hs

This module includes input of computations from previous modules.

```
{-# LANGUAGE ScopedTypeVariables #-}

module Test where

import Fields
import WeierstrassEquations
import GroupLaw
import Rationals
import Applications

import Data.Either (rights)
```

---

```
-- Prime and composite integers

data P2 = P2 deriving (Enum, Show)
instance Prime P2

data P3 = P3 deriving (Enum, Show)
instance Prime P3

data P5 = P5 deriving (Enum, Show)
instance Prime P5

data P199843247 = P199843247 deriving (Enum, Show)
instance Prime P199843247

data P1715761513 = P1715761513 deriving (Enum, Show)
instance Prime P1715761513

data P2147483647 = P2147483647 deriving (Enum, Show)
instance Prime P2147483647
```

---

```
-- Auxiliary functions

throw :: Either String a -> a
throw = either error id

writeLMS :: Field f => EC f -> String
writeLMS e = "Weierstrass equation transformations:\nfrom long " ++ show e
  ++ ",\nto medium " ++ show (throw $ l2m e)
  ++ ",\nand to short " ++ show (throw $ l2m e >>= m2s) ++ "\n"

writeAddition :: Field f => P f -> P f -> String
writeAddition p p' = "Point P = " ++ show p ++ " and P' = " ++ show p'
  ++ " addition:\nP + P' = " ++ show (add p p') ++ "\n"

writeFinite :: Prime p => EC (Fp p) -> String
writeFinite (e :: EC (Fp p)) = "Group of " ++ show e ++ " over F_"
  ++ show (char (undefined :: Fp p)) ++ ":\n"
```

```
  ++ unlines (map show $ enumPoints e)

writeTorsion :: EC Q -> String
writeTorsion e = "Torsion subgroup of " ++ show e ++ ":\n"
  ++ unlines (map show $ computeTors e)

writeRank :: EC Q -> String
writeRank e = "Rank equations for a of " ++ show e ++ ":\n"
  ++ unlines (map show a) ++ "Rank equations for a' of " ++ show e ++ ":\n"
  ++ unlines (map show a')
  where
    (a, a') = getRankEqns e

writeDivision :: Integer -> String
writeDivision n = "Naive integer factorisation on " ++ show n ++ ":\n"
  ++ show n ++ " = Pi " ++ show (division n) ++ "\n"

writePollard :: Integer -> Integer -> String
writePollard n b = "Pollard's p - 1 method on " ++ show n ++ " with B = "
  ++ show b ++ ":\n" ++ show (pollard n b) ++ "\n"

writeLenstra :: Prime p => Fp p -> Fp p -> Fp p -> Integer -> String
writeLenstra (f :: Fp p) x y c =
  "Lenstra's elliptic curve factorisation method on "
  ++ show (char (undefined :: Fp p)) ++ " with C = " ++ show c ++ ":\n"
  ++ show (lenstra f x y c) ++ "\n"

writeTrial :: Integer -> String
writeTrial n = "Naive primality test on " ++ show n ++ ":\n" ++ show n
  ++ (if trial n then " is prime" else " is composite") ++ "\n"

writeFermat :: Integer -> Integer -> String
writeFermat n t = "Fermat's primality test on " ++ show n ++ " with "
  ++ show t ++ " tests:\n" ++ show n
  ++ (if fermat n t then " is probably prime" else " is composite") ++ "\n"

writePocklington :: Integer -> Integer -> String
