university of groningen

faculty of science
and engineering

mathematics and applied
mathematics

Proving (in)dependence of rational points on elliptic curves

Bachelor's Project Mathematics

July 2018

Student: Y.B. van Oppen

First supervisor: Dr. J.S. Müller

Second assessor: Dr. M. Derickx

Abstract

It is well known that independence of rational points on an elliptic curve may be proved using canonical heights. In this thesis, an alternative method is explained and implemented in the computer algebra system PARI. Given a set of rational points on an elliptic curve points, we can prove their independence by constructing an injective homomorphism from the Mordell-Weil group (modulo doubles) to a binary vector space. If the images of these points by this homomorphism are independent, then the points are. We may also find dependence relations using this homomorphism. This has a great advantage over finding dependence relations using canonical heights, in which case we can only be certain they hold numerically. If a number of rational points on an elliptic curve is shown to be independent, then this number is a lower bound on the rank of the elliptic curve. Finding the rank is a necessary first step for finding the generators of the Mordell-Weil group.

Contents

1 Introduction

1.1 Motivation

This thesis aims to explain a method to prove independence or dependence of rational points on an elliptic curve, and to implement it in the computer algebra system PARI. To give some motivation, consider the following. A *diophantine equation* is an equation of the form

$$F(x_1, x_2, \ldots, x_n) = 0$$

for some polynomial F with integer or rational coefficients, c.f. page 1 of (Stoll, 2010). A classical problem is to find solutions $(x_1, \ldots, x_n)$ in integers or rationals, respectively. Suppose we restrict our attention to rational coefficients and solutions. If it turns out that F can be reduced to the form

$$F(x, y) = y^2 - x^3 - ax^2 - bx - c \quad \text{for} \quad a, b, c \in \mathbb{Q} \tag{1.1}$$

we could determine whether the curve C consisting of all points $(x, y) \in \mathbb{R}^2$ satisfying (1.1) contains any rational points. According to a famous theorem by Louis J. Mordell, if C is the affine part of an elliptic curve E, then the group of rational points on C (in the projective sense) composes a finitely generated abelian group. We may therefore describe the set of solutions to the diophantine equation by finding the generators of this group. Finding the rank of this group is a necessary first step if we want to find these generators. We can find a lower bound on this rank if we prove some set of rational points on the curve is independent.

1.2 Outline of the method

For now, define an elliptic curve E over $\mathbb{Q}$ as a smooth curve given by an equation

$$y^2 = x^3 + ax + b, \quad \text{where} \quad a, b \in \mathbb{Q},$$

along with a point at infinity. We will make things more precise in the next section, but for the time being, assume we can impose a group structure on the set $E(\mathbb{Q})$ of rational points on E. Because this group turns out to be finitely generated and abelian,

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times T, \quad \text{implying} \quad E(\mathbb{Q})/T \cong \mathbb{Z}^r$$

for some nonnegative integer r, called the *rank* of E. Here T is the torsion subgroup of $E(\mathbb{Q})$. If we have points $P_1, \ldots, P_n \in E(\mathbb{Q})/T$ (which are the technically cosets $P_i + T$ the points $P_i \in E(\mathbb{Q})$ represent) at our disposal and prove they are independent, then n must be a lower bound for r. Independence means that for any $c_1, \ldots, c_n \in \mathbb{Z}$,

$$c_1 P_1 + \cdots + c_n P_n = Q$$

where Q is a points of finite order (with respect to the group structure), implies

$$c_1, \ldots, c_n = 0.$$

To prove independence of the points P_i, we first constructing a homomorphism

$$\varepsilon : E(\mathbb{Q})/2E(\mathbb{Q}) \to (\mathbb{Z}/2\mathbb{Z})^M \quad \text{for some positive integer} \quad M, \tag{1.2}$$

which should be injective. If the images v_i of the points P_i under ε turn out to be linearly independent, then the points P_i must be independent in $E(\mathbb{Q})/2E(\mathbb{Q})$, and so forth, in $E(\mathbb{Q})$. It needs to be emphasized that finding a suitable homomorphism ε will comprise the majority of the theoretical part of this thesis.

The remainder of this thesis is organized as follows: Section 2 explains some background material on elliptic curves and projective geometry. In Section 3, we have a brief look at how independence of rational points on an elliptic curve can be proved using canonical heights instead. Section 4 illustrates the method in detail, and presents the construction of the homomorphism $E(\mathbb{Q})/2E(\mathbb{Q}) \to (\mathbb{Z}/2\mathbb{Z})^M$. The method is tested on three examples (two with independent and one with dependent points) in Section 5, for which the source codes used can be found in Appendix A. At last, an outlook is given in the final section of this thesis.

2 Preliminaries

2.1 The projective plane

In order to fully understand the material in this thesis, the reader should at the very least have a basic understanding of group theory and modular arithmetic. That is, we will assume concepts like and revolving around (sub)groups, factor groups, homomorphisms and isomorphisms to be well understood. Any introductory book on group theory may serve as a reference, for instance (Lang, 2005).

Since elliptic curves are defined in the projective plane, we will first need to address this concept. Let us denote the affine plane by

$$\mathbb{A}^2 := \{ (x, y) \mid x, y \text{ are numbers} \} .$$

We will call pairs (x, y) representing points in $\mathbb{A}^2$ *affine coordinates*. In $\mathbb{A}^2$, pairs of lines have a unique intersection point if and only if they are not parallel. We can extend $\mathbb{A}^2$ in a way that ensures parallel lines have a unique intersection point corresponding to their direction (from a non-oriented point of view).

Definition 1 (Projective plane)**.** A *homogeneous coordinate triple* is a triple $[a, b, c]$ with numbers a, b, c not all zero. The numbers a, b, c are called *homogeneous coordinates*. Two homogeneous coordinates triples $[a_1, b_1, c_1]$, $[a_2, b_2, c_2]$ represent the same point if there exists some nonzero t such that

$$[a_1, b_1, c_1] = [ta_2, tb_2, tc_2],$$

In this case, we say they are equivalent (w.r.t. the equivalence relation $\sim$), so

$$[a_1, b_1, c_1] \sim [a_2, b_2, c_2].$$

We define the *projective plane* $\mathbb{P}^2$ to be the set of equivalence classes of homogeneous coordinates, that is

$$\mathbb{P}^2 = \{ [a, b, c] \text{ is a homogeneous coordinate triple} \} / \sim$$

Analogously, the *projective line* $\mathbb{P}^1$ is the set of equivalence classes of coordinate pairs $[a, b]$ for numbers a, b, not both zero. Two pairs $[a_1, b_1]$, $[a_2, b_2]$ are again equivalent when there exists some nonzero t such that

$$[a_1, b_1] = [ta_2, tb_2].$$

The points on $[a, b] \in \mathbb{P}^1$ represent intersection 'points' of lines parallel to ℓ, given by

$$\ell : ay = xb.$$

For $b \neq 0$, this is simply the slope of such a line. Otherwise, $[a, b] = [a, 0]$ is the *point at infinity*, corresponding to the intersection point of any pair of vertical lines.

So, in a sense, $\mathbb{P}^2$ is the union of $\mathbb{A}^2$ and $\mathbb{P}^1$. For a point $[a, b, c] \in \mathbb{P}^2$, if $c \neq 0$, we may *dehomogenize* the coordinate triple to

$$(a \cdot c^{-1}, b \cdot c^{-1})$$

in affine coordinates. In case $c = 0$, we obtain the point $[a, b] \in \mathbb{P}^1$. Moreover, points $(a, b) \in \mathbb{A}^2$ and $[c, d] \in \mathbb{P}^1$ are can be *homogenized* to

$$[a, b, 1] \quad \text{and} \quad [c, d, 0],$$

respectively.

2.2 Elliptic curves

We need to briefly address the notion of a field before defining elliptic curves.

Definition 2. A *field* is 5-tuple $(F, +, \cdot, 0, 1)$ where F is a set, $+$ and $\cdot$ are operators and $0, 1$ are elements in F, such that for $a, b, c \in F$,

(F1) $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

(F2) $a + b = b + a$ and $a \cdot b = b \cdot a$;

(F3) $a + 0 = a = a \cdot 1$;

(F4) there exists an element $-a \in F$ such that $a + (-a) = 0$;

(F5) for $a \neq 0$, there exists an element $a^{-1} \in F$ such that $a \cdot a^{-1} = 1$;

(F6) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Its *characteristic* $\operatorname{char}(F)$ is the minimal number k such that

$$k \cdot 1 = \underbrace{1 + \cdots + 1}_{k \text{ summands}} = 0,$$

or 0 if no such k exists. This number is always zero or prime.

Definition 3. A *finite field* (or *Galois field*) is field with a finite number of elements. For a prime power q, we denote the field with q elements by $\mathbb{F}_q$, and this field is unique up to isomorphism. The *multiplicative group* of $\mathbb{F}_q$ is denoted $\mathbb{F}_q^\times$.

Note that elliptic curves are curves defined on a projective plane.

Definition 4 (Elliptic curve)**.** An *elliptic curve E over a field* $\mathbb{K}$ is a geometric object defined by an equation

$$E/\mathbb{K} : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \quad a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}. \tag{2.1}$$

Such an equation is called a *homogeneous Weierstrass equation*. An elliptic curve is *nonsingular*, that is, it has a nonzero discriminant

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6,$$

where

$$\begin{aligned} b_2 &:= a_1^2 + 4a_2, \\ b_4 &:= 2a_4 + a_1 a_3, \\ b_6 &:= a_3^2 + 4a_6, \\ b_8 &:= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 + a_4^2. \end{aligned}$$

The *affine part* of an elliptic curve consists of all points that can be dehomogenized to affine coordinates. We may also dehomogenize a homogeneous Weierstrass equation by substituting $x = X/Z$, $y = Y/Z$ to obtain to an *affine Weierstrass equation*

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6. \tag{2.2}$$

To consider only the affine Weierstrass equation is sufficient for most purposes, as an elliptic curve only has one point on the projective line. To see this, note that such a point will necessarily be of the form $[X, Y, 0]$. Substituting this into (2.1), we find $X^3 = 0$, or $X = 0$. So, the only point not included in its affine part is $\mathcal{O} := [0, 1, 0]$, which we will refer to as its *base point*. To simplify notation, we will generally consider affine Weierstrass equations, always remembering there is an additional point $\mathcal{O}$.

Suppose we have an elliptic curve $E/\mathbb{K}$ given by an equation of the form (2.2), where $\mathbb{K}$ is some field with characteristic not equal to 2. Applying the coordinate change

$$y \mapsto \tfrac{1}{2}(y - a_1 x - a_3),$$

allows us to complete the square on the left-hand side of (2.2), yielding

$$y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6,$$

c.f. Section II.1, page 42 in (Silverman, 2009). After performing another coordinate change

$$(x, y) \mapsto (x/4, y/4)$$

we find, after multiplication each side of the resulting equation by 16,

$$y^2 = x^3 + b_2 x^2 + 8b_4 x + 16b_6.$$

Hence, each elliptic curve over a field $\mathbb{K}$ with characteristic not equal to 2 can be expressed by an equation

$$y^2 = x^3 + ax^2 + bx + c, \quad a, b, c \in \mathbb{K}. \tag{2.3}$$

Suppose now that $\mathbb{K} = \mathbb{Q}$ (note $\mathbb{Q}$ has characteristic $0 \neq 2$), and write

$$a = \frac{p}{P}, \quad b = \frac{q}{Q}, \quad c = \frac{r}{R} \quad \text{for integers} \quad p, q, r \in \mathbb{Z} \quad \text{and} \quad P, Q, R \in \mathbb{Z} \setminus \{0\},$$

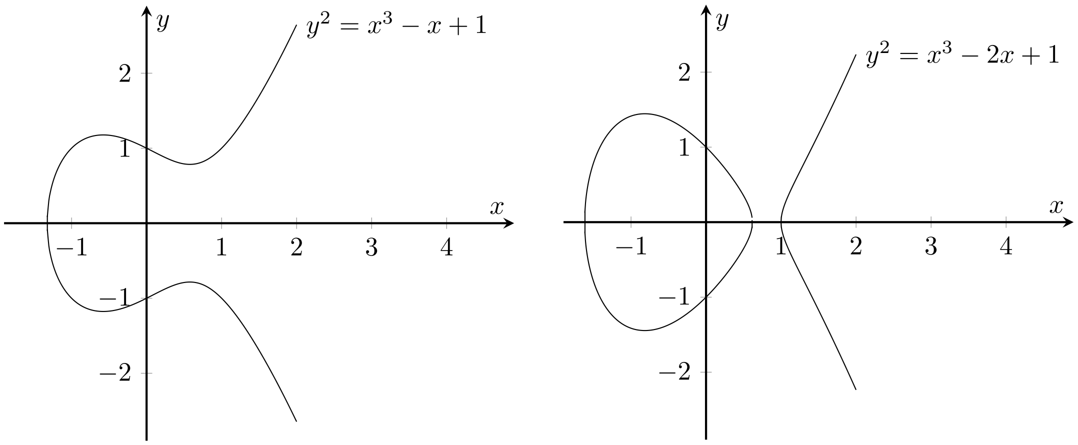

Figure 2.1: Two examples of elliptic curves

in (2.3). Applying another coordinate change

$$(x, y) \mapsto \left(\frac{x}{(PQR)^2}, \frac{y}{(PQR)^3} \right)$$

and multiplying each side by $(PQR)^6$, we find

$$y^2 = x^3 + pQR(PQR)x^2 + qPR(PQR)^3x + rPQ(PQR)^5.$$

This shows any elliptic curve over $\mathbb{Q}$ can be represented by an equation

$$y^2 = x^3 + Ax^2 + Bx + C, \quad A, B, C \in \mathbb{Z}. \tag{2.4}$$

Two examples of elliptic curves over $\mathbb{Q}$ are shown in Figure 2.1, along with appropriate affine Weierstrass equations.

2.3 The group of $\mathbb{K}$-rational points

Let $E/\mathbb{K}$ be an elliptic curve over a field $\mathbb{K}$. It will be convenient to assume $\mathrm{char}(\mathbb{K}) \neq 2$, so that we may assume $E/\mathbb{K}$ is given by an equation of the form (2.3). This simplification will not cause problems, since in the method we will explain in Section 1.2 we can simply choose primes in a manner that avoids this situation. We will denote the group of $\mathbb{K}$-rational points (points with coordinates in $\mathbb{K}$) by $E(\mathbb{K})$. Note this includes the base point $\mathcal{O}$, which we will define to be its unit element. The group law '+' acts on $E(\mathbb{K})$ as follows. Take $P, Q \in E(\mathbb{K})$, and draw a line L_1 through them. If $P = Q$, take this line to be the line tangent to E at P. By a special case of Bezout's theorem, there is a unique third intersection point between L_1 and E. Section A.4 of (Silverman & Tate, 2015) supplies a proof of this theorem (Theorem A.1 in this section). We consider P to be a double intersection point if $P = Q$. This third intersection point is denoted $P * Q$ (note $P * Q = Q$ if L_1 happens to be tangent to E at Q). We now draw a second line L_2 through $\mathcal{O}$ and $P * Q$. Again by Bezout's theorem, there is a third intersection between L_2 and E, which we will define to be $P + Q$. This construction is depicted in Figure 2.2.