writePocklington n b = "Pocklington-Lehmer primality test on " ++ show n
  ++ " with B = " ++ show b ++ ":\n" ++ show (pocklington n b)

writeRSA :: Integer -> Integer -> Integer -> String
writeRSA p q m = "Rivest-Shamir-Adleman cryptosystem on p = " ++ show p
  ++ " and q = " ++ show q ++ ":\n" ++ show (rsa p q) ++ "\n"

writeDH :: Key -> Integer -> Integer -> String
writeDH k @ (Key p g) a b =
  "Diffie-Hellman key exchange on p = " ++ show p ++ " and g = " ++ show g
  ++ ":\n" ++ show (dh k a b) ++ "\n"

writeECDH :: Prime p => P (Fp p) -> Integer -> Integer -> String
writeECDH (p @ (A e x y) :: P (Fp p)) a b =
  "Elliptic curve Diffie-Hellman on P = " ++ show p ++ ":\nP in E : "
  ++ show e ++ " over F_" ++ show (char (undefined :: Fp p)) ++ "\n"
  ++ show (ecdh p a b) ++ "\n"
```

```
writeECDH _ _ _ =
  "Elliptic curve Diffie-Hellman on O:\nChoose a different point\n"

--------------------------------------------------------------------------------

-- Main functions

main :: IO ()
main = writeFile "Output.txt" . unlines $
  [ writeLMS eLMS
  , writeAddition (A eAddition 0 (-1)) (A eAddition 1 2)
  , writeAddition (A eAddition 0 (-1)) (A eAddition 0 (-1))
  , writeAddition (A eAddition 1 2) (A eAddition 1 2)
  ] ++
  map writeFinite e2s ++
  map writeFinite e3s ++
  map writeFinite [e5] ++
  [ writeTorsion e0
  , writeTorsion e0'
  , writeTorsion e1
  , writeTorsion e2
  , writeTorsion e3
  , writeTorsion e4
  , writeRank e1
  , writeRank e2
  , writeRank e3
  , writeRank e4
  , writeDivision 420
  , writeDivision 421
  , writePollard 246082373 7
  , writePollard 246082373 9
  , writePollard 7591548931 20
  , writePollard 7591548931 25
  , writeLenstra (undefined :: Fp P1715761513) 2 1 17
  , writeLenstra (undefined :: Fp P199843247) 1 1 11
  , writeTrial 420
  , writeTrial 421
  , writeTrial 561
  , writeFermat 420 1
  , writeFermat 421 1
  , writeFermat 561 1
  , writeFermat 561 2
  , writePocklington 2147483647 200
  , writePocklington 9223372036854775783 400000
  , writeRSA 2147483647 2147483659 123456789
  , writeDH (Key 2147483647 65537) 16777259 16777289
  , writeECDH (A eDH 0 1) 16777259 16777289
  ]
  where
    eLMS = throw $ lW 2 (-1) (1 / 3) (-1 / 3) (-1 / 27) :: EC Q
    eAddition = throw $ sW 2 1 :: EC Q
    e0 = throw $ sW 0 4 :: EC Q
    e0' = throw $ sW 0 (-4) :: EC Q
    e1 = throw $ sW (-1) 0 :: EC Q
    e2 = throw $ sW (-5) 0 :: EC Q
```

```
e3 = throw $ sW (-17) 0 :: EC Q
e4 = throw $ sW (-226) 0 :: EC Q
e5 = throw $ sW 1 1 :: EC (Fp P5)
e2s = rights [lW a_1 a_2 a_3 a_4 a_5 | a_1 <- values, a_2 <- values,
  a_3 <- values, a_4 <- values, a_5 <- values] :: [EC (Fp P2)]
  where
    values = [minBound .. maxBound]
e3s = rights [mW a b c | a <- values, b <- values, c <- values]
  :: [EC (Fp P3)]
  where
    values = [minBound .. maxBound]
eDH = throw $ sW 65537 1 :: EC (Fp P2147483647)
```