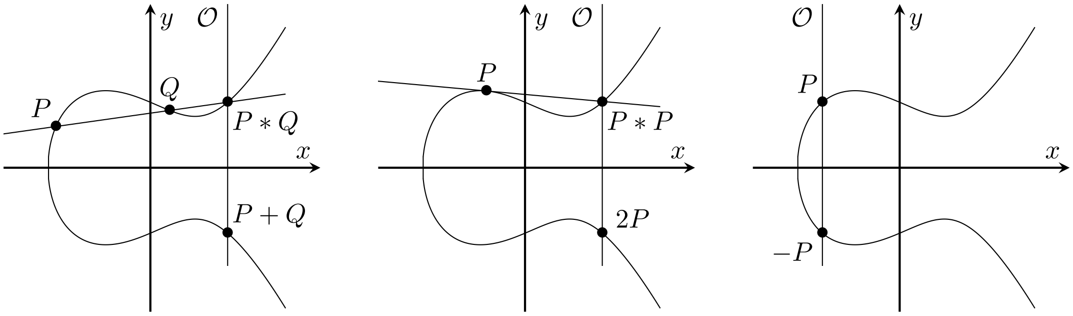

Figure 2.2: The group law on $E(\mathbb{Q})$

Remark that the line through $P * Q$ and $\mathcal{O}$ is necessarily vertical, by the definition of $\mathcal{O}$. Because $\mathrm{char}(\mathbb{K}) \neq 2$, the affine part of E can be represented by an equation of the form (2.3), which is symmetric about the x-axis. We therefore obtain $P + Q$ in the above construction by negating the y-coordinate of $P * Q$. We will adopt the convention that $\mathbb{P}^1$ intersects E at $\mathcal{O}$ with multiplicity 3, and that the line tangent to E at $\mathcal{O}$ is $\mathbb{P}^1$. This ensures $\mathcal{O}$ acts as the identity element of $E(\mathbb{K})$. From this, we derive that the negative (or inverse) of a point $P = (x, y) \in E(\mathbb{K}) \setminus \{\mathcal{O}\}$ is simply $-P = (x, -y)$, as elliptic curves given by an equation (2.3) are symmetric about the x-axis. Recall that we can write P in affine coordinates since the only point not in $\mathbb{A}^2$ is $\mathcal{O}$, which is its own inverse.

It remains to be verified that $P + Q$ indeed lies in $E(\mathbb{K})$. Since this is trivial if P or Q equals $\mathcal{O}$, suppose the contrary. Write $P = (x_1, y_1)$, $Q = (x_2, y_2)$ and $P * Q = (x_3, y_3)$. Let the line L_1 through P, Q and $P * Q$ be given by

$$L_1 : y = \lambda x + \nu,$$

where necessarily $\lambda, \nu \in \mathbb{K}$. Let the affine part of E be given by

$$y^2 = x^3 + ax^2 + bx + c, \quad a, b, c \in \mathbb{K}.$$

The x-coordinates of the intersection points between L_1 and E are the solutions to

$$(\lambda x + \nu)^2 = x^3 + ax^2 + bx + c,$$

that is, the zeros of a third degree polynomial $F(x)$ with coefficients in $\mathbb{K}$. Suppose now that $x_3 \notin \mathbb{K}$, then in

$$F(x) = (x - x_1)(x - x_2)(x - x_3) = x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3,$$

the coefficient of x^2 is not an element of $\mathbb{K}$, a clear contradiction. So, $x_3 \in \mathbb{K}$. It follows $y_3 \in \mathbb{K}$ as well, since

$$y_3 = \lambda x_3 + \nu.$$

We conclude $P + Q = (x_3, -y_3)$ must be a $\mathbb{K}$-rational point.

An amazing result on $E(\mathbb{Q})$ is Mordell's theorem, credited to Louis J. Mordell (1888 – 1972).

Theorem 1 (Mordell)**.** *If E is an elliptic curve over $\mathbb{Q}$, then $E(\mathbb{Q})$ is a finitely generated group.*

Although interesting, a proof of this theorem would be far to lengthy for this thesis. A detailed treatment can be found in Section VIII.4 of (Silverman, 2009). Mordell's theorem is a special case of the famous Mordell-Weil theorem, which states $E(\mathbb{K})$ is finitely generated for any number field $\mathbb{K}$ (actually, this holds more generally for $A(\mathbb{K})$, where A is an abelian variety over a number field $\mathbb{K}$, but this is beyond the scope of this thesis). Using this together with the fact that $E(\mathbb{Q})$ is abelian, the fundamental theorem of finitely generated abelian groups implies that

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times T, \tag{2.5}$$

where $T := E(\mathbb{Q})_{\text{tor}}$ is the torsion subgroup of $E(\mathbb{Q})$. As noted before, the nonnegative integer r is the *rank* of E. Note that for $r = 0$, the group $E(\mathbb{Q})$ has finite order, implying there are only finitely many rational points satisfying its affine Weierstrass equation.

Note that (2.5) implies that

$$E(\mathbb{Q})/T \cong \mathbb{Z}^r.$$

This allows us to define the notion of *independence* of points $P_1, \dots, P_n \in E(\mathbb{Q})$, that is, the points P_i are independent if for any $Q \in T$,

$$c_1 P_1 + \ldots + c_n P_n = Q \quad \text{implies} \quad c_1 = \cdots = c_n = 0 \quad (c_i \in \mathbb{Z}).$$

An important observation to make is the following. By Mazur's theorem, c.f Theorem 8 in (Mazur, 1977) (the proof of which is a notable triumph credited to Barry C. Mazur), T is isomorphic to one of the following 15 groups:

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} \quad &\text{for} \quad m = 1, 2, \dots, 10, 12, \quad (m \neq 11) \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \quad &\text{for} \quad n = 1, 2, 3, 4. \end{aligned}$$

So, $E(\mathbb{Q})/2E(\mathbb{Q})$ must be isomorphic to one of the groups

$$\begin{aligned} (\mathbb{Z}/2\mathbb{Z})^r \times (\mathbb{Z}/m\mathbb{Z})/2(\mathbb{Z}/m\mathbb{Z}) \quad &\text{for} \quad m = 1, 2, \dots, 10, 12, \\ (\mathbb{Z}/2\mathbb{Z})^r \times (\mathbb{Z}/2\mathbb{Z})/2(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2n\mathbb{Z})/2(\mathbb{Z}/2n\mathbb{Z}) \quad &\text{for} \quad n = 1, 2, 3, 4. \end{aligned}$$

The group $(\mathbb{Z}/k\mathbb{Z})/2(\mathbb{Z}/k\mathbb{Z})$ for a positive integer k can only be trivial or isomorphic to $\mathbb{Z}/2\mathbb{Z}$, that is

$$(\mathbb{Z}/k\mathbb{Z})/2(\mathbb{Z}/k\mathbb{Z}) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{if } k \text{ is even,} \\ 0 & \text{otherwise,} \end{cases}$$

since $\mathbb{Z}/k\mathbb{Z} = 2(\mathbb{Z}/k\mathbb{Z})$ for k odd. So,

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

for some t. Note that $(\mathbb{Z}/2\mathbb{Z})^t$ corresponds to the subgroup $E(\mathbb{Q})[2]$ of elements $P \in E(\mathbb{Q})$ such that $2P = \mathcal{O}$. Consequently, it must be that t equals the number of non-trivial 2-torsion points in $E(\mathbb{Q})$ needed to generate $E(\mathbb{Q})[2]$. Moreover, t is completely determined by the structure of T, i.e.

$$t = \begin{cases} 0 & \text{if} \quad T \cong \mathbb{Z}/m_1\mathbb{Z} \quad \text{for} \quad m_1 = 1, 3, 5, 7, 9, \\ 1 & \text{if} \quad T \cong \mathbb{Z}/m_2\mathbb{Z} \quad \text{for} \quad m_2 = 2, 4, 6, 8, 10, 12, \\ 2 & \text{if} \quad T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \quad \text{for} \quad n = 1, 2, 3, 4. \end{cases}$$

This shows that after factoring $E(\mathbb{Q})$ by doubles, the 2-torsion subgroup persists. It will therefore be necessary to add generators of $E(\mathbb{Q})[2]$ to our list of point $P_1, \dots, P_n \in E(\mathbb{Q})$ when checking their independence, the procedure of which will be explained in Section 4.2.

2.4 Reduction modulo a prime p

Let $\mathbb{K}$ be a field and define $\mathbb{P}^2(\mathbb{K})$ to be the points in $\mathbb{P}^2$ with (homogeneous) coordinates in $\mathbb{K}$. Throughout this subsection, we assume primes p to be odd, so as to avoid having $\mathrm{char}(\mathbb{F}_p) = 2$.

Definition 5 (Normalized coordinate triple)**.** A homogeneous coordinate triple $[A, B, C] \in \mathbb{P}^2(\mathbb{Q})$ is said to be *normalized* if A, B, C are integers with no common factors.

Every point $[a, b, c] \in \mathbb{P}^2(\mathbb{Q})$ can be expressed by a normalized coordinate triple. This is achieved by multiplying out any denominators and by subsequently dividing by any common factors. The resulting triple is unique up to sign.

We are now ready to define reduction of an elliptic curve modulo a prime p, which will be central to the method explained in Section 1.2.

Definition 6. Let p be a prime and let E be an elliptic curve over $\mathbb{Q}$ given by

$$E/\mathbb{Q}: \quad Y^2Z = X^3 + AX^2Z + BXZ^2 + CZ^3, \quad A, B, C \in \mathbb{Z},$$

where A, B and C have no common factors. Let Δ denote its discriminant. Then the *reduction of E modulo p* is given by

$$\tilde{E}/\mathbb{F}_p: \quad Y^2Z = X^3 + \tilde{A}X^2Z + \tilde{B}XZ^2 + \tilde{C}Z^3, \quad \tilde{A}, \tilde{B}, \tilde{C} \in \mathbb{F}_p,$$

where

$$\tilde{A} = A \bmod p, \quad \tilde{B} = B \bmod p, \quad \tilde{C} = C \bmod p.$$

The discriminant of $\tilde{E}/\mathbb{F}_p$ is $\tilde{\Delta} = \Delta \bmod p$.

Note that $\tilde{E}/\mathbb{F}_p$ in the above definition will be an elliptic curve if and only if $\tilde{\Delta} \neq 0$, i.e. if and only if $p \nmid \Delta$. We can also reduce points in $\mathbb{P}^2(\mathbb{Q})$ to points in $\mathbb{P}^2(\mathbb{F}_p)$, and if $\tilde{E}$ is an elliptic curve, this moreover defines a map from $E(\mathbb{Q})$ to $\tilde{E}(\mathbb{F}_p)$.

Definition 7. Let p be a prime and let $P \in \mathbb{P}^2(\mathbb{Q})$ be given by a normalized homogeneous coordinate triple $[A, B, C]$. The *reduction of P modulo p* is

$$\tilde{P} := [\tilde{A}, \tilde{B}, \tilde{C}], \quad \text{where} \quad \tilde{A} = A \bmod p, \quad \tilde{B} = B \bmod p, \quad \tilde{C} = C \bmod p.$$

The *reduction modulo p map* is the map $\mathbb{P}^2(\mathbb{Q}) \to \mathbb{P}^2(\mathbb{F}_p)$ that sends P to $\tilde{P}$ as above.

For an elliptic curve E over $\mathbb{Q}$, assuming $\tilde{E}$ is an elliptic curve, restricting the reduction modulo p map to $E(\mathbb{Q})$ now gives the desired map $E(\mathbb{Q}) \to \tilde{E}(\mathbb{F}_p)$. The reason that $P \in E(\mathbb{Q})$ gets mapped to $\tilde{P} \in \tilde{E}(\mathbb{F}_p)$, is because we assumed the normalized coordinate triple representing P to have no common factors. This way, no prime p can divide all coordinates simultaneously, ensuring $\tilde{P} \neq [0, 0, 0]$. Moreover, E is represented by some equation

$$Y^2Z - X^3 - AX^2Z - BXZ^2 - CZ^3 = 0, \quad A, B, C \in \mathbb{Z}. \tag{2.6}$$

The fact that $P = [U, V, W] \in E(\mathbb{Q})$ (as a normalized coordinate triple) is a solution to (2.6) implies that $\tilde{P} = [\tilde{U}, \tilde{V}, \tilde{W}]$ is a solution to

$$Y^2Z - X^3 - \tilde{A}X^2Z - \tilde{B}XZ^2 - \tilde{C}Z^3 = 0, \quad A, B, C \in \mathbb{F}_p.$$

This shows $\tilde{P} \in \tilde{E}(\mathbb{F}_p)$. There is one important result we will need later on.

Proposition 1. *Let E be an elliptic curve over $\mathbb{Q}$, and let $\tilde{E}$ be the reduction of E modulo p for a prime p. Assume $\tilde{E}$ is an elliptic curve. The reduction modulo p map restricted to $E(\mathbb{Q})$ is a homomorphism from $E(\mathbb{Q})$ to $\tilde{E}(\mathbb{F}_p)$.*

Proof. We will not give complete proof here (in particular, we assume Proposition A.5 in (Silverman & Tate, 2015)). The details can be found in Section A.5 in (Silverman & Tate, 2015) (from Proposition A.5 until the end of the section).

Let a line L be given by

$$L : ay = bx + c, \quad a, b, c \in \mathbb{Q}.$$

Multiplying out any denominators and dividing any common factors, L can be written as

$$L : Ay = Bx + C, \quad A, B, C \in \mathbb{Q} \text{ having no common factors.}$$

If $A = B = 0$, then $C \neq 0$ and in this case L is the line at infinity. Define the reduction of L modulo p, denoted $\tilde{L}$, by

$$\tilde{L} : \tilde{A}y = \tilde{B}x + \tilde{C}, \quad A, B, C \in \mathbb{F}_p.$$

Proposition A.5 in (Silverman & Tate, 2015) tells us that if

$$E \cap L = \{P, Q, R\},$$

listing multiple intersections a number of times equal to their multiplicity, then

$$\tilde{E} \cap \tilde{\mathcal{L}} = \{\tilde{P}, \tilde{Q}, \tilde{R}\}.$$

Here $\tilde{P}$ is the image of $P \in E(\mathbb{Q})$ by the reduction modulo p map.

Now, suppose $P, Q \in E(\mathbb{Q})$. Then the line L_1 through P, Q (recall, tangent to E at P if $P = Q$) intersects E in a third point $P * Q$. So,

$$E \cap L_1 = \{P, Q, P * Q\}.$$

A second line L_2 through $\mathcal{O}$ and $P * Q$ intersects E in a third point $P + Q$, that is

$$E \cap L_2 = \{\mathcal{O}, P * Q, P + Q\}.$$

The line through $\tilde{P}$ and $\tilde{Q}$ is $\tilde{L}_1$, and therefore

$$\tilde{E} \cap \tilde{L}_1 = \{\tilde{P}, \tilde{Q}, \widetilde{P * Q}\}$$

tells us the third intersection point with $\tilde{E}$ is $\widetilde{P * Q}$. Similarly, the line through $\tilde{O}$ and $\widetilde{P * Q}$ intersects $\tilde{E}$ a third time in $\widetilde{P + Q}$, which completes the proof.

□

3 Canonical heights

The method described in Section 1.2 is entirely based on (Cremona, 2002) (a paper by John E. Cremona, a leading figure in the field of computations involving elliptic curves) and (Silverman, 2000) (a paper by Joseph H. Silverman, a leading figure on arithmetic of elliptic curves). According to Cremona, the method was described to him by Armand Brumer

Another well-known and rather straightforward way to prove independence of points in $E(\mathbb{Q})/T$ (again $T := E(\mathbb{Q})_{\text{tor}}$) is by calculating the determinant of the height pairing matrix. We will briefly explain how the method works, but we will refer the reader to Section 8.5 of (Washington, 2008) for a detailed explanation and proofs. First, we need some definitions.

Definition 8. For a rational number $x = a/b$ written in lowest terms, the *height* $H(x)$ is defined as

$$H(x) = \max\{|a|, |b|\}.$$

Definition 9. For an elliptic curve E over $\mathbb{Q}$, the *height* $H(P)$ of a point $P = (x, y) \in E(\mathbb{Q})$ is defined as

$$H(P) = H(x).$$

Conventionally, $H(\mathcal{O}) = 1$.

Let $h(P) := \log H(P)$ and define a function $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$ by

$$\hat{h}(P) = \frac{1}{2} \lim_{n\to\infty} \frac{1}{4^n} h(2^n P) \quad \text{for} \quad P \in E(\mathbb{Q}).$$

This is the *canonical height function*. The limit in the right-hand side exists, c.f the proof of Theorem 8.18 in (Washington, 2008). Subsequently, we can establish the *height pairing*

$$\langle P, Q\rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$$

for rational points P, Q on E. Now for rational points $P_1, \ldots, P_n$ on E, if we let M be the $n \times n$ matrix with $\langle P_i, P_j\rangle$ as its i, j-th value, then $P_1, \ldots, P_n$ are independent (recall independence is defined modulo the torsion subgroup of $E(\mathbb{Q})$) if and only if

$$\det M \neq 0,$$

c.f. Theorem 8.25 in (Washington, 2008). Cremona implemented this method in the computer algebra system SAGE; the code can be found in (Cremona, 2008). We can use M to find dependence relations as well, should the points P_i be dependent. A major deficit of this method is that we can only prove numerically that some linear combination of rational points equates to a torsion point, as we can only approximate $\hat{h}(P)$ at a given point P. This is discussed in more detail in Appendix F of (Silverman, 2000). Apart from this shortcoming, proving independence using canonical heights definitely has the advantage of being much more straightforward than the method discussed in this thesis.