## C.7 Output.txt

This file includes output of computations from previous modules.

```
Weierstrass equation transformations:
from long y^2 + 2xy + 1/3y = x^3 - 1x^2 - 1/3x - 1/27,
to medium y^2 = x^3 - 1/108,
and to short y^2 = x^3 - 1/108

Point P = (0,-1) and P' = (1,2) addition:
P + P' = (8,-23)

Point P = (0,-1) and P' = (0,-1) addition:
P + P' = (1,2)

Point P = (1,2) and P' = (1,2) addition:
P + P' = (-7/16,-13/64)

Group of y^2 + 1y = x^3 over F_2:
ord(O) = 1
ord((0,0)) = 3
ord((0,1)) = 3

Group of y^2 + 1y = x^3 + 1 over F_2:
ord(O) = 1
ord((1,0)) = 3
ord((1,1)) = 3

Group of y^2 + 1y = x^3 + 1x over F_2:
ord(O) = 1
ord((0,0)) = 5
ord((0,1)) = 5
ord((1,0)) = 5
ord((1,1)) = 5

Group of y^2 + 1y = x^3 + 1x + 1 over F_2:
ord(O) = 1

Group of y^2 + 1y = x^3 + 1x^2 over F_2:
ord(O) = 1
ord((0,0)) = 5
ord((0,1)) = 5
ord((1,0)) = 5
ord((1,1)) = 5

Group of y^2 + 1y = x^3 + 1x^2 + 1 over F_2:
ord(O) = 1

Group of y^2 + 1y = x^3 + 1x^2 + 1x over F_2:
ord(O) = 1
ord((0,0)) = 3
ord((0,1)) = 3

Group of y^2 + 1y = x^3 + 1x^2 + 1x + 1 over F_2:
ord(O) = 1
```

```
ord((1,0)) = 3
ord((1,1)) = 3

Group of y^2 + 1xy = x^3 + 1 over F_2:
ord(O) = 1
ord((0,1)) = 2
ord((1,0)) = 4
ord((1,1)) = 4

Group of y^2 + 1xy = x^3 + 1x over F_2:
ord(O) = 1
ord((0,0)) = 2
ord((1,0)) = 4
ord((1,1)) = 4

Group of y^2 + 1xy + 1y = x^3 + 1 over F_2:
ord(O) = 1
ord((1,0)) = 2

Group of y^2 + 1xy + 1y = x^3 + 1x + 1 over F_2:
ord(O) = 1
ord((1,1)) = 2

Group of y^2 + 1xy = x^3 + 1x^2 + 1 over F_2:
ord(O) = 1
ord((0,1)) = 2

Group of y^2 + 1xy = x^3 + 1x^2 + 1x over F_2:
ord(O) = 1
ord((0,0)) = 2

Group of y^2 + 1xy + 1y = x^3 + 1x^2 over F_2:
ord(O) = 1
ord((0,0)) = 4
ord((0,1)) = 4
ord((1,0)) = 2

Group of y^2 + 1xy + 1y = x^3 + 1x^2 + 1x over F_2:
ord(O) = 1
ord((0,0)) = 4
ord((0,1)) = 4
ord((1,1)) = 2

Group of y^2 = x^3 + 1x over F_3:
ord(O) = 1
ord((0,0)) = 2
ord((2,1)) = 4
ord((2,2)) = 4

Group of y^2 = x^3 + 1x + 1 over F_3:
ord(O) = 1
ord((0,1)) = 4
ord((0,2)) = 4
ord((1,0)) = 2
```

```
Group of y^2 = x^3 + 1x + 2 over F_3:
ord(O) = 1
ord((1,1)) = 4
ord((1,2)) = 4
ord((2,0)) = 2

Group of y^2 = x^3 + 2x over F_3:
ord(O) = 1
ord((0,0)) = 2
ord((1,0)) = 2
ord((2,0)) = 2

Group of y^2 = x^3 + 2x + 1 over F_3:
ord(O) = 1
ord((0,1)) = 7
ord((0,2)) = 7
ord((1,1)) = 7
ord((1,2)) = 7
ord((2,1)) = 7
ord((2,2)) = 7

Group of y^2 = x^3 + 2x + 2 over F_3:
ord(O) = 1

Group of y^2 = x^3 + 1x^2 + 1 over F_3:
ord(O) = 1
ord((0,1)) = 6
ord((0,2)) = 6
ord((1,0)) = 2
ord((2,1)) = 3
ord((2,2)) = 3

Group of y^2 = x^3 + 1x^2 + 2 over F_3:
ord(O) = 1
ord((1,1)) = 3
ord((1,2)) = 3

Group of y^2 = x^3 + 1x^2 + 1x + 1 over F_3:
ord(O) = 1
ord((0,1)) = 3
ord((0,2)) = 3
ord((1,1)) = 6
ord((1,2)) = 6
ord((2,0)) = 2

Group of y^2 = x^3 + 1x^2 + 1x + 2 over F_3:
ord(O) = 1
ord((2,1)) = 3
ord((2,2)) = 3

Group of y^2 = x^3 + 1x^2 + 2x over F_3:
ord(O) = 1
ord((0,0)) = 2
```

```
ord((1,1)) = 3
ord((1,2)) = 3
ord((2,1)) = 6
ord((2,2)) = 6

Group of y^2 = x^3 + 1x^2 + 2x + 1 over F_3:
ord(O) = 1
ord((0,1)) = 3
ord((0,2)) = 3

Group of y^2 = x^3 + 2x^2 + 1 over F_3:
ord(O) = 1
ord((0,1)) = 5
ord((0,2)) = 5
ord((1,1)) = 5
ord((1,2)) = 5

Group of y^2 = x^3 + 2x^2 + 2 over F_3:
ord(O) = 1
ord((2,0)) = 2

Group of y^2 = x^3 + 2x^2 + 1x + 1 over F_3:
ord(O) = 1
ord((0,1)) = 5
ord((0,2)) = 5
ord((2,1)) = 5
ord((2,2)) = 5

Group of y^2 = x^3 + 2x^2 + 1x + 2 over F_3:
ord(O) = 1
ord((1,0)) = 2

Group of y^2 = x^3 + 2x^2 + 2x over F_3:
ord(O) = 1
ord((0,0)) = 2

Group of y^2 = x^3 + 2x^2 + 2x + 2 over F_3:
ord(O) = 1
ord((1,1)) = 5
ord((1,2)) = 5
ord((2,1)) = 5
ord((2,2)) = 5

Group of y^2 = x^3 + 1x + 1 over F_5:
ord(O) = 1
ord((0,1)) = 9
ord((0,4)) = 9
ord((2,1)) = 3
ord((2,4)) = 3
ord((3,1)) = 9
ord((3,4)) = 9
ord((4,2)) = 9
ord((4,3)) = 9
```

```
Torsion subgroup of y^2 = x^3 + 4:
ord(O) = 1
ord((0,2)) = 3
ord((0,-2)) = 3

Torsion subgroup of y^2 = x^3 - 4:
ord(O) = 1

Torsion subgroup of y^2 = x^3 - 1x:
ord(O) = 1
ord((0,0)) = 2
ord((1,0)) = 2
ord((-1,0)) = 2

Torsion subgroup of y^2 = x^3 - 5x:
ord(O) = 1
ord((0,0)) = 2

Torsion subgroup of y^2 = x^3 - 17x:
ord(O) = 1
ord((0,0)) = 2

Torsion subgroup of y^2 = x^3 - 226x:
ord(O) = 1
ord((0,0)) = 2

Rank equations for a of y^2 = x^3 - 1x:
Y^2 = + 1X^4 - 1Z^4
Y^2 = - 1X^4 + 1Z^4
Rank equations for a' of y^2 = x^3 - 1x:
Y^2 = + 1X^4 + 4Z^4
Y^2 = + 2X^4 + 2Z^4
Y^2 = - 1X^4 - 4Z^4
Y^2 = - 2X^4 - 2Z^4

Rank equations for a of y^2 = x^3 - 5x:
Y^2 = + 1X^4 - 5Z^4
Y^2 = + 5X^4 - 1Z^4
Y^2 = - 1X^4 + 5Z^4
Y^2 = - 5X^4 + 1Z^4
Rank equations for a' of y^2 = x^3 - 5x:
Y^2 = + 1X^4 + 20Z^4
Y^2 = + 2X^4 + 10Z^4
Y^2 = + 5X^4 + 4Z^4
Y^2 = + 10X^4 + 2Z^4
Y^2 = - 1X^4 - 20Z^4
Y^2 = - 2X^4 - 10Z^4
Y^2 = - 5X^4 - 4Z^4
Y^2 = - 10X^4 - 2Z^4

Rank equations for a of y^2 = x^3 - 17x:
Y^2 = + 1X^4 - 17Z^4
Y^2 = + 17X^4 - 1Z^4
Y^2 = - 1X^4 + 17Z^4
```

```
Y^2 = - 17X^4 + 1Z^4
Rank equations for a' of y^2 = x^3 - 17x:
Y^2 = + 1X^4 + 68Z^4
Y^2 = + 2X^4 + 34Z^4
Y^2 = + 17X^4 + 4Z^4
Y^2 = + 34X^4 + 2Z^4
Y^2 = - 1X^4 - 68Z^4
Y^2 = - 2X^4 - 34Z^4
Y^2 = - 17X^4 - 4Z^4
Y^2 = - 34X^4 - 2Z^4

Rank equations for a of y^2 = x^3 - 226x:
Y^2 = + 1X^4 - 226Z^4
Y^2 = + 2X^4 - 113Z^4
Y^2 = + 113X^4 - 2Z^4
Y^2 = + 226X^4 - 1Z^4
Y^2 = - 1X^4 + 226Z^4
Y^2 = - 2X^4 + 113Z^4
Y^2 = - 113X^4 + 2Z^4
Y^2 = - 226X^4 + 1Z^4
Rank equations for a' of y^2 = x^3 - 226x:
Y^2 = + 1X^4 + 904Z^4
Y^2 = + 2X^4 + 452Z^4
Y^2 = + 113X^4 + 8Z^4