Nevertheless, using the homomorphism (1.2) is in a sense much 'cleaner'. The algorithm we will use is explained in even more detail in Appendices D and G of (Silverman, 2000). An implementation is included by default in SAGE, but to my knowledge, no implementation exists for PARI. As PARI is still widely appreciated for its speed, a PARI program is included in the appendix of this thesis.

4 Method

4.1 Constructing the homomorphism

Let the elliptic curve $E/\mathbb{Q}$ be given by

$$y^2 = f(x) = x^3 + Ax^2 + Bx + C, \quad \text{for} \quad A, B, C \in \mathbb{Z}, \tag{4.1}$$

where $f(x)$ (and hence E) has a nonzero discriminant

$$\Delta := A^2B^2 + 18ABC - 4B^3 - 4A^3C - 27C^2.$$

Note the discriminant of E, as defined in Definition 4, is simply -16Δ. We will refer to primes not dividing 6Δ as "good" primes. This will ensure that the characteristic of the field $\mathbb{F}_q$ for a good prime q is not 2 or 3, which would unnecessarily make matters more complicated. It also implies that no prime different from 2 or 3 divides Δ, ensuring the reduction of E modulo p yields an elliptic curve. Moreover, we assume the model (4.1) is minimal at all odd primes. This means for any other equation of the form (4.1) with discriminant Δ' describing this curve, the p-adic valuation of Δ' is larger than that of Δ for each odd prime p. For p prime, the p-adic valuation of an integer a is

$$v_p(a) = \begin{cases} n & \text{if } a = r \cdot p^n \quad (r \in \mathbb{Z} \text{ nonzero, } n \in \mathbb{Z} \text{ nonnegative and } p \nmid r), \\ \infty & \text{if } a = 0. \end{cases}$$

We will require the map $\psi : \mathbb{F}_p^\times \to \mathbb{Z}/2\mathbb{Z}$ defined below.

Definition 10. For an odd prime p, the *Legendre symbol* $\left(\frac{\cdot}{p}\right) : \mathbb{Z} \to \{-1, 0, 1\}$ is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } \exists b \in \mathbb{F}_p^\times : \ b^2 = a \bmod p \neq 0, \\ -1 & \text{if } \nexists b \in \mathbb{F}_p^\times : \ b^2 = a \bmod p \neq 0, \\ 0 & \text{if } a \bmod p = 0, \end{cases} \qquad (a \in \mathbb{Z}).$$

Let $\psi : \mathbb{F}_p^\times \to \mathbb{Z}/2\mathbb{Z}$ be the homomorphism such that $\left(\frac{a}{p}\right) = (-1)^{\psi(a)}$ for $a \in \mathbb{F}_p^\times$, that is

$$\psi(a) = \begin{cases} 0 & \text{if } \exists b \in \mathbb{F}_p^\times : \ y^2 = a, \\ 1 & \text{otherwise,} \end{cases} \qquad (a \in \mathbb{F}_p^\times).$$

The fact that ψ is a homomorphism will follow from Proposition 2. Define $\tilde{f}$ to be the reduction of f modulo a prime p, that is

$$\tilde{f}(x) = x^3 + \tilde{A}x^2 + \tilde{B}x + \tilde{C},$$

where a tilde on a coefficients of $\tilde{f}$ represents its residue modulo p. For a good prime p, we will write $k_p = 0$, 1 or 2 if the number of roots $x \in \mathbb{F}_p$ of $\tilde{f}(x)$ is 0, 1 or 3, respectively. Remark that k_p equals the number of generators of the subgroup $E(\mathbb{F}_p)[2]$ of elements $P \in \tilde{E}(\mathbb{F}_p)$ such that $2P = \tilde{\mathcal{O}}$. We need not consider the primes p for which $k_p = 0$. Namely, this would imply that 2 does not divide the number of elements of $\tilde{E}(\mathbb{F}_p)$ (as there are no points in $\tilde{E}(\mathbb{F}_p)$ of order 2), and therefore $\tilde{E}(\mathbb{F}_p) = 2\tilde{E}(\mathbb{F}_p)$. As the map to be constructed in the next subsections factors through $\tilde{E}(\mathbb{F}_p)/2\tilde{E}(\mathbb{F}_p)$, this would not be particularly useful. Although it would be easier to consider only primes p for which $k_p = 1$, for some elliptic curves the are no such primes. This happens if Δ is a perfect square, and so we will need to consider both $k_p = 1, 2$. For $f(x)$ irreducible, the density of primes for which $k_p \neq 0$ is at least $\frac{1}{3}$, c.f. Section 2 in (Cremona, 2008) (as a consequence of the Chebotarev density theorem, but this is beyond the scope of this thesis).

Case one: A unique root in $\mathbb{F}_p$

Let p be a good prime for which $k_p = 1$, and let θ_p be the unique root of $\tilde{f}(x)$ in $\mathbb{F}_p$. The following result will be important in the proof of Proposition 3. We let $(\mathbb{F}_p^\times)^2$ be the subgroup of squares of $\mathbb{F}_p^\times$.

Proposition 2. *Let p be prime and let $a, b \in \mathbb{F}_p^\times \setminus (\mathbb{F}_p^\times)^2$. Then ab is a quadratic residual, that is $ab \in (\mathbb{F}_p^\times)^2$.*

Proof. This result trivially holds for $p = 2, 3$, as in this case $\mathbb{F}_p^\times \setminus (\mathbb{F}_p^\times)^2$ is empty. Therefore, from now on we consider only $p > 3$.

The multiplicative group $\mathbb{F}_p^\times$ of the finite field $\mathbb{F}_p$ is cyclic. Hence, there exists some generator $g \in \mathbb{F}_p^\times$ such that each $a \in \mathbb{F}_p^\times$ can be expressed as $a = g^k$ for some integer k. Naturally, a is a quadratic residual if and only if k is even. This shows half of the elements of $\mathbb{F}_p^\times$ are quadratic residuals, because the order of $\mathbb{F}_p^\times$ is even. Hence,

$$[\mathbb{F}_p^\times : (\mathbb{F}_p^\times)^2] = 2.$$

Take any $a, b \in \mathbb{F}_p^\times \setminus (\mathbb{F}_p^\times)^2$. We conclude that

$$\mathbb{F}_p^\times / (\mathbb{F}_p^\times)^2 = \left\{ (\mathbb{F}_p^\times)^2, a \cdot (\mathbb{F}_p^\times)^2 \right\}.$$

So,

$$a \cdot (\mathbb{F}_p^\times)^2 = b \cdot (\mathbb{F}_p^\times)^2,$$

and therefore

$$ab \cdot (\mathbb{F}_p^\times)^2 = \left(a \cdot (\mathbb{F}_p^\times)^2\right) \cdot \left(b \cdot (\mathbb{F}_p^\times)^2\right) = \left(a \cdot (\mathbb{F}_p^\times)^2\right) \cdot \left(a \cdot (\mathbb{F}_p^\times)^2\right) = a^2 \cdot (\mathbb{F}_p^\times)^2 = (\mathbb{F}_p^\times)^2.$$

Henceforth, $ab \in (\mathbb{F}_p^\times)^2$. □

We are now ready to establish an important component of our homomorphism. Let $\tilde{E}$ be the elliptic curve obtained by reducing E modulo p, and denote the unit element of $\tilde{E}(\mathbb{F}_p)$ by $\tilde{\mathcal{O}}$.

Proposition 3. *For a good prime p with $k_p = 1$, the map $\overline{\varepsilon}_p : \tilde{E}(\mathbb{F}_p) \to \mathbb{Z}/2\mathbb{Z}$ defined by*

$$\overline{\varepsilon}_p(P) = \begin{cases} \psi(x - \theta_p) & \textit{if } \tilde{\mathcal{O}} \neq P = (x, y) \textit{ and } x \neq \theta_p, \\ \psi(f'(\theta_p)) & \textit{if } \tilde{\mathcal{O}} \neq P = (x, y) = (\theta_p, 0), \\ 0 & \textit{if } P = \tilde{\mathcal{O}}, \end{cases}$$

is a homomorphism.

Proof. First of all, for any $P \in \tilde{E}(\mathbb{F}_p)$,

$$\overline{\varepsilon}_p(P + \tilde{\mathcal{O}}) = \overline{\varepsilon}_p(P) = \overline{\varepsilon}_p(P) + 0 = \overline{\varepsilon}_p(P) + \overline{\varepsilon}(\tilde{\mathcal{O}}),$$

and since $\overline{\varepsilon}_p(P) = \overline{\varepsilon}_p(-P)$,

$$\overline{\varepsilon}_p(P + (-P)) = \overline{\varepsilon}_p(\tilde{\mathcal{O}}) = 0 = 2\overline{\varepsilon}_p(P) = \overline{\varepsilon}_p(P) + \overline{\varepsilon}(-P),$$

because ε_p maps into $\mathbb{Z}/2\mathbb{Z}$. We can therefore restrict our attention to combinations $P, Q \in \tilde{E}(\mathbb{F}_p)$ not including $\tilde{\mathcal{O}}$ where P and Q are not each others inverse.

Let $\tilde{E}'$ represent the elliptic curve over $\mathbb{F}_p$ with base point $\tilde{\mathcal{O}}'$ obtained by shifting $\tilde{E}$ back by θ_p with respect to the x-axis (and so moving the unique 2-torsion point of $\tilde{E}(\mathbb{F}_p)$ to the origin). Specifically, we map points $[X, Y, Z] \in \tilde{E}$ to $\tilde{E}'$ according to

$$[X, Y, Z] \mapsto [X - \theta_p Z, Y, Z].$$

Then, $\tilde{E}'$ is given by an affine equation

$$y^2 = g(x) = x^3 + A'x^2 + B'x.$$

for some $A', B' \in \mathbb{F}_p$. Note the constant term on the right-hand side is zero as a result of the shift by θ_p. Moreover, $f'(\theta_p) = g'(0)$. We will thus define three maps

(i) $$\rho : \tilde{E}(\mathbb{F}_p) \to \tilde{E}'(\mathbb{F}_p) : \begin{cases} (x, y) & \mapsto (x - \theta_p, y), \\ \tilde{\mathcal{O}} & \mapsto \tilde{\mathcal{O}}', \end{cases}$$

(ii) $$\varphi : \tilde{E}'(\mathbb{F}_p) \to (\mathbb{F}_p^\times)/(\mathbb{F}_p^\times)^2 : P \mapsto \begin{cases} x \bmod (\mathbb{F}_p^\times)^2 & \text{if } P = (x, y) \neq (0, 0), \\ g'(0) \bmod (\mathbb{F}_p^\times)^2 & \text{if } P = (0, 0), \\ 1 \bmod (\mathbb{F}_p^\times)^2 & \text{if } P = \tilde{\mathcal{O}}', \end{cases}$$

(iii) $$\mu : (\mathbb{F}_p^\times)/(\mathbb{F}_p^\times)^2 \to \mathbb{Z}/2\mathbb{Z} : x \bmod (\mathbb{F}_p^\times)^2 \mapsto \begin{cases} 1 & \text{if } x \notin (\mathbb{F}_p^\times)^2, \\ 0 & \text{otherwise.} \end{cases}$$

This way $\varepsilon_p = \mu \circ \varphi \circ \rho$. We will show that μ, φ and ρ are homomorphisms.

(i) Clearly ρ is an isomorphism (and hence a homomorphism) since it is a change of coordinates.

(ii) Let $P = (x, y) \in \tilde{E}'(\mathbb{F}_p)$ be different from $\tilde{\mathcal{O}}'$ (since for $\tilde{\mathcal{O}}'$ the following holds trivially). Note that φ maps negatives to inverses:

$$\begin{aligned}\varphi(-P) = \varphi(x, -y) &= x \bmod (\mathbb{F}_p^\times)^2 \\ &= x^{-1}x^2 \bmod (\mathbb{F}_p^\times)^2 \\ &= x^{-1} \bmod (\mathbb{F}_p^\times)^2 \\ &= (\varphi(P))^{-1},\end{aligned}$$

if $P \neq (0, 0)$. Otherwise,

$$\begin{aligned}\varphi(-P) = \varphi(0, 0) &= f'(0) \bmod (\mathbb{F}_p^\times)^2 \\ &= (f'(0))^{-1}(f'(0))^2 \bmod (\mathbb{F}_p^\times)^2 \\ &= (f'(0))^{-1} \bmod (\mathbb{F}_p^\times)^2 \\ &= (\varphi(P))^{-1}.\end{aligned}$$

Hence, φ is a homomorphism if we now show that for $P, Q, R \in \tilde{E}'(\mathbb{F}_p)$

$$P + Q + R = \tilde{\mathcal{O}}'$$

implies

$$\varphi(P)\varphi(Q)\varphi(R) = 1 \bmod (\mathbb{F}_p^\times)^2.$$

To see this, note that R must equal $-(P + Q)$. Consequently,

$$\varphi(P)\varphi(Q)\varphi(-(P + Q)) = 1 \bmod (\mathbb{F}_p^\times)^2,$$

and so

$$\varphi(P)\varphi(Q) = [\varphi(-(P + Q))]^{-1} = \varphi(P + Q).$$

So, suppose we have $P, Q, R \in \tilde{E}'(\mathbb{F}_p) \setminus \{\tilde{\mathcal{O}}'\}$ such that $P + Q + R = \tilde{\mathcal{O}}'$. This can only happen if P, Q and R lie on a line L.

Let us first treat the case where P, Q, R are all different from $(0, 0)$. Let the line L be given by the equation $y = \lambda x + \nu$ for some $\lambda, \nu \in \mathbb{F}_p$. Since none of P, Q, R is equal to $(0, 0)$, we find that ν is nonzero (otherwise L would intersect the curve at the origin) and so, $\nu \in \mathbb{F}_p^\times$. The x-coordinates of the intersections of this line and the elliptic curve (i.e. the points P, Q, R) must be the solutions in x of

$$x^3 + A'x^2 + B'x = y^2 = (\lambda x + \nu)^2 = \lambda^2 x^2 + 2\lambda\nu x + \nu^2,$$

or equivalently, of

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

Let x_1, x_2, x_3 be the x-coordinates of P, Q, R, respectively. By solving

$$(x - x_1)(x - x_2)(x - x_3) = x^3 + (A' - \lambda^2)x^2 + (B' - 2\lambda\nu)x - \nu^2,$$

for x_1, x_2, x_3, we easily acquire

$$x_1 + x_2 + x_3 = \lambda^2 - A', \quad x_1x_2 + x_1x_3 + x_2x_3 = B' - \lambda\nu, \quad x_1x_2x_3 = \nu^2.$$

This shows that

$$\varphi(P)\varphi(Q)\varphi(R) = x_1x_2x_3 \bmod (\mathbb{F}_p^\times)^2 = \nu^2 \bmod (\mathbb{F}_p^\times)^2 = 1 \bmod (\mathbb{F}_p^\times)^2.$$

Let us now treat the case where one of P, Q, R equals $(0, 0)$. This can happen for at most one of the three points, as otherwise another point must equal $\tilde{\mathcal{O}}'$ since E is assumed to have good reduction modulo p, a contradiction. Without loss of generality, assume that $R = (0, 0)$. Now the line L must be given by some equation $y = \lambda x$ (the line must go through the origin R) with $\lambda, \in \mathbb{F}_p^\times$. Let again $x_1, x_2, x_3 = 0$ be the x-coordinates of P, Q, R, respectively. This time, the x-coordinates of the intersections of this line and the elliptic curve (i.e. the points P, Q, R) must be the solutions of

$$x^3 + A'x^2 + B'x = \lambda^2x^2,$$

or equivalently, of

$$x^3 + (A' - \lambda^2)x^2 + B'x = 0.$$

As before, this yields

$$B' = x_1x_2 + x_1x_3 + x_2x_3 = x_1x_2$$

since $x_3 = 0$. Note furthermore that

$$g'(0) = 3x^2 + 2A'x + B'\big|_{x=0} = B',$$

so we find

$$\varphi(R) = g'(0) \bmod (\mathbb{F}_p^\times)^2 = B' \bmod (\mathbb{F}_p^\times)^2 = x_1x_2 \bmod (\mathbb{F}_p^\times)^2 = \varphi(P)\varphi(Q).$$

Because $R = -R = P + Q$,

$$\varphi(P + Q) = \varphi(-R) = \varphi(R) = \varphi(P)\varphi(Q),$$

showing φ is a homomorphism.

(iii) Only for the remainder of this proof we shall denote $x \bmod (\mathbb{F}_p^\times)^2$ by $\overline{x}$ for $x \in \mathbb{F}_p^\times$. Note that by the proof of Proposition 2, the group $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$ has order 2. So, letting $a \in \mathbb{F}_p^\times \setminus (\mathbb{F}_p^\times)^2$ allows us to write

$$\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 = \left\{\overline{1}, \overline{a}\right\}.$$

Now it is straightforward to verify

$$\begin{aligned}\mu\left(\overline{1} \cdot \overline{1}\right) &= 0 = 0 + 0 = \mu\left(\overline{1}\right) + \mu\left(\overline{1}\right),\\ \mu\left(\overline{1} \cdot \overline{a}\right) &= \mu\left(\overline{a}\right) + 0 = \mu\left(\overline{a}\right) + \mu\left(\overline{1}\right),\\ \mu\left(\overline{a} \cdot \overline{a}\right) &= 0 = 1 + 1 = \mu\left(\overline{a}\right) + \mu\left(\overline{a}\right),\end{aligned}$$

since $\overline{a} \cdot \overline{a} = \overline{1}$ by Proposition 2 and μ maps into $\mathbb{Z}/2\mathbb{Z}$. Because both $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$ and $\mathbb{Z}/2Z$ are abelian, μ is hereby a homomorphism.

The proof is complete since a composition of homomorphisms is a homomorphism. □

To derive the important result that $E(\mathbb{F}_p)/2E(\mathbb{F}_p) \cong \mathbb{Z}/2\mathbb{Z}$, we need to show the following.

Proposition 4. *For a good prime p with $k_p = 1$, the homomorphism $\overline{\varepsilon}_p$ in Proposition 3 is surjective, and its kernel is precisely $2\tilde{E}(\mathbb{F}_p)$.*

Proof. If we fix $P \in 2\tilde{E}(\mathbb{F}_p)$, then there exists $Q \in \tilde{E}(\mathbb{F}_p)$ so that $2Q = P$. Because $\overline{\varepsilon}_p$ is a homomorphism by Proposition 3,

$$\overline{\varepsilon}_p(P) = \overline{\varepsilon}_p(2Q) = 2\overline{\varepsilon}_p(Q) = 0.$$

Hence, $2\tilde{E}(\mathbb{F}_p) \subset \ker \overline{\varepsilon}_p$.

For the other inclusion, take $P \in \ker \overline{\varepsilon}_p$ and let the maps ρ, φ and μ and the elliptic curve $\tilde{E}'$ be as in the proof of Proposition 3. If $P = \tilde{\mathcal{O}}$, then trivially $P \in 2\tilde{E}(\mathbb{F}_p)$. To prove $P \in 2\tilde{E}(\mathbb{F}_p)$ if $P \neq \tilde{\mathcal{O}}$ it now suffices to show $P' = \rho(P)$ is in $2\tilde{E}'(\mathbb{F}_p)$, since $P' \in \ker \varphi$. Recall that E' is given by

$$y^2 = g(x) = x^3 + A'x^2 + B'x, \quad A', B' \in \mathbb{F}_p.$$

Let the elliptic curve $\overline{E'}$ over $\mathbb{F}_p$ be given by

$$y^2 = x^3 + \overline{A'}x^2 + \overline{B'}x, \quad \overline{A'}, \overline{B'} \in \mathbb{F}_p,$$

where

$$\begin{aligned} \overline{A'} &= -2A', \\ \overline{B'} &= (A')^2 - 4B'. \end{aligned}$$

Denote be the unit element of $\overline{E'}(\mathbb{F}_p)$ by $\overline{\mathcal{O}'}$. Note that $\tilde{E}'(\mathbb{F}_p)$ and $\overline{E'}(\mathbb{F}_p)$ a point of order 2, namely $T = (0,0)$. Define the maps

$$\Phi : \tilde{E}' \to \overline{E'} : P' \mapsto \begin{cases} \left(y^2x^{-2}, y(x^2 - B')x^{-2}\right) & \text{if } P' = (x,y) \neq \mathcal{O}', T, \\ \overline{\mathcal{O}'} & \text{if } P' = \tilde{\mathcal{O}}', T, \end{cases}$$

$$\Psi : \overline{E'} \to \tilde{E}' : \overline{P'} \mapsto \begin{cases} \left(\overline{y}^2\overline{x}^{-2}, \overline{y}(\overline{x}^2 - \overline{B'})\overline{x}^{-2}\right) & \text{if } \overline{P'} = (\overline{x},\overline{y}) \neq \overline{\mathcal{O}'}, T, \\ \tilde{\mathcal{O}}' & \text{if } \overline{P'} = \overline{\mathcal{O}'}, T. \end{cases}$$

The following argument is heavily based on Proposition 3.7 and the succeeding discussion in (Silverman & Tate, 2015). Part (c) of Proposition 3.7 shows

$$\Psi \circ \Phi : \tilde{E}' \to \tilde{E}'$$

is the multiplication-by-two map (actually, the proposition only shows this for elliptic curves over the rationals, but the proof is completely analogous if we consider an elliptic curve over $\mathbb{F}_p$). So,

$$(\Psi \circ \Phi)(\tilde{E}'(\mathbb{F}_p)) = 2\tilde{E}'(\mathbb{F}_p).$$

Suppose now that $\overline{P} = (\overline{x}, \overline{y})$ with $\overline{x} \neq 0$ lies in $\Phi(E'(\mathbb{F}_p))$ Then there must exist some $P = (x, y) \in E'(\mathbb{F}_p)$ such that $\overline{x} = y^2 x^{-2} \in (\mathbb{F}_p^\times)^2$. Conversely, if $\overline{x} = \overline{w}^2$ for some $w \in \mathbb{F}_p^\times$, then the points

$$\left(\tfrac{1}{2}\left(\overline{w}^2 - A' + \overline{y} \cdot \overline{w}^{-1}\right), \tfrac{1}{2}\overline{w}\left(\overline{w}^2 - A' + \overline{y} \cdot \overline{w}^{-1}\right)\right)$$

and

$$\left(\tfrac{1}{2}\left(\overline{w}^2 - A' - \overline{y} \cdot \overline{w}^{-1}\right), -\tfrac{1}{2}\overline{w}\left(\overline{w}^2 - A' - \overline{y} \cdot \overline{w}^{-1}\right)\right)$$

lie on $E'(\mathbb{F}_p)$ and are mapped to $\overline{P}$ by Φ, so $\overline{P} \in \Phi(E'(\mathbb{F}_p))$. Recall $1/2 = 2^{-1}$ is defined since p is good. As such, for $\overline{P'} = (\overline{x}, \overline{y}) \in \overline{E'}(\mathbb{F}_p)$ with $\overline{x} \neq 0$,

$$\overline{P'} \in \Phi(\tilde{E}'(\mathbb{F}_p)) \quad \text{if and only if} \quad \overline{x} \in (\mathbb{F}_p^\times)^2.$$

If we now define another elliptic curve $\overline{\overline{E'}}/\mathbb{F}_p$, with base point $\overline{\overline{\mathcal{O}'}} = \mathcal{O}'$, by

$$y^2 = x^3 + \overline{A'}x^2 + \overline{B'}x, \quad \overline{A'}, \overline{B'} \in \mathbb{F}_p,$$

where

$$\begin{aligned} \overline{\overline{A'}} &= -2\overline{A'} = 4A', \\ \overline{\overline{B'}} &= \overline{A'}^2 - 4\overline{B'} = 16B', \end{aligned}$$

we see E' and $\overline{\overline{E'}}$ are isomorphic by the coordinate change

$$\overline{\overline{E'}} \to E' : \begin{array}{rl} (x, y) & \mapsto (4x, 8y), \\ \overline{\overline{\mathcal{O}'}} & \mapsto \mathcal{O}'. \end{array}$$

Applying the previous result to $\overline{E'}$ and $\overline{\overline{E'}}$, for $\overline{\overline{P'}} = (\overline{\overline{x}}, \overline{\overline{y}}) \in \overline{\overline{E'}}(\mathbb{F}_p)$ with $\overline{\overline{x}} \neq 0$,

$$\overline{\overline{P'}} \in \Psi(\overline{E'}(\mathbb{F}_p)) \quad \text{if and only if} \quad \overline{\overline{x}} \in (\mathbb{F}_p^\times)^2.$$

We will now show that

$$P' \in \Psi(\Phi(\tilde{E}'(\mathbb{F}_p))) = 2\tilde{E}'(\mathbb{F}_p),$$

to complete the proof. Let us first consider the case where $P' = (x, y) \neq (0, 0)$. Then $P' \in \ker \varphi$ implies $x = w^2 \in (\mathbb{F}_p^\times)^2$ for some $w \in \mathbb{F}_p^\times$. Note that P' corresponds to the point

$$\overline{\overline{P'}} = \left(\tfrac{1}{4}w^2, \tfrac{1}{8}y\right) \in \overline{\overline{E'}}(\mathbb{F}_p).$$

As before,

$$\overline{Q}_1 := \left(\tfrac{1}{2}\left(\tfrac{1}{4}w^2 - \overline{A'} + \tfrac{1}{4}y \cdot w^{-1}\right), \tfrac{1}{4}w\left(\tfrac{1}{4}w^2 - \overline{A'} + \tfrac{1}{4}y \cdot w^{-1}\right)\right)$$

and

$$\overline{Q}_2 := \left(\tfrac{1}{2}\left(\tfrac{1}{4}w^2 - \overline{A'} - \tfrac{1}{4}y \cdot w^{-1}\right), -\tfrac{1}{4}w\left(\tfrac{1}{4}w^2 - \overline{A'} - y \cdot \tfrac{1}{4}w^{-1}\right)\right)$$

are in $\overline{E'}(\mathbb{F}_p)$ and must get mapped to $\overline{\overline{P'}}$ by Ψ. Furthermore, they each lie in $\Psi(\tilde{E}'(\mathbb{F}_p)$ if and only if

$$\tfrac{1}{2}\left(\tfrac{1}{4}w^2 - \overline{A'} + \tfrac{1}{4}y \cdot w^{-1}\right) \in (\mathbb{F}_p^\times)^2 \quad \text{and} \quad \tfrac{1}{2}\left(\tfrac{1}{4}w^2 - \overline{A'} - \tfrac{1}{4}y \cdot w^{-1}\right) \in (\mathbb{F}_p^\times)^2,$$

respectively. Now, letting $\overline{x}_i$ represent the x-coordinate of $\overline{Q}_i$ for $i = 1, 2$,

$$\begin{aligned}
\overline{x}_1\overline{x}_2 &= \frac{1}{4}\left(\left(\tfrac{1}{4}w^2 - \overline{A'}\right)^2 - \tfrac{1}{16}y^2 \cdot w^{-2}\right) \\
&= \frac{1}{4}\left(\left(\tfrac{1}{4}x - \overline{A'}\right)^2 - \tfrac{1}{16}y^2 \cdot x^{-1}\right) \\
&= \frac{1}{4}\left(\tfrac{1}{16}x^3 - \tfrac{1}{2}\overline{A'}x^2 + \overline{A'}^2x - 4\tfrac{1}{64}y^2\right) \cdot x^{-1} \\
&= \overline{B'},
\end{aligned}$$

where the last equality follows from the fact that

$$\begin{aligned}
\tfrac{1}{64}y^2 = \left(\tfrac{1}{8}y\right)^2 &= \left(\tfrac{1}{4}x\right)^3 + \overline{\overline{A'}}\left(\tfrac{1}{4}x\right)^2 + \overline{\overline{B'}}\left(\tfrac{1}{4}x\right) \\
&= \tfrac{1}{64}x^3 + \tfrac{1}{16}(-2\overline{A'})x^2 + \tfrac{1}{4}(\overline{A'}^2 - 4\overline{B'})x.
\end{aligned}$$

Again, powers of 2 are defined, since p is good. We know that $\overline{B'} = (A')^2 - 4B'$ is not a perfect square, for otherwise

$$x^3 + A'x^2 + B'x = x(x^2 + A'x + B')$$

would have three rational roots. This would in turn imply g and thus $\tilde{f}$ would have three roots in $\mathbb{F}_p$, contradicting $k_p = 1$. Hence, it must be that one of $\overline{x}_1$, $\overline{x}_2$ is a square by Proposition 2, showing that one of $\overline{Q}_1$, $\overline{Q}_2$ is mapped to P' by $\Psi \circ \Phi$.

Suppose now that $P' = (0, 0)$. Then $g'(0) = B'$ must be a square, as well as

$$16B' = \overline{\overline{B'}} = \overline{A'}^2 - 4\overline{B'}$$

This implies that

$$\overline{x}^3 + \overline{A'}\overline{x}^2 + \overline{B'}\overline{x} = \overline{x}(\overline{x}^2 + \overline{A'}\overline{x} + \overline{B'})$$

has a nonzero rational solution in $\overline{x}$. Hence, there exists a point $(\overline{x}, 0) \in \overline{E'}(\mathbb{F}_p)$ which is mapped to $(0, 0)$ by Ψ. This point must necessarily be either

$$\overline{R}_1 := \left(\tfrac{1}{2}\left(\overline{A'} + \sqrt{\overline{A'}^2 - 4\overline{B'}}\right), 0\right) \quad \text{or} \quad \overline{R}_2 := \left(\tfrac{1}{2}\left(\overline{A'} - \sqrt{\overline{A'}^2 - 4\overline{B'}}\right), 0\right).$$

The product of their x-coordinates is

$$\tfrac{1}{2}\left(\overline{A'} + \sqrt{\overline{A'}^2 - 4\overline{B'}}\right) \cdot \tfrac{1}{2}\left(\overline{A'} - \sqrt{\overline{A'}^2 - 4\overline{B'}}\right) = \overline{B'},$$

which we know not to be a perfect square. As before, this must mean either $\overline{R}_1$ or $\overline{R}_2$ is lies in $\Phi(\tilde{E}'(\mathbb{F}_p))$. Thus,

$$P' \in \Psi(\Phi(\tilde{E}'(\mathbb{F}_p))) = 2\tilde{E}'(\mathbb{F}_p),$$

proving that $\ker \overline{\varepsilon}_p = 2\tilde{E}(\mathbb{F}_p)$.

In an effort to show $\overline{\varepsilon}_p$ is surjective, suppose the contrary. Then it must be that $\tilde{E}(\mathbb{F}_p) = 2\tilde{E}(\mathbb{F}_p)$, so for any $P \in \tilde{E}(\mathbb{F}_p)$, there exists some $Q \in \tilde{E}(\mathbb{F}_p)$ such that $2Q = P$. Of course, the same holds for Q, and in turn for some R such that $2R = Q$, and so on *ad infinitum*. Since $k_p = 1$, there exists an element of order 2 in $\tilde{E}(\mathbb{F}_p)$, and so 2 divides $|\tilde{E}(\mathbb{F}_p)|$. This implies the above sequence cannot be periodic, and so there exists an element in $\tilde{E}(\mathbb{F}_p)$ of infinite order. This clearly contradicts the fact that $\tilde{E}(\mathbb{F}_p)$ is finite. In consequence, $\overline{\varepsilon}_p$ must be surjective. □

Consequently, we have

$$\tilde{E}(\mathbb{F}_p)/2(\tilde{E}(\mathbb{F}_p) \cong \mathbb{Z}/2\mathbb{Z}.$$

Composition with the reduction modulo p map and factoring through doubles gives the desired homomorphism

$$\varepsilon_p : E(\mathbb{Q})/2E(\mathbb{Q}) \to \tilde{E}(\mathbb{F}_p)/2(\tilde{E}(\mathbb{F}_p) \to \mathbb{Z}/2\mathbb{Z} : P \mapsto \overline{P} \mapsto \overline{\varepsilon}_p(\overline{P}).$$

Proposition 5. *A non-identity point $P \in E(\mathbb{Q})$ can be be written as $P = (u/w^2, v/w^3)$ for integers u, v, w, satisfying* $\gcd(u, w) = \gcd(v, w) = 1$

This follows from inserting $x = u/U$ and $y = v/V$ with $u, v, U, V \in \mathbb{Z}$ and $U, V \neq 0$ in the elliptic curve equation, and deriving $U^3 = V^2$. Letting $w = V/U$ now proves the claim. A complete proof can be found in e.g. Section 3.2, pg. 71, 72 of (Silverman & Tate, 2015).

Now, define the map $\alpha : E(\mathbb{Q}) \setminus \{\mathcal{O}\} \to \mathbb{F}_p^\times$ by

$$\alpha(P) = \begin{cases} \tilde{u} - \theta_p \tilde{w}^2 & \text{if} \quad \tilde{u} \neq \theta_p \tilde{w}^2, \\ f'(\theta_p) & \text{otherwise,} \end{cases}$$

for $P = (u/w^2, v/w^3) \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$ with $u, v, w \in \mathbb{Z}$ and $\gcd(u, w) = \gcd(v, w) = 1$. Here, a tilde on an integer denotes its residue modulo p. This allows us to write

$$\varepsilon_p(P) = \begin{cases} \psi(\alpha(P)) & \text{if } P \neq \mathcal{O}, \\ 0 & \text{otherwise.} \end{cases}$$

To see this, note that in normalized projective coordinates,

$$P = [uw, v, w^3].$$

The reduction modulo p yields

$$\tilde{P} = [\tilde{u}\tilde{w}, \tilde{v}, \tilde{w}^3],$$

which, assuming $\tilde{w} \neq 0$, translates to $\tilde{P} = (\tilde{u}\tilde{w}^{-2}, \tilde{v}\tilde{w}^{-3})$ in affine coordinates. The assertion follows, in this case, because $\tilde{u}\tilde{w}^{-2} - \theta_p$ is a square if and only if $\tilde{u} - \theta_p \tilde{w}^2$ is. So what if $\tilde{w} = 0$? Substitution of $\tilde{P}$ in the homogeneous Weierstrass equation for E,

$$Y^2 Z = X^3 + AX^2 Z + BXZ^2 + CZ^3,$$

yields

$$\tilde{v}^2 \tilde{w}^3 = \tilde{u}^3 \tilde{w}^3 + A\tilde{u}^2 \tilde{w}^5 + B\tilde{u}\tilde{w}^7 + C\tilde{w}^9.$$

Using $\tilde{w} = 0$, we find

$$\tilde{v}^2 = \tilde{u}^3 \quad \text{or} \quad \tilde{u} = \tilde{v}^2 \tilde{u}^{-2} \in (\mathbb{F}_p^\times)^2.$$

This insists $\psi(\alpha(P)) = 0$, as required.

Case two: Three roots in $\mathbb{F}_p$

Fix a good prime p for which $k_p = 2$, so $\tilde{f}(x)$ has three (distinct) roots $\theta_{i,p} \in \mathbb{F}_p$, $i = 1, 2, 3$. If we now take $P = (x, y)$ to be a point not equal to a 2-torsion point in $E(\mathbb{F}_p)$, the elements $x - \theta_{i,p}$ are in $\mathbb{F}_p^\times$. Their product is a square, for the reason that

$$f(x) = \prod_i (x - \theta_{i,p}) = y^2.$$

Recall from proof of Proposition 3 that we may write

$$\mathbb{F}_p^\times / (\mathbb{F}_p^\times)^2 = \{\overline{1}, \overline{a}\},$$

for any $a \in \mathbb{F}_p^\times \setminus (\mathbb{F}_p^\times)^2$. The group $\left(\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2\right)^3$ equipped with component-wise multiplication with identity element $(\overline{1}, \overline{1}, \overline{1})$ therefore has order 8, and each of its elements has order 2. The set H of elements with the product of their components equal to a square forms a subgroup of order 4. It consists of all vectors with an even number of components equal to $\overline{a}$, that is

$$H := \left\{ \begin{pmatrix} \overline{1} \\ \overline{1} \\ \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} \\ \overline{a} \\ \overline{a} \end{pmatrix}, \begin{pmatrix} \overline{a} \\ \overline{1} \\ \overline{a} \end{pmatrix}, \begin{pmatrix} \overline{a} \\ \overline{a} \\ \overline{1} \end{pmatrix} \right\}$$

Before proving the following Proposition 6, we need to introduce the notion of congruent polynomials.

Definition 11. A *ring R* is a field for which multiplication is not necessarily commutative and nonzero elements need not have a multiplicative inverse. A *polynomial ring over R* is a ring $R[x]$, consisting of polynomials in the variable x with coefficients in R. Two polynomials $f(x), g(x) \in R[x]$ are said to be *congruent modulo $p(x) \in R[x]$* if $p(x)$ divides their difference, in which case we write

$$f(x) \equiv g(x) \bmod p(x).$$

Now, we can construct a map $\overline{\varepsilon}_p$ in a similar manner as in Proposition 3.

Proposition 6. *For a good prime p with $k_p = 2$, the map $\overline{\varepsilon}_p : \tilde{E}(\mathbb{F}_p) \to \left((\mathbb{F}_p^\times)^2\right)^3$ defined by*

$$\overline{\varepsilon}_p(P) = (\overline{\varepsilon}_{1,p}, \overline{\varepsilon}_{2,p}, \overline{\varepsilon}_{3,p})(P), \quad P \in \tilde{E}(\mathbb{F}_p),$$

where for $i = 1, 2, 3$,

$$\overline{\varepsilon}_{i,p}(P) = \begin{cases} x - \theta_{i,p} \bmod (\mathbb{F}_p^\times)^2 & \text{if } \tilde{\mathcal{O}} \neq \mathbb{P} = (x, y) \text{ and } x \neq \theta_{i,p}, \\ f'(\theta_{i,p}) \bmod (\mathbb{F}_p^\times)^2 & \text{if } \tilde{\mathcal{O}} \neq \mathbb{P} = (\theta_i, 0), \\ 1 \bmod (\mathbb{F}_p^\times)^2 & \text{if } P = \tilde{\mathcal{O}}, \end{cases}$$

is a homomorphism with image H and kernel $2\tilde{E}(\mathbb{F}_p)$.

Proof. Each component $\overline{\varepsilon}_{p,i}$ of $\overline{\varepsilon}_p$ is a homomorphism for the same reason that $\overline{\varepsilon}_p$ from Proposition 3 was a homomorphism (in this case define the 'shifted' elliptic curve for each $i = 1, 2, 3$, then the rest of the proof is identical). Seeing that each component of $\overline{\varepsilon}_p$ is a homomorphism, the same must hold for $\overline{\varepsilon}_p$.

To show the image of $\overline{\varepsilon}_p$ lies in H, note that $P = (x, y) \in \tilde{E}(\mathbb{F}_p)$ with $x \neq \theta_{i,p}$ for $i = 1, 2, 3$ implies $\overline{\varepsilon}_p(P) \in H$, by the argument preceding Definition 11. Also, $\overline{\varepsilon}_p(\tilde{O}) = (\overline{1}, \overline{1}, \overline{1}) \in H$ because $\overline{\varepsilon}_p$ is a homomorphism. Consider now $P = (\theta_{i,p}, 0)$, and note that all $\theta_{i,p}$'s are distinct since p is good. Assume without loss of generality that $P = (\theta_{1,p}, 0)$. Then, since $\tilde{E}$ is given by

$$y^2 = x^3 + \tilde{A}x^2 + \tilde{B}x + \tilde{C}, \quad \tilde{A}, \tilde{B}, \tilde{C} \in \mathbb{F}_p. \tag{4.2}$$

we find

$$f'(\theta_{1,p})(\theta_{1,p} - \theta_{2,p})(\theta_{1,p} - \theta_{3,p}) = (3\theta_{1,p}^2 + 2\tilde{A}\theta_{1,p} + \tilde{B})(\theta_{1,p} - \theta_{2,p})(\theta_{1,p} - \theta_{3,p}).$$

Since

$$x^3 + \tilde{A}x^2 + \tilde{B}x + \tilde{C} = f(x) = \prod_i (x - \theta_{i,p}),$$

we know

$$\tilde{A} = -(\theta_{1,p} + \theta_{2,p} + \theta_{3,p}) \quad \text{and} \quad \tilde{B} = \theta_{1,p}\theta_{2,p} + \theta_{1,p}\theta_{3,p} + \theta_{2,p}\theta_{3,p}.$$

Doing some simple algebra, we find

$$f'(\theta_{1,p}) = (\theta_{1,p} - \theta_{2,p})(\theta_{1,p} - \theta_{3,p}),$$

so

$$f'(\theta_{1,p})(\theta_{1,p} - \theta_{2,p})(\theta_{1,p} - \theta_{3,p}) = (\theta_{1,p} - \theta_{2,p})^2(\theta_{1,p} - \theta_{3,p})^2 \in (\mathbb{F}_p^\times)^2.$$

As a consequence $\overline{\varepsilon}_p(P) \in H$, thus we derive $\overline{\varepsilon}_p(\tilde{E}(\mathbb{F}_p)) \subset H$. The other inclusion will follow from $\ker \overline{\varepsilon}_p = 2\tilde{E}(\mathbb{F}_p)$.

By Proposition 2, it must be that $2\tilde{E}(\mathbb{F}_p) \subset \ker \overline{\varepsilon}_p$ due to $\overline{\varepsilon}_p$ being a homomorphism. The proof that $\ker \overline{\varepsilon}_p \subset 2\tilde{E}(\mathbb{F}_p)$ below is profoundly based on and nearly identical to the second part of the poof of Theorem 8.14 in (Washington, 2008). Because p is good, $\operatorname{char}(\mathbb{F}_p) \neq 3$. We may therefore perform the change of coordinates on $\tilde{E}$ given by

$$(x, y) \mapsto \left((x - 12\tilde{B}) \cdot 36^{-1}, y \cdot 108^{-1}\right),$$

to transform (4.2) to an equation of the form

$$y^2 = x^3 + \tilde{A}'x + \tilde{B}',$$

c.f. pages 42, 43 in (Silverman, 2009). Again, $36 = 2^2 3^2$ and $108 = 2^2 3^3$ are defined since p is good. Suppose first that $P = (x, y) \in \ker \overline{\varepsilon}_p$ is such that $2P \neq 0$. Then for $i = 1, 2, 3$,

$$x - \theta_{i,p} := v_i^2$$

for some $v_i \in \mathbb{F}_p^\times$. There exists a (unique) quadratic polynomial

$$f(T) = u_0 + u_1 T + u_2 T^2 \in \mathbb{F}_p[T] \quad \text{such that} \quad f(\theta_{i,p}) = v_i \quad \text{for} \quad i = 1, 2, 3,$$

since for n points with distinct x-coordinates there is always a unique polynomial of degree $n-1$ whose graph contains all n points. Now,

$$g(T) = x - T - (f(T))^2 \quad \text{satisfies} \quad g(\theta_{i,p}) = x - \theta_{i,p} - v_i^2 = 0 \quad \text{for} \quad i = 1, 2, 3.$$

So, $g(T)$ can be factored as

$$g(T) = (T - \theta_{1,p})(T - \theta_{2,p})(T - \theta_{3,p})h(T)$$

for some $h \in \mathbb{F}_p[T]$ with $\deg h < \deg g$. Since $(T - \theta_{1,p})(T - \theta_{2,p})(T - \theta_{3,p}) = T^3 + \tilde{A}'T + \tilde{B}'$,

$$g(T) \equiv 0 \bmod (T^3 + \tilde{A}'T + \tilde{B}'),$$

and therefore

$$\begin{aligned} x - T &\equiv (u_0 + u_1 T + u_2 T^2)^2 && \bmod (T^3 + \tilde{A}'T + \tilde{B}') \\ &\equiv u_0^2 + 2u_0u_1T + (u_1^3 + 2u_0u_2)T^2 + 2u_1u_2T^3 + u_2^2T^4 && \bmod (T^3 + \tilde{A}'T + \tilde{B}'). \end{aligned}$$

Additionally, $T^3 \equiv -\tilde{A}'T - \tilde{B}' \bmod (T^3 + \tilde{A}'T + \tilde{B}')$, so

$$\begin{aligned} x - T \equiv (u_0^2 - 2\tilde{B}'u_1u_2) &+ (2u_0u_1 - 2\tilde{A}'u_1u_2 - \tilde{B}'u_2^2)T \\ &+ (u_1^2 + 2u_0u_2 - \tilde{A}'u_2^2)T^2 \qquad \bmod (T^3 + \tilde{A}'T + \tilde{B}'). \end{aligned}$$

This must imply

$$u_0^2 - 2\tilde{B}'u_1u_2 = x, \tag{4.3}$$

$$2u_0u_1 - 2\tilde{A}'u_1u_2 - \tilde{B}'u_2^2 = -1, \tag{4.4}$$

$$u_1^2 + 2u_0u_2 - \tilde{A}'u_2^2 = 0. \tag{4.5}$$

We know that $u_2 \neq 0$, since otherwise $u_1 = 0$ and consequently $f(T)$ must be constant, i.e

$$f(T) = v_1 = v_2 = v_3, \quad \text{so} \quad x - \theta_{1,p} = x - \theta_{2,p} = x - \theta_{3,p}.$$

From this it would follow the $\theta_{i,p}$ are equal, contradicting p being good. Thus, we may multiply (4.4) by $-u_2^{-2}$, and using $u_1^2 + 2u_0u_2 - \tilde{A}'u_2^2 = 0$, we acquire

$$\left(u_2^{-1}\right)^2 = \left(u_1u_2^{-1}\right)^3 + \tilde{A}'\left(u_1u_2^{-1}\right) + \tilde{B}'.$$

showing $\tilde{Q} = (\hat{x}, \hat{y})$ with $\hat{x} = u_1u_2^{-1}, \hat{y} = u_2^{-1}$ lies on $\tilde{E}(\mathbb{F}_p)$. From (4.5) we have

$$u_0 = \tfrac{1}{2}(\tilde{A}'u_2^2 - u_1^2)u_2^{-1} = \tfrac{1}{2}(\tilde{A}' - u_1^2u_2^{-2})u_2 = \tfrac{1}{2}(\tilde{A}' - \hat{x}^2)\hat{y}^{-1}.$$

From substitution of this into (4.3) follows

$$\begin{aligned} x &= \tfrac{1}{4}(\tilde{A}'^2 - 2\tilde{A}\hat{x}^2 + \hat{x}^4)\hat{y}^{-2} - 2\tilde{B}'u_1u_2 \\ &= \tfrac{1}{4}(\tilde{A}'^2 - 2\tilde{A}\hat{x}^2 + \hat{x}^4 - 8\tilde{B}'\hat{x})\hat{y}^{-2} \\ &= (\hat{x}^4 - 2\tilde{A}\hat{x}^2 - 8\tilde{B}'\hat{x} + \tilde{A}'^2)(4\hat{x}^3 + 4\tilde{A}'\hat{x} + 4\tilde{B}\tilde{)}^{-1}. \end{aligned}$$

This is the duplication formula, c.f. page 27 in (Silverman & Tate, 2015) (actually, the one referenced is for $E(\mathbb{Q})$, but it generalizes to $E(\mathbb{K})$ for a general field $\mathbb{K}$). This means x is the x-coordinate of $2(\hat{x}, \hat{y})$. The y-coordinate is determined by the x-coordinate up to sign, so

$$P = 2(\hat{x}, \hat{y}) \quad \text{or} \quad P = 2(\hat{x}, -\hat{y}),$$

whereby $P \in 2E(\mathbb{Q})$.

Assume now that $P = (\theta_{i,p}, 0) \in \ker \overline{\varepsilon}_p$ and that, without loss of generality, $i = 1$. This must mean that

$$(\theta_{1,p} - \theta_{2,p}), (\theta_{1,p} - \theta_{3,p}) \in (\mathbb{F}_p^\times)^2,$$

since $f'(\theta_{1,p}) = (\theta_{1,p} - \theta_{2,p})(\theta_{1,p} - \theta_{3,p})$. Apply the same procedure, this time letting

$$\theta_{1,p} - \theta_{i,p} = v_i^2,$$

where $v_i \in \mathbb{F}_p^\times$ if $i \neq 1$ and $v_i = 0$ otherwise. The rest of the proof is then the same as before. This concludes $\ker \overline{\varepsilon}_p = 2\tilde{E}(\mathbb{F}_p)$.

The argument given in the proof of Proposition 4 to prove that $\overline{\varepsilon}_p$ from Proposition 3 is surjective also shows the image of $\overline{\varepsilon}_p$ cannot be trivial. So, it contains at least one nontrivial element of H. This implies the other nontrivial elements of H must lie in the image of $\overline{\varepsilon}_p$ as well, so this image of $\overline{\varepsilon}_p$ must equal H. □

Since all nontrivial elements of H have order 2, $H \cong (\mathbb{Z}/2\mathbb{Z})^2$. This remains true if we project onto the first two coordinates of $\overline{\varepsilon}_p$ and H, and switch to additive notation. Hence, we obtain an isomorphism

$$\tilde{E}(\mathbb{F}_p)/2\tilde{E}(\mathbb{F}_p) \to (\mathbb{Z}/2\mathbb{Z})^2,$$

which we can again compose with the reduction modulo p map, yielding

$$\varepsilon_p : E(\mathbb{Q})/2E(\mathbb{Q}) \to (\mathbb{Z}/2\mathbb{Z})^2.$$

Define the map $\alpha_i : E(\mathbb{Q}) \to \mathbb{F}_p^\times$ by

$$\alpha_i(P) = \begin{cases} \tilde{u} - \theta_{i,p}\tilde{w}^2 & \text{if} \quad \tilde{u} \neq \theta_p \tilde{w}^2, \\ f'(\theta_{i,p}) & \text{otherwise,} \end{cases} \qquad (i = 1, 2, 3)$$

for a non-identity point $P = (u/w^2, v/w^3) \in E(\mathbb{Q})$, where u, v, w are integers such that $\gcd(u, w) = \gcd(v, w) = 1$. A tilde on an integer once more denotes its residue modulo p. This allows us to write

$$\varepsilon_p(P) = (\psi(\alpha_1(P)), \psi(\alpha_2(P)))$$

for $P \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$, analogous to the case where $k_p = 1$.

The final homomorphism

Take a set of good primes $\{p_1, p_2, \ldots, p_m\}$ with $k_{p_i} \neq 0$ for $i = 1, \ldots, m$, and define the homomorphism

$$\varepsilon : E(\mathbb{Q})/2E(\mathbb{Q}) \to (\mathbb{Z}/2\mathbb{Z})^M : P \mapsto (\varepsilon_{p_1}(P), \varepsilon_{p_2}(P), \ldots, \varepsilon_{p_m}(P)), \quad M = \sum_i k_{p_i}.$$

Before showing this map is injective for a sufficient amount good primes, let us consider how to halve a point $Q = 2R \in 2E(\mathbb{Q})$ (we will need it in the proof of Lemma 1). If $Q = (\alpha, \beta)$, the x-coordinate of R is computed by finding a rational x such that (c.f. the duplication formula on page 27 in (Silverman & Tate, 2015))

$$\alpha = \frac{U}{V} = \frac{x^4 - 2Bx^2 - 8Cx + B^2 - 4AC}{4x^3 + 4Ax^2 + 4Bx + 4C} \quad (U, V \in \mathbb{Z},\ V \neq 0)$$

where $U, V \in \mathbb{Z}$ and $V \neq 0$. This is equivalent to finding a rational root of

$$F(x) := V(x^4 - 2Bx^2 - 8Cx + B^2 - 4AC) - U(4x^3 + 4Ax^2 + 4Bx + 4C). \tag{4.6}$$

This may be accomplished with use of the quartic formula or by factoring the 4th degree polynomial F. The y-coordinate is obtained by substituting this value of of x into the affine Weierstrass equation. Note that the same procedure can be used when halving points in $2\tilde{E}(\mathbb{F}_p)$, putting tildes over the coefficients A, B, C if preferred.

We require one more ingredient to prove Lemma 1. The following result is stated without proof, so as to avoid having to get into Galois theory and algebraic number theory. This is Theorem 3.1.7 from (Pesiri, 2007), which also contains a proof.

Theorem 2. *Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial that does not have a root modulo only finitely many primes. Then $f(x)$ has degree 1.*

Lemma 2.1 from (Cremona, 2002) is as follows.

Lemma 1. *For a rational point $P \notin 2E(\mathbb{Q})$ on E, there exists a good prime p with $k_p \neq 0$ satisfying $\varepsilon_p(P) \neq 0$.*

Proof. Take $P = (\alpha, \beta) \in E(\mathbb{Q}) \setminus 2E(\mathbb{Q})$ where $\alpha = U/V$, with $U, V \in Z$ and $V \neq 0$. Let $F(x)$ be as in (4.6). Suppose first that $F(x)$ is irreducible. If we assume $F(x)$ has no roots modulo only finitely many primes, then $F(x)$ is linear by Theorem 2, a contradiction. So, $F(x)$ has no roots modulo infinitely many primes. Suppose now that $F(x)$ is reducible. Let $G_1(x), \ldots, G_k(x) \in \mathbb{Q}[x]$ be irreducible polynomials such that

$$F(x) = G_1(x) \cdots G_k(x).$$

Because $P \notin 2E(\mathbb{Q})$, $F(x)$ cannot have any roots in $\mathbb{Q}$. Therefore, $k = 2$, and $G_1(x)$, $G_2(x)$ are both of degree 2. Because we are only interested in the roots of $G_1(x)$ and $G_2)$, we may multiply out any denominators and divide by any common factors, to make sure $G_i(x)$ has integer coefficients for $i = 1, 2$. Again, $G_i(x)$ does not have a root modulo infinitely many primes for $i = 1, 2$ by Theorem 2. Hence, $F(x)$ has no roots modulo infinitely many primes.

Because there are only finitely primes that are not good, there must also be infinitely many good primes for which this holds. For these primes p, there exists no $\tilde{R} \in \tilde{E}(\mathbb{F}_p)$ such that the $\tilde{P} = 2\tilde{R}$, where $\tilde{P}$ is the reduction modulo p of P. Consequently $\tilde{P} \notin \tilde{2}E(\mathbb{F}_p)$. Note that we cannot have $k_p = 0$, as this would imply $\tilde{E}(\mathbb{F}_p) = 2\tilde{E}(\mathbb{F}_p)$, even though $\tilde{P} \in \tilde{E}(\mathbb{F}_p)$. This completes the proof. □

Lemma 1 says that for a sufficient amount of good primes p for which $k_p \neq 0$, the homomorphism ε will have a trivial kernel, in which case it must be injective. The following proposition from Appendix D in (Silverman, 2000) shows that a 'sufficient' amount will, in practice, not be infeasibly large. A proof can be found there as well, and since it is quite straightforward, we will not repeat it here. As is easily seen, the given probability rapidly tends to 1 as we increase M.

Proposition 7. *For randomly chosen homomorphisms $\xi_1, \ldots, \xi_M : \mathbb{Z}^n \to \mathbb{Z}/2\mathbb{Z}$, the map*

$$\Xi = (\xi_1, \ldots, \xi_M) : \mathbb{Z}^n \to (\mathbb{Z}/2\mathbb{Z})^M \quad (M \geqslant n)$$

is injective with probability

$$\prod_{i=0}^{n-1} \left(1 - \frac{1}{2^{M-i}}\right).$$

4.2 Checking independence or finding an explicit dependence relation

Now that we have constructed a homomorphism $\varepsilon : E(\mathbb{Q})/2E(\mathbb{Q}) \to (\mathbb{Z}/2\mathbb{Z})^M$, assume we have rational points $P_1, \ldots, P_n$ on E, which include generators of $E(\mathbb{Q})[2]$ (we explained the reason for this in Section 2.3). We denote by $v_i = \varepsilon(P_i)$ the image of P_i under ε. The points P_i are independent if the images v_i are; in particular if the rank of

$$A := (v_1, \ldots, v_n)$$

equals n. If not, we can first add more good primes until we reach a certain threshold. Using Proposition 7, we find that the probability that ε is not injective for n points on $E(\mathbb{Q})$ is less than 10^{-6} if we have $M \geqslant n + 20$. Since M is greater than the number of good primes p for which $k_p \neq 0$, we can let the maximum number of primes used equal $n + 20$. So, say we have reached this threshold, however A still has rank less than n. In that case, we take any nontrivial vector from $\ker A$, and substitute 1 for $1 \bmod 2$ and 0 for $0 \bmod 2$. In this manner we obtain a vector $c = (c_1, \ldots, c_n)$ with each $c_i \in \{0, 1\}$, and we subsequently compute

$$Q := c_1 P_1 + \cdots + c_n P_n.$$

There are three cases to consider.

1. If Q has finite order, we have found an explicit dependence relation.

2. If Q does not have finite order and moreover $Q \notin 2E(Q)$, then increasing the number of good primes will prove the points P_i are independent. The reason is that ε is not injective for the current amount of good primes.

3. If Q does not have finite order and $Q \in 2E(\mathbb{Q})$, then we attempt an iterative procedure, which will certainly terminate when the points P_i are independent (we will elaborate on this in a moment). If they are not, however, we may face some complications.

Lifting the dependence relation from $E(\mathbb{Q})/2E(\mathbb{Q})$

Suppose therefore that we have obtained some linear combination

$$Q := c_1P_1 + \cdots + c_nP_n \quad (c_i \in \{0,1\}),$$

and that $Q \in 2E(\mathbb{Q}) \setminus T$, where $T := E(\mathbb{Q})_{\text{tor}}$. There must exist some point $R \in E(\mathbb{Q}) \setminus T$ that satisfies $Q = 2R$. We now replace a point P_i for which $c_i = 1$ by R, so that we obtain a new set of points

$$\left\{P_1^{(1)}, \ldots, P_n^{(1)}\right\}$$

to which we apply the same procedure as before until, hopefully, at some step k one of three cases occurs:

1. The set $\left\{P_1^{(k)}, \ldots, P_n^{(k)}\right\}$ is independent, whereby the original points were independent. If the original set of points is independent, this is bound to happen after finitely many iterations. This is due to the span of the set of points being strictly larger than the span of the previous set of points, where the span of a set of points $R_1, \ldots, R_d$ on $E(\mathbb{Q})$ is defined as

   $$\operatorname{span}\{R_1, \ldots, R_d\} = \{\, z_1R_1 + \cdots + z_dR_d \mid z_i \in \mathbb{Z}\,\}.$$

   Namely, after replacing a point P_i in a combination $2R = \sum_i c_iP_i$ for which c_i = 1 by R, the new set of points spans

   $$\left\{ \sum_i z_i\left(\tfrac{1}{2}c_i + (1-c_i)\right)P_i \;\middle|\; z_i \in \mathbb{Z} \right\} \supsetneq \{\, z_1P_1 + \cdots + z_nP_n \mid z_i \in \mathbb{Z}\,\}.$$

2. We find some combination

   $$c_1^{(k)}P_1^{(k)} + \cdots + c_n^{(k)}P_n^{(k)} = Q \in T,$$

   from which we can construct an explicit dependence relation by recursively substituting

   $$P_i^{(k)} = R^{(\ell)} := \frac{1}{2}\left(c_1^{(\ell)}P_1^{(\ell)} + \cdots + c_n^{(\ell)}P_n^{(\ell)}\right),$$

   for $i = 1, \ldots, n$, where ℓ was the step after which $P_i^{(\ell)}$ was replaced by $R^{(\ell)}$. Afterwards, we can multiply the coefficients by a suitable power of 2 if we want them to be integer.

3. We obtain some $Q^{(k)} := \hat{Q}_1$ given by

   $$c_1^{(k)}P_1^{(k)} + \cdots + c_n^{(k)}P_n^{(k)} = \hat{Q}_1,$$

   which has a difference with some earlier encountered combination that is torsion, i.e. for

   $$c_1^{(\ell)}P_1^{(\ell)} + \cdots + c_n^{(\ell)}P_n^{(\ell)} = \hat{Q}_2 \quad (\ell < k),$$

   $\operatorname{ord}(\hat{Q}_1 - \hat{Q}_2) < \infty$. Analogous to the previous case, this allows us to construct an explicit dependence relation. This procedure is illustrated in the example in Section 5.3.

If the points are actually dependent, there is no guarantee that one of the last two cases ever occurs, c.f. Appendix D in (Silverman, 2000). In this case, we may result to using heights to find a dependence relation, that is to the method described in Section 3.

5 Examples

5.1 The Martin-McMillan curve

The following example was treated in (Cremona, 2002), and repeating it here is a good way to verify our implementation is correct (or at least not completely off). The "Martin-McMillan curve" is given by the equation

$$\begin{aligned} E: \quad y^2 + xy + y =& x^3 - 19252966408674012828065964616418441723x \\ &+ 32685500727716376257923347071452044295907443056345614006, \end{aligned}$$

and along with it, 23 points in $E(\mathbb{Q})$ are listed:

$$\begin{aligned}
P_1 &= (2509558762692426075, -4170888616355827764278386 28), \\
P_2 &= (-3152306069115988905, 7877320130079209226656589052), \\
P_3 &= (15693029027991085860, -59960725518716592640454389523), \\
P_4 &= (-15685545762070490045/9, 2107841830327082003324157 73604/27), \\
P_5 &= (2698930732460382795, 6186294313504323903889413 52), \\
P_6 &= (3055828716067659795, -15451000176289834607604626 48), \\
P_7 &= (5176107139118431770, -8468104093201669542836552123), \\
P_8 &= (3784518081907585155, 3745177334989174939461966292), \\
P_9 &= (3375602798684599395, 2481752453981065849886565352), \\
P_{10} &= (50254260027721383195, 354939157845809277536295633352), \\
P_{11} &= (-1426959665463488885, 5952303401545410666113166952), \\
P_{12} &= (-3221315322202018425, 7828039241604579170601658372), \\
P_{13} &= (2537753825844495495, 4121161808255576543735556 52), \\
P_{14} &= (2593670816475114795, -4445221991004209101702826 48), \\
P_{15} &= (3653122955244689466, 3332280856915069273216378309), \\
P_{16} &= (16913850473547768195, -67422028572509502534315689048), \\
P_{17} &= (91407152955412578142189035/137217796, \\
&\quad - 72163197090212782399483817880802250265 37/1607369262344), \\
P_{18} &= (2318736179743409595, -7139488122623641484213069 48), \\
P_{19} &= (854939343706550155/9, -149983616867035973534953843496/27), \\
P_{20} &= (2291515542997719795, 7745170829213338282454973 52), \\
P_{21} &= (-1722575558649090805, -7793513279470674099171802548), \\
P_{22} &= (-5015906559699694713, -17492255258064496128840051 32), \\
P_{23} &= (120758256425435359837 5/49, 413399002347769366578669729808 36/343).
\end{aligned}$$

p	**7**	31	43	47	**53**	59	67	71	83	89	97	109	113	127	**131**	139	149	**151**	157	163
P_1	0,1	1	1	1	1,0	1	0	0	0	1	0	0	0	0	0,1	0	0	1,1	1	1
P_2	1,0	1	0	0	0,1	1	1	1	0	1	1	1	0	0	1,1	0	0	1,1	1	1
P_3	1,1	1	0	0	1,0	0	1	1	1	1	1	1	0	0	0,0	0	0	1,1	1	0
P_4	0,1	0	1	1	1,0	1	1	0	1	1	1	0	0	1	0,0	0	1	1,0	1	0
P_5	0,0	1	1	0	1,0	0	1	1	0	1	0	1	0	0	0,1	0	0	1,0	1	0
P_6	0,0	1	1	0	0,1	0	0	0	1	1	1	1	0	1	0,1	0	0	0,1	0	1
P_7	0,1	0	0	1	1,0	1	1	1	0	0	1	0	0	1	0,0	1	1	0,0	0	1
P_8	1,1	0	0	1	0,0	0	1	1	1	1	1	1	1	1	1,1	1	0	1,0	1	0
P_9	1,0	0	1	0	1,1	1	0	0	1	0	0	1	1	1	0,0	1	1	1,0	1	1
P_{10}	0,1	1	0	1	1,0	1	1	1	0	1	0	1	1	1	0,1	0	1	1,0	0	1
P_{11}	0,1	0	1	0	1,0	1	0	1	0	1	0	0	1	1	1,1	1	0	0,0	1	0
P_{12}	0,1	0	0	1	1,1	1	1	0	1	0	0	0	0	1	1,1	0	1	0,0	0	1
P_{13}	1,0	1	0	1	1,1	1	0	0	0	1	1	0	0	1	0,1	0	0	0,0	1	1
P_{14}	1,0	1	0	0	1,0	1	1	0	0	0	0	1	0	1	1,1	1	1	0,1	0	0
P_{15}	0,1	0	1	0	1,0	1	1	1	0	0	0	1	1	0	1,0	1	1	0,1	0	1
P_{16}	1,1	0	0	1	1,1	0	0	0	0	0	0	0	0	1	1,1	0	1	1,1	1	0
P_{17}	1,0	0	0	0	1,0	1	0	0	1	0	1	0	0	1	1,1	0	0	1,1	1	0
P_{18}	0,1	0	1	1	1,0	1	1	0	0	0	0	1	1	1	1,0	1	0	1,0	1	1
P_{19}	0,1	0	0	0	0,0	1	0	0	0	1	1	1	1	0	0,1	1	1	0,0	1	0
P_{20}	0,1	0	1	0	1,1	0	1	1	0	1	0	1	1	1	1,1	1	1	0,1	1	0
P_{21}	1,1	0	0	0	1,1	0	0	1	0	1	1	1	0	0	0,0	0	0	1,0	0	0
P_{22}	0,1	0	1	0	1,0	0	1	1	1	0	1	1	0	1	0,1	0	0	0,1	0	1
P_{23}	0,0	0	0	1	0,1	1	1	1	0	1	0	1	1	0	1,0	1	1	1,1	1	0

Table 5.1: The images of the points on the Martin-McMillan curve under ε

With 19 good primes less than or equal to 157, we obtain a 23×23 matrix which has rank 22. Once we add 163 to the set of good primes, we acquire the final matrix presented in Table 5.1, which has rank 23. This proves the points $P_i, \dots, P_{23}$ are independent.

Apart from the columns corresponding to the boldface good primes, this matrix is identical to the one presented at the end of Section 2.3 in (Cremona, 2002). The difference stems from the choice of the roots of $\tilde{f}(x)$ in $\mathbb{F}_p$ for primes p with $k_p = 2$, and is not relevant to the independence or dependence of the points.

5.2 The Elkies curve

Of particular importance is the "Elkies curve"; this curve has rank 28, c.f. (Klagsbrun, Sherman, & Weigandt, 2018), which is the highest currently observed. It is given by

$$\begin{aligned} E: \quad y^2 + xy + y = x^3 - x^2 &- 20067762415575526585033208209338542750930230312178956502x \\ &+ 3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9, \end{aligned}$$

and we have a list of 28 points in $E(\mathbb{Q})$,

$$\begin{aligned}
P_1 &= (-2124150091254381073292137463, 259854492051899599030515511070780628911531), \\
P_2 &= (2334509866034701756884754537, 18872004195494469180868316552803627931531), \\
P_3 &= (-1671736054062369063879038663, 251709377261144287808506947241319126049131), \\
P_4 &= (2139130260139156666492982137, 36639509171439729202421459692941297527531), \\
P_5 &= (1534706764467120723885477337, 85429585346017694289021032862781072799531), \\
P_6 &= (-2731079487875677033341575063, 262521815484332191641284072623902143387531),
\end{aligned}$$

$$\begin{aligned}
P_7 &= (2775726266844571649705458537, 12845755474014060248869487699082640369931),\\
P_8 &= (1494385729327188957541833817, 88486605527733405986116494514049233411451),\\
P_9 &= (1868438228620887358509065257, 59237403214437708712725140393059358589131),\\
P_{10} &= (2008945108825743774866542537, 47690677880125552882151750781541424711531),\\
P_{11} &= (2348360540918025169651632937, 17492930006200557857340332476448804363531),\\
P_{12} &= (-1472084007090481174470008663, 246643450653503714199947441549759798469131),\\
P_{13} &= (2924128607708061213363288937, 28350264431488878501488356474767375899531),\\
P_{14} &= (5374993891066061893293934537, 286188908427263386451175031916479893731531),\\
P_{15} &= (1709690768233354523334008557, 71898834974686089466159700529215980921631),\\
P_{16} &= (2450954011353593144072595187, 4445228173532634357049262550610714736531),\\
P_{17} &= (2969254709273559167464674937, 32766893075366270801333682543160469687531),\\
P_{18} &= (2711914934941692601332882937, 2068436612778381698650413981506590613531),\\
P_{19} &= (20078586077996854528778328937, 2779608541137806604656051725624624030091531),\\
P_{20} &= (2158082450240734774317810697, 34994373401964026809969662241800901254731),\\
P_{21} &= (2004645458247059022403224937, 48049329780704645522439866999888475467531),\\
P_{22} &= (2975749450947996264947091337, 33398989826075322320208934410104857869131),\\
P_{23} &= (-2102490467686285150147347863, 259576391459875789571677393171687203227531),\\
P_{24} &= (311583179915063034902194537, 168104385229980603540109472915660153473931),\\
P_{25} &= (2773931008341865231443771817, 12632162834649921002414116273769275813451),\\
P_{26} &= (2156581188143768409363461387, 35125092964022908897004150516375178087331),\\
P_{27} &= (3866330499872412508815659137, 121197755655944226293036926715025847322531),\\
P_{28} &= (2230868289773576023778678737, 28558760030597485663387020600768640028531).
\end{aligned}$$

With 23 good primes between 29 and 197 we obtain a 28×28 matrix with rank 26. Adding 211 to our list of good primes, the new matrix has dimension 28×30 and rank 27. After adding the prime 227, we obtain a 28×31 matrix of rank 28, showing the points $P_1, \ldots, P_{28}$ are independent. This final matrix is depicted in Table 5.3.

5.3 Elliptic Curve 44755.a1

An important functionality of this method is that we can find explicit dependence relations. We will test this functionality on the (rather arbitrarily chosen) elliptic curve with Cremona label 44755b1 is given by

$$E' : \quad y^2 + y = x^3 + x^2 - 410x + 3306.$$

We choose four integral points on E,

$$\begin{aligned}
P'_1 &= (105, 1062),\\
P'_2 &= (680, 17737),\\
P'_3 &= (1653, 67221),\\
P'_4 &= (2470, 122777).
\end{aligned}$$

and since E has rank 3, they must be dependent. We first make a coordinate change to get the affine Weierstrass equation in the form

$$y^2 = x^3 + Ax^2 + Bx + C, \quad A, B, C \in \mathbb{Z},$$

yielding

$$E: \quad y^2 = x^3 + 4x^2 - 6560x + 211600.$$

and

$$\begin{aligned} P_1 &= (420, 8500), \\ P_2 &= (2720, 141900), \\ P_3 &= (6612, 537772), \\ P_4 &= (9880, 982220). \end{aligned}$$

Allowing for a maximum of $24 = 4 + 20$ good primes for each iteration, no addition to the set of existing good primes can render the rank of the resulting matrix above 3, as expected). When the threshold of 24 is reached, we end up with

$$P_1 + P_2 + P_4 = Q = 2R = \left(\frac{39537880}{233289}, \frac{227677109500}{112678587}\right)$$

with $\varepsilon(Q) = \mathbf{0} \in \mathbb{F}_2^M$. We can write $Q = 2R$ since $Q \in 2E(\mathbb{Q})$. Repeating the procedure yields

$$\begin{aligned} R + P_2 + P_4 = Q^{(1)} = 2R^{(1)} &= \left(-\frac{630262195630680}{19945950955921}, -\frac{557254659586759 74323500}{89080392158778262969}\right), \\ R^{(1)} + P_2 + P_3 + P_4 = Q^{(2)} = 2R^{(2)} &= \left(\frac{6564070977660}{357851614849}, \frac{672830495661404 25820}{214069340963975743}\right), \\ R^{(2)} = Q^{(3)} = 2R^{(3)} &= \left(\frac{66120}{961}, \frac{9648500}{29791}\right), \\ R^{(3)} + P_4 = Q^{(4)} &= \left(\frac{39537880}{233289}, \frac{227677109500}{112678587}\right) = Q. \end{aligned}$$

where each $\varepsilon\left(Q^{(j)}\right) = \mathbf{0}$. An explicit dependence relation can be obtained e.g. by backward substitution, as follows:

$$\begin{aligned} \mathcal{O} = Q^{(4)} - Q &= R^{(3)} + P_4 - P_1 - P_2 - P_4 \\ &= \tfrac{1}{2}R^{(2)} - P_1 - P_2 \\ &= \tfrac{1}{4}(R^{(1)} + P_2 + P_3 + P_4) - P_1 - P_2 \\ &= \tfrac{1}{8}(R + P_2 + P_4) - P_1 - \tfrac{3}{4}P_2 + \tfrac{1}{4}P_3 + \tfrac{1}{4}P_4 \\ &= \tfrac{1}{16}(P_1 + P_2 + P_4) - P_1 - \tfrac{5}{8}P_2 + \tfrac{1}{4}P_3 + \tfrac{3}{8}P_4 \\ &= -\tfrac{15}{16} - \tfrac{9}{16}P_2 + \tfrac{1}{4}P_3 + \tfrac{7}{16}P_4. \end{aligned}$$

It is therefore given by

$$-15P_1 - 9P_2 + 4P_3 + 7P_4 = \mathcal{O}.$$

Recall that this also holds for the points P_i' on the original curve E', because the coordinate change we applied is an isomorphism.

p	29	31	**41**	43	47	**59**	67	71	83	89	101	103	**107**	109	**131**	**137**	139	157	163	173	181	193	197	**211**	227
P_1	0	0	0,1	1	1	1,1	1	0	0	0	1	1	1,0	0	1,0	1,0	1	0	0	1	1	0	0	1,0	1
P_2	0	0	1,1	1	0	1,0	0	0	1	0	0	0	0,0	0	1,1	1,0	0	1	1	1	0	1	1	0,0	0
P_3	1	0	1,1	0	1	1,0	0	0	1	1	0	0	1,1	1	1,0	1,1	0	1	1	1	0	0	1	0,1	1
P_4	0	0	0,0	0	0	1,0	0	1	0	0	0	1	0,1	0	1,0	0,1	0	0	0	1	1	0	1	0,0	1
P_5	0	1	1,0	0	0	0,1	0	0	0	1	0	0	0,1	0	1,0	1,1	0	0	0	1	1	0	1	1,1	1
P_6	0	0	1,1	0	0	1,0	0	1	0	1	0	0	0,1	1	0,1	1,0	0	0	1	0	1	1	1	1,1	0
P_7	1	1	0,1	1	1	0,1	1	1	1	1	0	1	1,1	0	1,0	0,0	0	0	1	0	0	0	1	0,0	0
P_8	0	1	0,0	0	1	1,1	1	1	1	1	1	1	0,1	0	1,1	0,0	0	0	1	0	0	0	0	0,0	0
P_9	0	0	0,0	0	0	1,0	0	0	0	1	0	0	1,1	1	1,0	1,1	0	1	0	1	0	0	1	0,0	1
P_{10}	1	1	0,0	1	1	1,0	0	0	0	1	1	1	0,0	0	0,0	1,1	0	1	0	1	0	1	0	0,0	0
P_{11}	0	0	1,1	0	0	0,0	0	1	0	0	0	0	0,0	1	1,0	1,1	0	1	0	0	0	1	0	0,1	0
P_{12}	1	0	1,1	1	0	0,0	0	1	0	1	0	1	1,1	0	0,0	1,0	0	1	1	1	0	0	1	0,1	0
P_{13}	0	1	0,1	1	0	0,1	0	1	1	0	0	1	0,0	1	1,1	1,1	0	1	1	1	0	1	0	0,1	0
P_{14}	1	0	1,1	0	0	1,0	1	1	1	0	0	1	1,1	1	0,0	0,1	0	1	0	0	0	1	1	1,0	0
P_{15}	1	0	0,1	1	0	0,1	1	0	0	1	0	0	1,1	0	0,1	0,1	0	1	0	1	0	1	1	1,1	1
P_{16}	1	0	1,1	0	1	0,0	1	0	1	0	0	1	0,1	1	0,1	1,1	1	1	0	1	0	0	1	0,0	1
P_{17}	1	0	0,1	0	0	1,0	0	1	0	0	0	0	0,1	1	0,0	1,0	0	0	1	1	0	1	1	1,1	1
P_{18}	0	1	1,1	0	0	0,0	0	0	0	1	1	0	0,1	0	1,1	0,1	0	0	0	1	1	0	0	0,0	0
P_{19}	1	0	1,0	1	0	1,0	1	0	0	0	0	0	1,1	0	0,1	0,0	1	1	1	1	1	0	1	0,0	0
P_{20}	0	0	1,1	1	0	1,1	0	0	0	1	0	0	0,0	1	0,0	0,0	1	1	0	0	0	0	1	0,1	0
P_{21}	0	0	0,1	0	1	0,0	0	1	0	0	0	1	0,0	1	1,1	0,0	0	1	0	0	1	1	1	1,1	0
P_{22}	1	1	0,0	0	1	0,0	0	1	0	1	0	1	0,0	1	0,1	0,0	0	0	1	0	0	0	1	0,0	0
P_{23}	0	1	0,0	1	0	1,1	0	0	1	0	1	0	1,1	1	0,1	0,1	1	0	0	1	0	1	1	1,1	0
P_{24}	0	0	1,1	1	0	0,1	1	0	1	1	1	0	0,0	1	0,1	1,1	0	1	1	0	0	1	1	1,1	0
P_{25}	1	0	1,1	1	1	0,0	0	0	1	1	1	0	1,1	0	1,0	1,0	1	1	0	0	0	1	1	1,0	0
P_{26}	0	0	0,0	0	1	1,0	1	1	0	0	0	1	1,1	0	1,1	1,0	1	0	1	1	0	0	0	1,0	0
P_{27}	1	0	1,1	0	0	0,1	0	0	1	0	0	1	1,1	1	1,1	0,1	1	0	0	0	0	1	1	1,0	0
P_{28}	0	1	0,0	1	0	1,1	0	0	0	0	1	1	1,0	0	1,1	0,0	1	0	1	1	1	0	0	0,0	1

Table 5.2: The images of the points on the Elkies curve under ε

6 Further research

One might ask where to go from here. The fact that dependence relations found by using this method need not be verified is one of its major features. The question is: can we use it to find all dependence relations? After computing the images v_i of a set of n points $P_i \in E(\mathbb{Q})$ by the homomorphism ε, we could branch out from all vectors in the kernel of $A = (v_1, \dots, v_n)$. Subsequently, we can de the same when it comes to replacing a point P_i which appeared in some combination $Q = \sum_j c_j P_j$ ($c_j \in \{0, 1\}$) with $c_i = 1$. However, there might be dependence relations which cannot be uncovered in this manner, and this remains a question for further research.

Moreover, in Section 4.2 we mentioned the process described there might not terminate, and in that case we may resort to using heights instead. In (Silverman, 2000), this is only remarked, and no example of such a set of rational points on an elliptic curve is given. It would be interesting to find an explicit example where this occurs, as to find out why the method central to this thesis fails.

Finally, a natural next step would be to try to extend this algorithm to Jacobians J of genus 2 curves over $\mathbb{Q}$. The Jacobian variety of a genus 2 curve is a geometric object on which we can impose an abelian group structure similar to one on the $\mathbb{K}$-rational points of an elliptic curve $E/\mathbb{K}$ (for a field $\mathbb{K}$). It turns out that group $J(\mathbb{Q})$ of rational points on J is finitely generated, by the Mordell-Weil theorem. Finding the rank of $J(\mathbb{Q})$ gives us information about the set of rational points on the genus 2 curve in question, and we can again bound this rank from below by proving a set of points on $J(\mathbb{Q})$ is independent.

Bibliography

Cremona, J. E. (2002, September). On the computation of mordell-weil and 2-selmer groups of elliptic curves. *Rocky Mountain J. Math.*, *32*(3), 953–966.

Cremona, J. E. (2008, October). *Elliptic curves in sage.* Retrieved from `https://pdfs.semanticscholar.org/presentation/92d3/41c1a47e5e8140acf5a170a7e5a0d484a0e8.pdf` (University of Warwick, UK)

Klagsbrun, Z., Sherman, T., & Weigandt, J. (2018, 05). The elkies curve has rank 28 subject only to grh. *Mathematics of Computation*.

Lang, S. (2005). *Undergraduate algebra*. Springer New York.

Mazur, B. (1977, 05). Modular curves and the eisenstein ideal. *Publications Mathématiques de l'IHÉS*, *47*, 33–186.

Pesiri, A. (2007). *The chebotarev density theorem applications* (Unpublished masters thesis, UNIVERSITA DEGLI STUDI ROMA TRE). Retrieved from `http://www.mat.uniroma3.it/users/pappa/sintesi/16_Pesiri.pdf`

Silverman, J. H. (2000, April). The xedni calculus and the elliptic curve discrete logarithm problem. *Des. Codes Cryptography*, *20*(1), 5–40.

Silverman, J. H. (2009). *The arithmetic of elliptic curves* (2nd ed.). Springer New York.

Silverman, J. H., & Tate, J. T. (2015). *Rational points on elliptic curves* (2nd ed.). Springer Publishing Company, Incorporated.

Stoll, M. (2010, February). How to Solve a Diophantine Equation. *ArXiv e-prints*.

Washington, L. C. (2008). *Elliptic curves: Number theory and cryptography* (2nd ed.). Chapman & Hall/CRC.

A Source codes

elldep(E, P)

Remark 1. The program given below has one major shortcoming. As explained in section 2.3, it is necessary to add generators of the 2-torsion subgroup to the list of points, prior to calculating any images by the homomorphism we constructed. A consequence is that we may find a dependence relation that only includes these added points.

With a little bit of work, however, this may be avoided. For instance, we can include a verification step, and re-run the algorithm using different vectors from the kernel of A should the found dependence relation not include any of the supplied rational points. Here A is the matrix with the images of the points by the homomorphism ε as its columns.

```
/* This function determines if a set P of n rational points on an
   elliptic curve E is independent. If not, it returns an explicit dependence
   relation in the form of a vector of coefficients [c1, ..., cn]. If
   depform == 0 (which it is by default), the combination c1*P1 + ... + cn*Pn
   always equates to the identity element. For some purposes this is not
   preferred, in which case we just want to find some relation such that
   c1*P1 + ... + cn*Pn is torsion. In that case, make sure depform == 1. These
   vectors of coefficients are always given with elements without common factors.
   The variables maxprimes and maxit (by default n + 20 and 20, respectively)
   determine how many good primes to consider before attempting to find an
   explicit dependence relation, and how many iterations to perform,
   respectively.

   The output [dep, rhs, deprel] consists of
     - dep: 1 if P is independent, 0 otherwise,
     - rhs: the evaluation of c1*P1 + ... + cn*Pn,
     - deprel: the explicit dependence relation given as a vector of
       coefficients, always a vector of zeros if dep == 1. */
elldep(E, P, depform, maxprimes, maxit) = {
  local(nold, Eold, Pold, n, v, F, D, f, deprel, tors, torspoints, twotors,
    ntwotors, rhs, dep);

  dep = 0;
  nold = #P;
  Eold = E;
  Pold = P;

  /* Check if each point in Pold lies on E */
  for (i = 1, nold,
    if (ellisoncurve(E, P[i]) == 0,
      error("not␣all␣points␣lie␣on␣the␣specified␣elliptic␣curve");
      return(NULL);
    );
  );

  /* Set maxprimes and maxit to default values if nonspecified */
  if (maxprimes == 0, maxprimes = nold + 20);
  if (maxit == 0, maxit = 20);
```

```
/* Determine the complete torsion subgroup. */
torspoints = elltorspoints(E);

/* Determine generators of the 2-torsion subgroup of E, if non-trivial. */
ntwotors = 1;
twotors = vector(0);
for (i = 1, #torspoints,
  if (ellorder(E, torspoints[i]) == 2,
    twotors = concat(twotors, [torspoints[i]]);
  );
);
if (#twotors == 0, twotors = NULL);
if (#twotors == 3, twotors = [twotors[1], twotors[3]]);

/* Keep the original curve and list of points to use later on, and add the
  generators of the 2-torsion subgroup to the list of points. */
if (twotors != NULL, P = concat(P, twotors));
n = #P;

/* Put the curve equation into the form y^2 = F(x) with integer coeff. */
v = [1, 0, -E[1]/2, -E[3]/2];
E = ellchangecurve(E, v);
P = ellchangepoint(P, v);
E = ellintegralmodel(E, &v);
P = ellchangepoint(P, v);

/* lhs of the elliptic curve equation */
F = Pol([1,E[2],E[4],E[5]]);
D = poldisc(F);
f = deriv(F);

/* Store dependence relations. */
relations = matrix(maxit, 3);

for (it = 1, maxit,
  local(goodPr, goodR, kp, A);

  /* Initialization */
  goodPr = vector(0); goodR = vector(0); kp = vector(0);
  A = matrix(n, 0);

  /* Keep adding coordinates to the homomorphism for additional good primes */
  while (matrank(A) < n & #goodPr < maxprimes,
    local(prev, temp, end, p, roots, ncol);

    if (matsize(goodPr)[2] == 0, prev = 3, prev = goodPr[#goodPr]);

    /* Find the next good prime with kp > 0 and store roots of F mod p */
    temp = nextgoodprime(D, F, prev);
    goodPr = concat(goodPr, [temp[1]]);
    goodR = concat(goodR, [temp[2]]);
    kp = concat(kp, [temp[3]]);

    /* Abbreviate to declutter */
    end = #goodPr;
    p = goodPr[end];
    roots = goodR[end];

    /* Resize A */
  if (kp[end] == 1, A = concat(A, vector(n)~), A = concat(A, matrix(n,2)));
  ncol = matsize(A)[2];

  /* Loop through all points P1,...,Pn and update the last column(s) of A */
  for (i = 1, n,
    local(Q, u, w);

    Q = P[i];
    u = numerator(Q[1]);
    w = denominator(Q[2])/denominator(Q[1]);

    if (Mod(u, p) != Mod(roots[1]*w^2, p),
      A[i, ncol - kp[end] + 1] = quadChar(u - roots[1]*w^2, p);
    ,
      A[i, ncol - kp[end] + 1] = quadChar(subst(f,x,roots[1]), p);
    );

    if (kp[end] == 2 ,
      if (Mod(u, p) != Mod(roots[2]*w^2, p),
        A[i, ncol] = quadChar(u - roots[2]*w^2, p);
      ,
        A[i, ncol] = quadChar(subst(f,x,roots[2]), p);
      );
    );
  );
);

/* We can only conclude the points are independent if A has rank A. If A
  does not have rank n, we try to find an explicit dependence relation. */
deprel = NULL;
if (matrank(A) == n,
  deprel = vector(n);
  dep = 1;
,
  local(kervec, combvec, Q, R, k, eq, diff);

  /* Find a vector in the kernel of A~ */
  kervec = matker(A~)[, 1];
  combvec = vector(length(kervec), i, (kervec[i] == Mod(1, 2)));

  /* Construct the first combination G = c1P1 + ... + cnPn. */
  relations[it, 1] = combvec;

  /* Evaluate c1*P1 + ... + cn*Pn */
  Q = ellsum(E, P, combvec);
  relations[it, 3] = Q;


  /* If Q is a torsion points, we have found a dependence relation,
    so we are done. */
  if (ellorder(E, Q) != 0,
    deprel = lincomb(relations, it);
    break;
  );


  /* Check if Q has a torsion difference with some point Q' earlier
    obtained, in which case we have found a dependence relation as well. */
  if (it >= 2,
    eq = 0;
```

```
        /* Find such a point. */
        for (k = 1, it - 1,
          diff = elladd(E, Q, ellneg(E, relations[k, 3]));
          if (ellorder(E, diff) != 0, eq = k; break;););

        /* If such a point has been found, construct the final dependence
          relation and break from the main loop */
        if (eq != 0,
          deprel = 2^(it-1) * (lincomb(relations, it) - lincomb(relations, eq));
          break;
        );
      );


      /* Otherwise, we check if Q is in 2E(Q) by checking if we can halve Q.
        If so, we try to lift the dependence relation from E(Q)/2E(Q). */
      R = elldivbytwo(E, Q, torspoints);
      if (R == NULL,
        /* In this case Q is not in 2E(Q), so the number of good primes is
          not suffient for the homomorphism to be injective. */
        print("Homomorphism␣not␣injective␣for␣[maxprimes]␣good␣primes,");
        print("increase␣[maxit]␣and␣repeat");
        return([NULL, NULL, NULL]);
      ,
        /* Q = c1*P1 + ... + cn*Pn is in 2E(Q), so we replace a point Pi for
          which ci = 1 by R = Q/2 and repeat the process */
        for (i = 1, n, if(combvec[i] == 1, k = i; break;););
        relations[it, 2] = k;
        P[k] = R;
      );
    );
  );
  if (deprel == NULL,
    print("Results␣inconclusive,␣increase␣[maxit].");
    return([NULL, NULL, NULL]);
  );

  /* Divide by any common factors in the dependence vector, and return the
    result. */
  deprel = deprel[1..nold];
  if (dep == 0 & gcd(deprel) != 0, deprel /= gcd(deprel));
  rhs = ellsum(Eold, Pold, deprel);
  if (depform == 0,
    deprel *= ellorder(Eold, rhs);
    rhs = [0];
  );
  return([dep, rhs, deprel]);
}
```

elltorspoints(E)

```
/* Compute the torsion subgroup of E from elltors(E). Note this may be
  shortened using Mazur's theorem. */
elltorspoints(E) = {
  local(tors, torspoints);
  tors = elltors(E);
  if (tors[1] == 1,
    torspoints = [[0]];
  ,
    torspoints = elltorspointshelper(E, elltors(E), 1);
  );
  return(torspoints);
}

elltorspointshelper(E, tors, index) = {
  local(torspoints, Q, new, newQlist);

  torspoints = vector(0);

  /* Base step */
  if (index == length(tors[2]),
    for (i = 0, tors[2][index] - 1,
      Q = ellmul(E, tors[3][index], i);
      torspoints = concat(torspoints, [Q]);
    );

  , /* Recursive step */
  new = elltorspointshelper(E, tors, index + 1);
    for (i = 0, tors[2][index] - 1,
      Q = ellmul(E, tors[3][index], i);
      newQlist = vector(#new, k, elladd(E, Q, new[k]));
      torspoints = concat(torspoints, newQlist);
    );
  );

  return(torspoints);
}
```

ellsum(E, P, v)

```
/* Evalulates v1*P1 + ... + vn*Pn on E for a list of points P and a vector
  of coefficients v. */
ellsum(E, P, v) = {
  if (v == NULL, return(NULL));
  local(Q, n);

  n = min(length(P), length(v));
  Q = if (v[1] != 0, ellmul(E, P[1], v[1]), [0]);

  for (i = 2, n,
    if (v[i] != 0, Q = elladd(E, Q, ellmul(E, P[i], v[i])));
  );

  return(Q);
}
```

nextgoodprime(D, F, q)

```
/* Finds the next good prime p after q with kp != 0, the roots of F mod p  in
  Z/pZ and kp, where D is the discriminant of F. */
nextgoodprime(D, F, q) = {
  local(p, roots, kp);
  roots = vector(0);
  p = q + 1;

  /* Find the next good prime p with kp != 0 */
  while (Mod(6*D, p) == Mod(0, p) || #roots == 0,
    p = nextprime(p + 1);
    roots = polrootsmod(F,p);
  );

  kp = (#roots == 1) + 2*(#roots == 3);
  return([p, roots, kp]);
}
```

quadChar(x, p)

```
/* Returns 1 if x is a quadratic residual mod p, 0 otherwise */
quadChar(x, p) = {
  if (kronecker(lift(x), p) == -1, return(Mod(1, 2)), return(Mod(0, 2)))
}
```

elldivbytwo(E, Q, tors)

```
/* This is a simplification of the more general divideByTwo algorithm from
  Appendix G in (Silverman, 2000) to curves given by an affine
  equation of the form y^2 = x^3 + a2x^2 + a4x + a6.

  Find R such that Q = [2]R on E, or return NULL if no such R exists,
  here tors is the complete torsion sugroup of E, not to be confused with
  elltors(E). */
elldivbytwo(E, Q, tors) = {
  local(a1, a2, a3, a4, a6, alp, bet, b2, b4, b6, b8, G, x, y);
  [a1, a2, a3, a4, a6] = E[1..5];
  [alp, bet] = Q;

  /* Now a1 = a3 = 0. */
  b2 = 4*a2;
  b4 = 2*a4;
  b6 = 4*a6;
  b8 = 4*a2*a6 - a4^2;

  G = Pol([1, -alp*4, -(b4 + alp*b2), -(2*b6 + 2*alp*b4), -(b8 + alp*b6)]);
  x = findrr(G);

  if (x == NULL,
    return(NULL);
  ,
    local(c0, c1, c2);
    c2 = -3*alp;
    c1 = -(2*a2*alp + a4);
    c0 = -(a4*alp + 2*a6);

    /* In case bet = 0, Q is a 2-torsion point, so we must
      check if there is a 4-torsion point R such that 2R = Q. */
    if (bet != 0,
      y = (x^3 + c2*x^2 + c1*x + c0) / (2*bet + a1*alp + a3);
    ,
      local(flag);
      flag = 0;
      for (i = 1, #tors,
        if (ellord(E, tors[i]) == 4,
          if (ellmul(E, tors[i], 2) == Q,
            [x, y] = tors[i];
            flag = 1;
            break;
          );
        );
      );
      if (flag == 0, return(NULL));
    );
    return([x, y]);
  );
}
```

findrr(F)

```
/* Find a rational root of F, or return NULL if f has no rational roots */
findrr(F) = {
  local(k, factors, f);

  k = 0;
  factors = factor(F);

  for (i = 1, matsize(factors)[1],
    if (poldegree(factors[i, 1]) == 1, k = i; break;);
  );

  if (k == 0,
    return(NULL);
  ,
    f = factors[k, 1];
    return(-polcoeff(f, 0)/polcoeff(f, 1));
  )
}
```

lincomb(relations, iteration)

```
/* Constructs a relation Q = c1P1 + ... + cnPn from a sequence of relations
  Q(i) = c1(i)P1(i) + ... + cn(i)P1(i) in 'relations', where 'iteration' is
  the index of the last iteration step. */
lincomb(relations, iteration) = {
  local(n, k, curr, prev, g, incr);
  n = length(relations[1, 1]);
  k = matsize(relations)[1];
  g = relations[1 .. iteration - 1, 2];
  incr = vector(n);

  /* Base case */
  if (iteration == 1,
    return(relations[1, 1]);

  , /* Recursive step */
    curr = relations[iteration, 1];

    /* Loop through each coefficient */
    for (i = 1, n,
      local(index);

      /* Find the most recent iteration where Pi was replaced,
        or verify that Pi has not been replaced*/
      index = 0;
      forstep(j = iteration - 1, 1, -1,
        if (i == g[j], index = j; break;);
      );

      /* If in fact a Pi was replaced, adjust the combination appropriately. */
      if (index != 0,
        /* This is where the recursion takes place */
        prev = lincomb(relations, index);

        prev *= curr[g[index]]/2;
        curr[g[index]] = 0;
        incr += prev;
      );
    );
    curr += incr;
  );

  return(curr);
}
```