Y^2 = + 226X^4 + 4Z^4
Y^2 = - 1X^4 - 904Z^4
Y^2 = - 2X^4 - 452Z^4
Y^2 = - 113X^4 - 8Z^4
Y^2 = - 226X^4 - 4Z^4

Naive integer factorisation on 420:
420 = Pi [2,2,3,5,7]

Naive integer factorisation on 421:
421 = Pi [421]

Pollard's p - 1 method on 246082373 with B = 7:
Choose a larger smoothness bound

Pollard's p - 1 method on 246082373 with B = 9:
2521 is a divisor

Pollard's p - 1 method on 7591548931 with B = 20:
Choose a larger smoothness bound

Pollard's p - 1 method on 7591548931 with B = 25:
79801 is a divisor

Lenstra's elliptic curve factorisation method on 1715761513 with C = 17:
26927 is a divisor

Lenstra's elliptic curve factorisation method on 199843247 with C = 11:
10289 is a divisor
```

```
Naive primality test on 420:
420 is composite

Naive primality test on 421:
421 is prime

Naive primality test on 561:
561 is composite

Fermat's primality test on 420 with 1 tests:
420 is composite

Fermat's primality test on 421 with 1 tests:
421 is probably prime

Fermat's primality test on 561 with 1 tests:
561 is probably prime

Fermat's primality test on 561 with 2 tests:
561 is composite

Pocklington-Lehmer primality test on 2147483647 with B = 200:
N = 2147483647 is certified prime
r = 6487866 divides N - 1 and r = Pi [2,3,3,7,11,31,151]
3^(N - 1) = 1 mod N and gcd(3^((N - 1)/2) - 1, N) = 1 mod N
5^(N - 1) = 1 mod N and gcd(5^((N - 1)/3) - 1, N) = 1 mod N
3^(N - 1) = 1 mod N and gcd(3^((N - 1)/7) - 1, N) = 1 mod N
3^(N - 1) = 1 mod N and gcd(3^((N - 1)/11) - 1, N) = 1 mod N
2^(N - 1) = 1 mod N and gcd(2^((N - 1)/31) - 1, N) = 1 mod N
3^(N - 1) = 1 mod N and gcd(3^((N - 1)/151) - 1, N) = 1 mod N

Pocklington-Lehmer primality test on 9223372036854775783 with B = 400000:
N = 9223372036854775783 is certified prime
r = 20223770418 divides N - 1 and r = Pi [2,3,3,3,3,17,23,319279]
3^(N - 1) = 1 mod N and gcd(3^((N - 1)/2) - 1, N) = 1 mod N
2^(N - 1) = 1 mod N and gcd(2^((N - 1)/3) - 1, N) = 1 mod N
2^(N - 1) = 1 mod N and gcd(2^((N - 1)/17) - 1, N) = 1 mod N
2^(N - 1) = 1 mod N and gcd(2^((N - 1)/23) - 1, N) = 1 mod N
2^(N - 1) = 1 mod N and gcd(2^((N - 1)/319279) - 1, N) = 1 mod N

Rivest-Shamir-Adleman cryptosystem on p = 2147483647 and q = 2147483659:
Public encryption key is (4611686039902224373, 5)
Private decryption key is (4611686039902224373, 461168603560725707)

Diffie-Hellman key exchange on p = 2147483647 and g = 65537:
First key is 751856369
Second key is 1654172966
Private symmetric key is 1288974049

Elliptic curve Diffie-Hellman on P = (0,1):
P in E : y^2 = x^3 + 65537x + 1 over F_2147483647
First key is (675295473,1821381850)
Second key is (294235749,438747352)
Private symmetric key is (1210475635,471187571)
```

# References


[1] S Lang. *Elliptic curves: Diophantine analysis*. Berlin, Heidelberg: Springer-Verlag, 1978.

[2] J H Silverman. *The arithmetic of elliptic curves*. Graduate texts in mathematics. Springer-Verlag, 1986.

[3] J H Silverman and J Tate. *Rational points on elliptic curves*. Undergraduate texts in mathematics: Springer-Verlag, 1992.

[4] N Duif. 'Transforming a general cubic elliptic curve equation to Weierstrass form'. In: (2011). URL: http://www.math.tamu.edu/~rojas/cubic2weierstrass.pdf.

[5] S Friedl. 'An elementary proof of the group law for elliptic curves'. In: (2004). URL: http://math.rice.edu/~friedl/papers/AAELLIPTIC.PDF.

[6] E Bombieri. 'Problems of the millennium: the Riemann hypothesis'. In: (2000). URL: https://www.claymath.org/sites/default/files/official_problem_description.pdf.

[7] A Weil. 'Numbers of solutions of equations in finite fields'. In: (1949). URL: https://projecteuclid.org/euclid.bams/1183513798.

[8] B M Dwork. 'On the rationality of the zeta function of an algebraic variety'. In: (1960). URL: https://www.jstor.org/stable/2372974.

[9] P R V Deligne. 'La conjecture de Weil I'. In: (1974). URL: https://arxiv.org/pdf/1807.10810.pdf.

[10] L C Washington. *Elliptic curves: number theory and cryptography*. Taylor and Francis Group, 2008. URL: https://people.cs.nctu.edu.tw/~rjchen/ECC2012S/Elliptic%20Curves%20Number%20Theory%20And%20Cryptography%202n.pdf.

[11] B C Mazur. 'Rational isogenies of prime degree'. In: (1978). URL: https://gdz.sub.uni-[]goettingen.de/id/PPN356556735_0044.

[12] J Achter. 'On computing the rank of elliptic curves'. In: (1992). URL: http://www.math.colostate.edu/~achter/math/brown.pdf.

[13] A Dujella. *History of elliptic curves rank records*. 2017. URL: https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html.

[14] M Bhargava and A Shankar. 'Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0'. In: (2013). URL: https://arxiv.org/pdf/1007.0052.pdf.

[15] J E Cremona. 'Numerical evidence for the Birch–Swinnerton-Dyer conjecture'. In: (2011). URL: https://www.dpmms.cam.ac.uk/research/BSD2011/bsd2011-[]Cremona.pdf.

[16] J H Coates and A J Wiles. 'On the conjecture of Birch and Swinnerton-Dyer'. In: (1977). URL: https://gdz.sub.uni-[]goettingen.de/id/PPN356556735_0039.

[17] B H Gross and D B Zagier. 'Heegner points and derivatives of L-series'. In: (1986). URL: https://wstein.org/papers/bib/Gross-[]Zagier_Heegner_points_and_derivatives_of_Lseries.pdf.

[18] V A Kolyvagin. 'Finiteness of E(Q) and X(E, Q) for a class of Weil curves'. In: (1989). URL: https://wstein.org/papers/bib/kolyvagin-[]finitess_of_EQ_and_sha_for_a_subclass.pdf.

[19] C Breuil et al. 'On the modularity of elliptic curves over Q: wild 3-adic exercises'. In: (2001). URL: http://www.ams.org/journals/jams/2001-[]14-[]04/S0894-[]0347-[]01-[]00370-[]8/S0894-[]0347-[]01-[]00370-[]8.pdf.

[20] J B Tunnell. 'A classical Diophantine problem and modular forms of weight 3/2'. In: (1983). URL: https://gdz.sub.uni-[]goettingen.de/id/PPN356556735_0072.

[21] A V Sutherland. *Elliptic curves*. 2017. URL: https://math.mit.edu/classes/18.783/2017.

[22] F Oort. 'The Weil conjectures'. In: (2014). URL: http://www.nieuwarchief.nl/serie5/pdf/naw5-[]2014-[]15-[]3-[]211.pdf.

[23] G Ellingsrud. 'The Lutz-Nagell theorem and torsion points'. In: (2014). URL: https://www.uio.no/studier/emner/matnat/math/MAT4250/h14/ell2.pdf.

[24] D Testa. 'Elliptic curves'. In: (2014). URL: https://homepages.warwick.ac.uk/~maskal/MA426_EllipticCurves_2018.pdf.

[25] A J Wiles. 'The Birch and Swinnerton-Dyer conjecture'. In: (2000). URL: http://www.claymath.org/sites/default/files/birchswin.pdf.

[26] M F Atiyah and I G Macdonald. *Introduction to commutative algebra*. Taylor and Francis Group, 1969. URL: https://wstein.org/edu/Fall2003/252/references/Atiyah-[]MacDonald/Atiyah-[]McDonald-[]Commutative_Algebra.pdf.

[27] R Hartshorne. *Algebraic geometry*. Graduate texts in mathematics. Springer-Verlag, 1977.

[28] W Fulton. *Algebraic curves*. 2008. URL: http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf.