Arithmetic Aspects of Elliptic Curves

David Bodiu
bodiud@tcd.ie

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

School of Mathematics
Trinity College Dublin,
College Green, Dublin 2

March 2022

Abstract

The theory of elliptic curves is both vast and profound spanning several fields and areas in mathematics. In this treatise we confine ourselves to approaching the subject in a predominantly-algebraic fashion resorting to some geometry and analysis whenever deemed instructive or necessary. After providing motivations and laying the necessary groundword we examine the unexpected group law for elliptic curves and briefly discuss its analogue for the related singular curves. Afterwards, we divide the remaining investigation into two broad segments: the more tractable finite order points and the remaining points of infinite order, culminating in a procedure for determining the general structure of the group of rational solutions for any elliptic curve over $\mathbb{Q}$. The procedure may also be duly extended to provide a complete generating set if required.

Contents

1 Background and History

For the purposes of this short historical summary one can assume that an expression resembling "y^2 = cubic polynomial" indicates an elliptic curve. Before we begin, it should be noted that this manuscript does not treat the subject of elliptic curves over the complexes and the associated topic of elliptic functions, however, the history of our work is closely tied to it, therefore we include some developments related to it for completeness.

3rd century: The first recorded instance of an elliptic curve appears (unsurprisingly) in Diophantus' Arithmetica. In the 24th problem of book IV he finds rational solutions to the curve $y(6-y) = x^3 - x$.

13th century: Fibonacci enconters a problem related to elliptic curves at the court of the Holy Roman Emperor Frederick II, specifically, finding a rational number r such that $r^2 - 5$ and $r^2 + 5$ are both rational squares. The origins of this question actually date back to certain Arabic manuscripts from the 8th century.

17th century: Bachet translates Arithmetica from Greek into Latin with an appendix containing Fibonacci's problem above. It also contains an interesting original result regarding rational solutions to the elliptic curve $y^2 = x^3 + c$.

17th century (again): Around 10 years later Fermat acquires a copy of the translation above in whose margin he makes his famous comment. The related problem will resurface later. Fermat's collected works also include numerous references to problems involving elliptic curves such as $y^2 = x^3 - 2$.

17th century (again): Newton begins to classify cubic curves, including those of the form $y^2 = ax^3 + bx^2 + cx + d$. He provides a geometric interpretation for the methods employed by Diophantus and Bachet when finding rational solutions to their respective problems. This would ultimately lead to the formulas for adding points on elliptic curves.

18th century: Euler acquires a copy of Fermat's collected works and verifies many of his hypotheses, including (at least) two regarding elliptic curves. He also works on the

congruent number problem—a generalized version of Fibonacci's problem above—still related to elliptic curves.

19$^{\text{th}}$ century: Jacobi points out a possible connection between cubic curves and elliptic functions. Around 10 years later Eisenstein provides a proof verifying this. Around 20 years later Clebsch introduces the idea of parameterizing cubic curves by elliptic functions, and Weierstrass adapts an addition formula for elliptic functions to these cubic curves.

20$^{\text{th}}$ century: Poincaré publishes a celebrated paper unifying many of the previous ideas mentioned. Mordell, Hasse and Weil continue to make significant contributions to the subject. Andrew Wiles and Richard Taylor provide a proof of Fermat's Last Theorem [Wil95], in which elliptic curves play a prominent role.

21$^{\text{st}}$ century: Elliptic curves begin to enter widespread use as a cryptographic method. Amongst many others, a currently popular area of research revolves around determining whether the "rank" of an elliptic curve is bounded or not. We will encounter this concept in one of the later sections below.

2 Introduction

2.1 Motivation

We begin our foray into the field of elliptic curves by first considering a seemingly innocuous question: Is it possible to find three consecutive numbers, whose product forms a square? If such numbers exist, how many can we find? Algebraically, we're asking for solutions to the equation $y^2 = x(x+1)(x+2)$, and geometrically we're looking for points on the curve defined by the equation above.

We begin by first looking for such solutions in the "largest" domain, that is, in $\mathbb{C}$. It shouldn't take too long to figure out that the problem can be solved quite easily if we assume knowledge of one of the most ubiquitous theorems in complex analysis: the Fundamental Theorem of Algebra.

Indeed, let x be any complex number of choice. Then the expression $y^2 - x(x+1)(x+2)$ becomes a quadratic polynomial in $\mathbb{C}$ with exactly two roots by the aforementioned result, which correspond to two solutions of the equation in $\mathbb{C}$. Since the choice of x is arbitrary, one deduces that there are infinitely many solutions in this domain, in fact an uncountably infinite number of solutions.

If we now restrict our field of vision, we can consider the problem in $\mathbb{R}$, where the answers may not be the same. In this domain we can now provide an illustration of the curve traced out by the given equation:

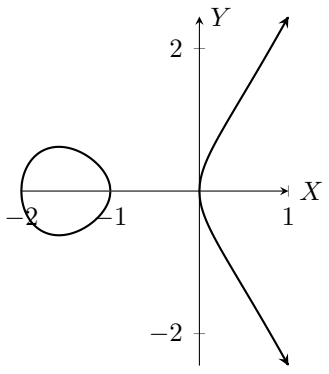


Figure 2.1

The graph of the curve certainly presents some interesting features, however, it need not be consulted any further in this case since the problem has a complete algebraic

solution.

The manner in which the problem is solved is nearly the same but with some additional alterations. Let $x \in \mathbb{R}$ satisfy $x \geq 0$. Then $x(x+1)(x+2) \geq 0$ and we can take the square root of both sides to obtain $y = \pm\sqrt{x(x+1)(x+2)}$, which yields two solutions for any particular value of $x \geq 0$. Since, the range which we can choose x from is infinite, we once again end up with an (uncountably) infinite set of solutions.

Placing even further restrictions, we find ourselves in $\mathbb{Q}$. The method employed for the previous two domains can no longer be applied here: we're not guaranteed to end up with rational solutions after applying it (as it involves taking square roots). However, there are clearly some "obvious" rational solutions, namely $(-2, 0)$, $(-1, 0)$ and $(0, 0)$. Are there any other rational solutions besides these though? Since we're at the beginning of our journey we might try a computer search, but we'd be out of luck. These are in fact the only rational solutions to the equation.

We might try to take a look at other equations of the form $y^2 = x(x+n)(x+2n)$, but we'd find ourselves in a very similar situation to the one above when $n < 5$. Upon letting $n = 5$ though, our computer finds the first non-obvious solution: $(-9, 6)$. The other obvious solutions to the equation $y^2 = x(x+5)(x+10)$ would be $(-10, 0)$, $(-5, 0)$ and $(0, 0)$. We could try to setting our computer loose again in order to find more rational solutions but we notice something interesting about the graph.

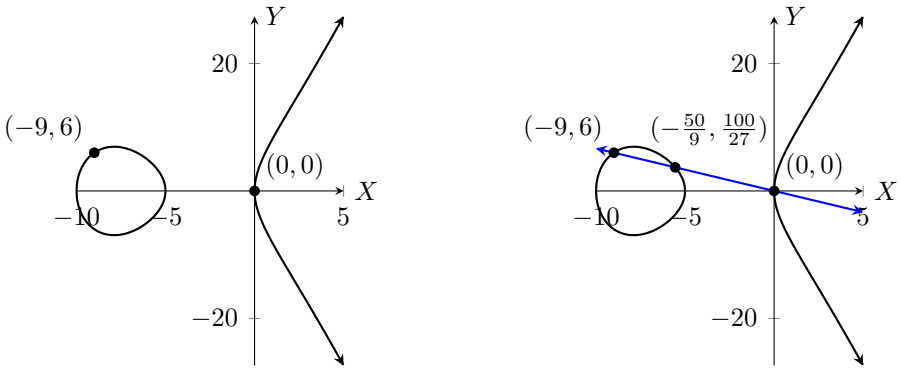


Figure 2.2

If we draw a line through the obvious point $(0, 0)$ and the non-obvious point $(-9, 6)$ we intersect the curve at a new point. We can check if this point is rational by doing a little algebra. The equation of the line passing through our two points is $y = -\frac{2}{3}x$.

Subbing this into our elliptic curve equation we get

$$(-\frac{2}{3}x)^2 = x^3 + 15x^2 + 50x \implies x^3 + \frac{131}{9}x^2 + 50x = 0.$$

If a cubic has three distinct roots x_1, x_2, x_3 then the coefficient of the x^2 term will be $-(x_1 + x_2 + x_3)$. Since we already have two of the roots we can easily find the third. In particular, we can see that the third root will also be rational

$$-(0 - 9 + x_3) = \frac{131}{9} \implies x_3 = -\frac{50}{9}.$$

To find the y coordinate we just plug in x_3 into the line equation to obtain $y_3 = \frac{100}{27}$. We've just been able to find a new rational point on the curve by using two previously known rational points! If you're wondering why we didn't try this earlier with the obvious rational points it's because you need at least one non-obvious point for the method to work.

We can use the method above with any two known points to obtain another rational point on the elliptic curve. However, there is no guarantee that the resulting rational point will always be new. It could very well happen that after a while, all our combinations of known rational points yield nothing new. We do not have a method yet for determining the size of the solution set.

Having said that, we've definitely made some steps in the right direction, but before we go any further we'd like to formalise and place everything above in a more general context. We'll begin by defining elliptic curves.

2.2 Definitions

Definition 2.1. An *elliptic curve* E over a field K is defined by the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in K$ such that the curve is non-singular.

The form of equation above is usually referred to as the *Generalized Weierstrass Equation* for an elliptic curve, but can be readily simplified if the characteristic of the field K is neither 2 nor 3.

Indeed, suppose that the characteristic of K is not 2. We divide the equation by 2 and complete the square to obtain

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(\frac{a_3^2}{4} + a_6\right).$$

Relabelling the bracketed terms above we then have

$$y_1^2 = x^3 + a_2'x^2 + a_4'x + a_6'.$$

Furthermore, suppose that the characteristic of K is not 3 either. Effecting the substitution $x = x_1 - \frac{a_2'}{3}$ and performing some relabelling again yields

$$y_1^2 = x_1^3 + Ax_1 + B.$$

Finally, for simplicity, we remove the now-unnecessary subscripts to get

$$y^2 = x^3 + Ax + B$$

with $A, B \in K$. The equation above is referred to as the *Weierstrass equation* for an elliptic curve and is the form which will be used throughout most of this discourse.

Example 2.1. Since we're currently interested in $K = \mathbb{Q}$ which does not have characteristic 2 nor 3 we shall be able to express any elliptic curve over $\mathbb{Q}$ in the form displayed above. In particular the curve $y^2 = x(x+5)(x+10)$ can be transformed to $y^2 = x^3 - 25x$. □

Notice also that since the transformation from the Generalized Weierstrass equation to the Weierstrass equation is linear, old rational points correspond to new rational points on the transformed curve and vice versa. In particular, finding rational solutions to the Generalized Weierstrass equation for a particular elliptic curve is equivalent to finding rational solutions for the corresponding Weierstrass equation.

For the remainder of this discourse we shall assume that the field which we are working over is $\mathbb{Q}$ and that curves are in their corresponding Weierstrass equation unless stated otherwise.

3 The Group Law

3.1 Addition

The procedure outlined in the in the first section for generating a third rational point from two previously known rational points is formally known as *addition*. More generally, if we know two points P and Q on some elliptic curve E, then we can obtain a third point $P + Q = R$ by the line method described above. Well, nearly. This isn't quite the definition of adding points on elliptic curves. We need to carry out one

more crucial step. Once the third point is obtained, it is reflected through the x-axis. This is always possible since elliptic curves are symmetric about the x-axis (take the square root of both sides of the equation). There are a few reasons for taking this last step, but primarily it's because it turns out that this modified operation allows us to define a group structure on the set of all rational points on the curve. We will turn our attention to this important result shortly.

Having now defined addition for distinct poins, one should begin to wonder whether there is a corresponding natural definition for adding a point to itself. That is, if $P = Q$, then what should $P + Q$ look like? Fortunately, there is a very natural way of defininining this, namely, imagine the point $Q \neq P$ creeping slowly towards P on the elliptic curve E. The line going through both of these points then tends to the tangent of the elliptic curve at the point P. Consequently, $P + P$ should equal the reflection of the point on the elliptic curve through which the tangent line at the point P passes through. The graph below should make this last statement a little bit clearer.

Another pertinent question one should be asking is whether there exists a point resembling 0 on the curve, that is, whether there exists a point Q, such that for all points P on the curve, $P + Q = P$. The short and deflating answer is that there are no such points. However, using a little bit of projective geometry we can define a point at infinity (denoted ∞) which non-intuitively lies simultaneously at the "very" top and at the "very" bottom of the graph. For an intuitive explanation of this unusual phenomenon see [Spe96]. Geometrically, any vertical line on the graph will intersect this point at infinity.

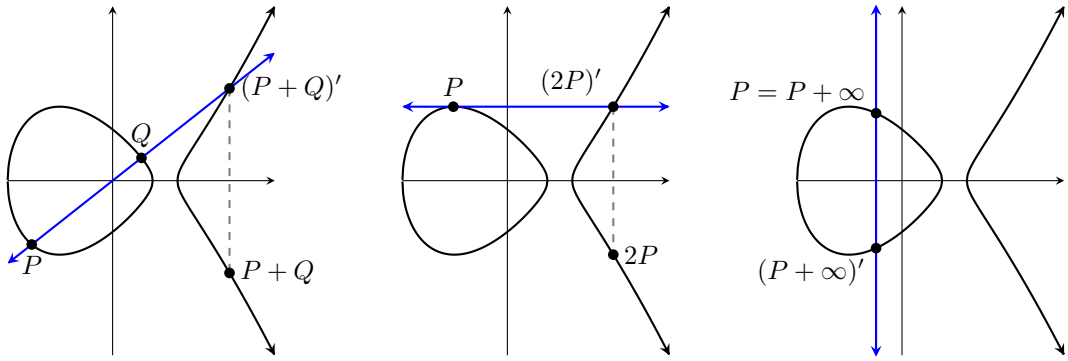


Figure 3.1

Now that we're done with the particulars of defining addition on an elliptic curve, we can figure out the general form of the resulting point.

Lemma 3.1. *(Addition formulae) Let E be an elliptic curve of the form $y^2 = x^3 + Ax + B$. Suppose that we know two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on the curve satisfying $P_1, P_2 \neq \infty$. Let $P_3 = (x_3, y_3)$ be the resulting point of $P_1 + P_2$. Then:*

1. If $x_1 \neq x_2$, we have

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m\,(x_1 - x_3) - y_1, \quad m = \frac{y_2 - y_1}{x_2 - x_1}.$$

2. If $x_1 = x_2$ but $y_1 \neq y_2$, then $P_1 + P_2 = \infty$.

3. If $P_1 = P_2$ and $y_1 \neq 0$, we have

$$x_3 = m^2 - 2x_1, \quad y_3 = m\,(x_1 - x_3) - y_1, \quad m = \frac{3x_1^2 + A}{2y_1}.$$

4. If $P_1 = P_2$ and $y_1 = 0$, then $P_1 + P_2 = \infty$.

Proof. 1.If $x_1 \neq x_2$, then the slope of the line passig through P_1 and P_2 is $m = \frac{y_2 - y_1}{x_2 - x_1}$. Subbing the line into the equation for the elliptic curve we get

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B \implies x^3 - m^2x^2 + ... = 0.$$

Notice that the x coordinates of P_1 and P_2 satisfy the equation above when plugged in because they lie on both the curve and the line. We now use the fact that the coefficient of the second order term of a monic cubic is the sum of its roots multiplied by negative one. In our case this means that $-(x_1 + x_2 + x_3) = -m^2$. Since we already know x_1 and x_2 we can just rearrange to get $x_3 = m^2 - x_1 - x_2$. To finish off, we sub in x_3 to get $y_3 = m\,(x_1 - x_3) - y_1$.

2. If $x_1 = x_2$ but $y_1 \neq y_2$ then P_2 is the reflection of P_1 in the x-axis. Consequently, the line passing through both of them is vertical and therefore intersects the curve at ∞. Reflecting the point ∞ over the x-axis we get ∞ again.

3. If $P_1 = P_2$ and the y coordinate is nonzero, we are looking for the tangent to the point P_1 on the curve. To obtain this we need to find the slope first. If we perform some implicit differentiation on the equation of the elliptic curve we obtain

$$2y\frac{dy}{dx} = 3x^2 + A \implies m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}$$

We can then perform the exact same steps as for part 1, with x_1 as a double root (since line is tangent at P_1 rather than intersecting) to obtain $x_3 = m^2 - 2x_1$ and $y_3 = m(x_1 - x_3) - y_1$.

4. We can see from the implicit differentiation carried out in part 3 that the tangent to any point with y coordinate will be infinte. This just means that the tangent line is vertical. Consequently, the third point of intersection is ∞ and reflecting this across the x-axis we get ∞ again. ■

The case when either of the points is ∞ is trivial. Moreover, notice that we have also demonstrated that the sum of any two rational points on an elliptic curve results in another rational point on the elliptic curve, as alluded to earlier. Technically though, this is true only if we treat the point ∞ as a rational point also, which we shall assume henceforth.

3.2 Addition as a Group Operation

We now formally state our assumption from the preceding section:

Definition 3.1. Let E be an elliptic curve over $\mathbb{Q}$ of the form $y^2 = x^3 + Ax + B$. Then

$$E(\mathbb{Q}) = \left\{(x, y) \in \mathbb{Q} \times \mathbb{Q} \mid y^2 = x^3 + Ax + B\right\} \cup \{\infty\}$$

that is, $E(\mathbb{Q})$ denotes the set of all rational points on the curve E along with the point at infinity.

We've seen from Lemma 3.1 that the sum of two rational points on an elliptic curve yields another rational point, that is, if $P, Q \in E(\mathbb{Q})$ then $P + Q \in E(\mathbb{Q})$. At this instance, we may begin considering whether $(E(\mathbb{Q}), +)$ might form a group. It turns out that it actually does.

Lemma 3.2. *Let E be an elliptic curve over $\mathbb{Q}$ of the form $y^2 = x^3 + Ax + B$. Then $(E(\mathbb{Q}), +)$ forms a group.*

Proof. Closure is implied by Lemma 3.1. For the identity we have the point at infinity. Now dealing with inverses, given any point P on $E(\mathbb{Q})$, we can define $-P$ to be the reflection of the point P through the x-axis. This ensures that the line passing through P and $-P$ is vertical which in turn gives $P + (-P) = \infty$. The last property which remains to be verified is associativity, that is, whether

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

holds. Unfortunately, the proof of this property is not so straightforward and spans several pages. We refer the interested reader to [Fri17]. ■

To compensate for the lack of proof with regards to the associativity property above, the reader may find it interesting to note that if we let the symbol $\oplus$ denote the operation of basic addition, that is, without reflection across the x-axis then the following are tantamount

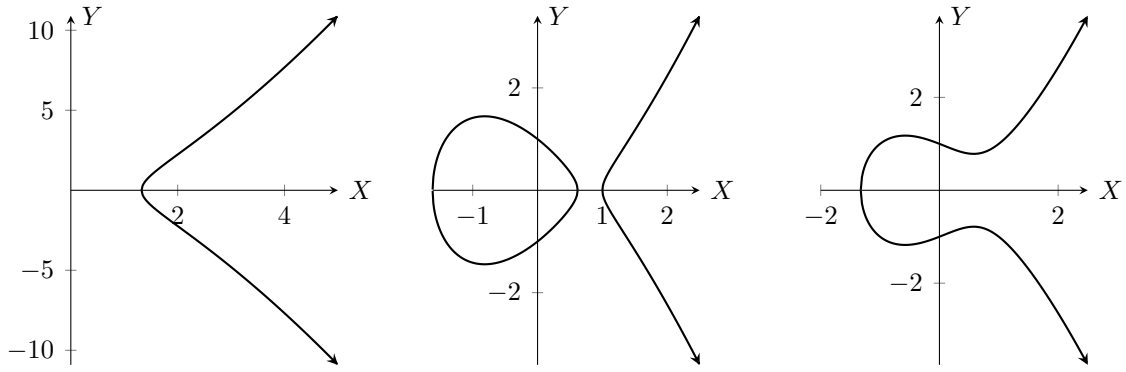
$$(P+Q)+R = P+(Q+R) \iff (P \oplus Q) \oplus -R = -P \oplus (Q \oplus R).$$

which provides a corresponding semi-associative rule for the $\oplus$ operation, and also demonstrates why $\oplus$ is not associative in general, thereby disqualifying $(E(\mathbb{Q}), \oplus)$ from forming a group.

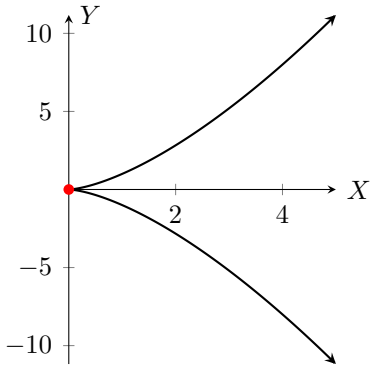
From here on we shall use $E(\mathbb{Q})$ to denote the group $(E(\mathbb{Q}), +)$ in order to simplify notation. The fact that $E(\mathbb{Q})$ turns out to be a group will prove to be of invaluable help in the work that follows. Before moving on to the next section one should also notice that $E(\mathbb{Q})$ is in fact abelian. This follows from the fact that for any two points P, Q on the elliptic curve E, the line passing through the points P and Q is same as that passing through the points Q and P.

3.3 Addition on Singular Curves

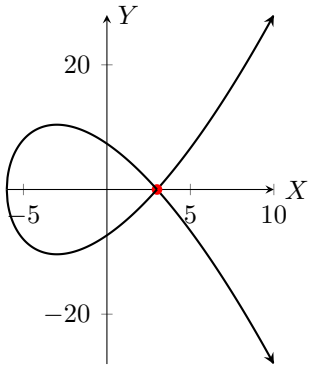
Before moving on, it is important to be able to distinguish between singular and non-singular cubic curves. By Definition 2.1 the former are not elliptic curves.



(a) $y^2 = x^3 - x - 1$ (b) $y^2 = x^3 - 2x + 1$ (c) $y^2 = x^3 - x + 1$



(d) $y^2 = x^3$



(e) $y^2 = x^3 - 27x + 54$

Figure 3.2

The first three cubic curves contain no singularities and are therefore elliptic curves. The last two cubic curves both contain singularities at the red points and as such are not elliptic curves. Assuming that our cubic curve is in Weierstrass form, there is a simple method for determining whether the cubic curve is non-singular, that is, whether it is an elliptic curve.

Lemma 3.3. *A curve $y^2 = x^3 + Ax + B$ is singular if and only if the discriminant of the cubic is zero, that is, $4A^3 + 27B^2 = 0$.*

Proof. Let $F(x, y) = y^2 - (x^3 + Ax + B)$ denote the implicit function for an elliptic curve E. By definition, a point P on the curve is singular if the partial derivatives F_y and F_x at the point P are both zero. We have $F_y = 2y$ and $F_x = 3x^2 + A$. Setting these both equal to zero gives $y = 0$ and $F_x = 0$.

First, notice that if $y = 0$ then plugging this into the equation of the curve we get $x^3 + Ax + B = 0$. Secondly, notice that $F_x = 0$ if and only if $\frac{d}{dx}(x^3 + Ax + b) = 0$. We therefore have that the cubic itself and its derivative are both zero at the point of singularity. This is true if and only if there is a double root present, which means that the discriminant of this cubic must be zero, that is, $4A^3 + 27B^2 = 0$.

The other direction is easily obtained by traversing back up the argument. ■

Example 3.1. The curve $y^2 = x^3$ displayed in fourth figure above has $A, B = 0$ so it's clearly singular. On the other hand, the corresponding Weierstrass equation of

$y^2 = x(x+5)(x+10)$ is $y^2 = x^3 - 25x$ which is nonsingular since $(-25)^3 \neq 0$. □

The method above is useful if the curve is given in Weierstrass form. However, one can look at the partial derivatives directly also, which may be more convenient sometimes than transforming a curve into Weierstrass form and then applying the result above.

Example 3.2. The implicit function for the last curve in the grid above is $F(x, y) = y^2 - x^3 - x^2$. We have $F_y = 2y$ and $F_x = -3x^2 - 2x$. Setting these both equal to 0 we obtain the singular point $(0, 0)$, which implies that this curve is singular. □

Example 3.3. The implicit equation of $y^2 = x(x+5)(x+10)$ is $F(x, y) = y^2 - x^3 - 15x^2 - 50x$, and $F_x = -3x^2 - 30x - 50$, $F_y = 2y$. Setting these both equal to 0 again yields no points on the curve, which means that the curve is non-singular. □

In what follows we shall concern ourselves very briefly with determining some properties of singular curves analogous to those which will be studied for non-singular elliptic curves.

Using elements in the proof of Lemma 3.3, we know that a cubic curve in Weierstrass form is singular only if $y = 0$ and the corresponding cubic has at least a double root. Since a cubic has at most three roots, the curve will be singular when we have either a double or triple root. We consider these two cases separately.

Suppose that the curve has a triple root at $y = 0$. Then $y^2 = (x - a)^3$ which becomes $y^2 = x^3$ after a change of coordinates with singularity at $(0, 0)$. Consider the set

$$E_N(K) = \{(x, y) \in K \times K \mid y^2 = x^3, (x, y) \neq (0, 0)\} \cup \{\infty\}$$

of non-singular points on the curve. Then $E_N(K) = (E_N(K), +)$ actually forms a group where the operation "$+$" is the aformentioned elliptic curve addition. Checking for identity and inverses is trivial. Associativity can be generalised from $\mathbb{Q}$ to any arbitrary field K, and for closure we just need to ensure that the sum of two points is never $(0, 0)$. However, by examining the graph (see Figure 3.2 (d)) or doing the required algebra, it is not difficult to see that any line passing through $(0, 0)$ can only intersect at most one other point on the curve. Consequently, since we cannot have a line passing through $(0, 0)$ and two other distinct points on the curve, no two points can sum to give $(0, 0)$, demonstrating closure. We therefore obtain that $E_N(K)$ is a group. We have the following theorem concerning the structure of $E_N(K)$ [Was08]:

Theorem 3.4. *Let E a curve over a field K defined by $y^2 = x^3$. Then the map*

$$\begin{aligned} \psi : \quad & E_N(K) \to K \\ & \infty \mapsto 0, \quad (x, y) \mapsto \frac{x}{y} \end{aligned}$$

is a group isomorphism, where K is regarded as a group under addition. ■

For the second scenario, a double root implies a curve of the form $y^2 = (x+a)(x+b)^2$ which by a simple change of coordinates becomes $y^2 = x^2(x+c)$ (see Figure 3.2 (e)). We define $E_N(K)$ correspondingly for this curve E which also turns out to be a group. The following theorem demonstrates this and gives the possible structures for $E_N(K)$ [Was08]:

Theorem 3.5. *Let E be a curve over a field K defined by $y^2 = x^2(x+c)$ with $c \neq 0$. Define $\gamma = \sqrt{c}$. Define the map*

$$\begin{aligned} \psi : \quad & E_N(K) \to K(\gamma)^\times \\ & \infty \mapsto 1, \quad (x, y) \mapsto \frac{y + \gamma x}{y - \gamma x}. \end{aligned}$$

1. If $\gamma \in K$, then ψ is a group isomorphism where $K^\times$ is regarded as a group under multiplication.
2. If $\gamma \notin K$, then ψ induces a group isomorphism

$$E_N(K) \cong \left\{ u + \gamma v \mid u, v \in K, u^2 - cv^2 = 1 \right\}$$

where the right-hand side is regarded as a group under multiplication. ■

The results above demonstrate that removing the corresponding singularities from each curve ensures that the remainings set of solutions $E_N(K)$ forms a group. In particular we have that $E_N(\mathbb{Q})$ forms a group for each singular curve. It should be noted however, that although $E_N(\mathbb{Q})$ and $E(\mathbb{Q})$ form groups with exactly same operation for their respective singular and non-singular curves, our results in the following sections will demonstrate that their structures are in fact quite different.

4 Points of Finite Order

4.1 Torsion Subgroup

From the previous section, we now know that $E(\mathbb{Q})$ forms a group for our elliptic curve $y^2 = x(x+5)(x+10)$. Recall that our primary goal was finding whether the set of

solutions to the elliptic curve E, that is, $E(\mathbb{Q})$, is finite or infinite. To solve this we split $E(\mathbb{Q})$ into two: the set of points with finite order and the set of points with non-finite order. In this section we concentrate on the former.

Definition 4.1. Let E be an elliptic curve over $\mathbb{Q}$ of the form $y^2 = x^3 + Ax + B$ and let $E(\mathbb{Q})$ be the set of all rational points on this curve. We define

$$E_T(\mathbb{Q}) = \{P \in E(\mathbb{Q}) \mid \exists n \in \mathbb{N} : nP = \infty\}$$

to be the set containing all points in $E(\mathbb{Q})$ which have finite order. $E_T(\mathbb{Q})$ is called the *torsion subgroup* of $E(\mathbb{Q})$. Henceforth, we refer to points of finite order as *torsion points*.

Lemma 4.1. *Let E be an elliptic curve over $\mathbb{Q}$ of the form $y^2 = x^3 + Ax + B$. Then $E_T(\mathbb{Q})$ is a subgroup of $E(\mathbb{Q})$.*

Proof. We can just check the group axioms one by one. We obviously have $\infty \in E_T(\mathbb{Q})$. Furthermore, we obtain associativity (and commutativity) for free since $E_T(\mathbb{Q}) \subset E(\mathbb{Q})$. This allows us to prove the next property. For inverses, if $nP = \infty$ then taking the inverse of both sides we obtain $-nP = n(-P) = \infty$ also. For closure, if $P_1, P_2 \in E_T(\mathbb{Q})$ then $nP_1 = mP_2 = \infty$, which means that $nm(P_1 + P_2) = \infty$, demonstrating that $P_1 + P_2$ must be an element of $E_T(\mathbb{Q})$ also. ■

Example 4.1. Recall the elliptic curve $y^2 = x(x + 1)(x + 2)$. We stated that the only rational points on this curve were the obvious $(0, 0), (-1, 0)$ and $(-2, 0)$. To check whether any of these are torsion points we might look at multiples of each point. Indeed, it's not difficult to see that for any of the preceding rational points P we have $2P = \infty$. This follows either from a direct calculation using Lemma 3.1 or by simply drawing the tangent to each of the points on the curve.

The point ∞ is obviously a torsion point also, but we did not have any notion of such a point in the beginning. As a result, for this elliptic curve E we have that $E_T(\mathbb{Q}) = E(\mathbb{Q}) = \{(0, 0), (-1, 0), (-2, 0), \infty\}$. Futhermore, by playing around with the elements, or by noticing that $|E_T(\mathbb{Q})| = 4$ and that three of the elements have order 2 we can deduce that $E_T(\mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. □

In the example above we were handed $E(\mathbb{Q})$. Moreover, $E(\mathbb{Q})$ and hence $E_T(\mathbb{Q})$ were known to be finite, however, we don't know whether this will the case in general. Ideally, we'd like to find a method which enables us to find the torsion points in $E(\mathbb{Q})$ without any of these assumptions, which is what we set out to do now.

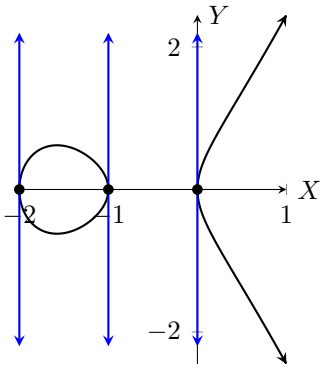


Figure 4.1

4.2 The Lutz-Nagell Theorem

Definition 4.2. Let x, y be relatively prime integers. Consider the rational number $\frac{x}{y} = p^r \frac{x'}{y'}$, where the prime p does not divide $x'y'$. We define the *p-adic valuation* to be

$$v_p\left(\frac{x}{y}\right) = r.$$

We also define $v_p(0) = \infty$.

Example 4.2. Let $q = \frac{5^2}{3}$. Then $v_3(q) = -1$, $v_5(q) = 2$ and $v_p(q) = 0$ for all other primes p. □

Definition 4.3. Let E be an elliptic curve of the form $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$. Then for any positive integer r and prime p we define

$$E_{p,r} = \{(x, y) \in E(\mathbb{Q}) \mid v_p(x) \leq -2r, v_p(y) \leq -3r\} \cup \{\infty\}.$$

In other words, $E_{p,r}$ is the set of rational points on the curve E whose x coordinate has at least p^{2r} in it's denominator, and whose y coordinate has at least p^{3r} in its denominator.

Convention: In what follows, we write $d \mid q$ for some rational number q, if d divides the numerator of q. Similarly, we also write $d \equiv r \pmod{p}$ if the r is the remainder after dividing the numerator of q by d.

Lemma 4.2. *Let E be an elliptic curve given by $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$. If $(x, y) \in E(\mathbb{Q})$ then $v_p(x) < 0$ if and only if $v_p(y) < 0$. If the previous is true, then there also exists a positive integer r such that $v_p(x) = -2r$ and $v_p(y) = -3r$.*

Proof. Since $y^2 = x^3 + Ax + B$ we must have that the denominator of the left-hand side must equal the denominator of the right-hand side. Using this, along with the fact that $A, B \in \mathbb{Z}$, we can see that p divides the denominator of y if and only if it divides the denominator of x. This proves the first part.

Now, let a be the greatest positive integer for which p^a divides the denominator of y. Then we must have that p^{2a} divides the denominator of y^2 exactly. Similarly, if b is the greatest positive integer such that p^b divides the denominator of x, then p^{3b} must divide $x^3 + Ax + B$ exactly. Consequently, we must have that $2a = 3b$, which implies that $a = 3r$ and $b = 2r$ for some positive integer r. By hypothesis, this now means that p^{3r} divides the denominator of y and p^{2r} divides the denominator of x. ■

Lemma 4.3. *Let E be an elliptic curve given by $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$. Define the variables $t = \frac{x}{y}$ and $s = \frac{1}{y}$. Then, the point $(x, y) \in E(\mathbb{Q})$ belongs to $E_{p,r}$ if and only if $p^{3r} \mid s$. If $p^{3r} \mid s$ then $p^r \mid t$.*

Proof. It's not difficult to see that $(x, y) \in E_{p,r}$ implies $p^{3r} \mid s$. On the other hand, suppose that $p^{3r} \mid s$. Then by definition, $p^3 r$ divides the denominator of y. By Lemma 4.2 it therefore follows that p^{2r} divides the denominator of x. For the second part, if $p^{3r} \mid s$ then by definition $p^3 r$ divides the denominator of y. Applying Lemma 4.2 again we obtain the result. ■

Lemma 4.4. *Let E be an elliptic curve given by $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$. Define the variables $t = \frac{x}{y}$ and $s = \frac{1}{y}$. A line $t = c$ with $c \in \mathbb{Q}$ satisfying $c \equiv 0 \pmod{p}$, intersects the curve $s = t^3 + As^2t + Bs^3$ in at most one point (s, t) such that $s \equiv 0 \pmod{p}$. If it exists, the line is not tangent at this point of intersection.*

Proof. Suppose not. Then there exist two distinct values $s_1 \neq s_2$ such that $s_1 \equiv s_2 \equiv 0 \pmod{p}$. This is the base case for the induction process. Suppose that $s_1 \equiv s_2 \pmod{p^k}$ for some $k > 1$. We wish to show that it then holds for $k + 1$. Let $s_i = ps_i'$. Then $s_1' \equiv s_2' \pmod{p^{k-1}}$ which implies that ${s_1'}^2 \equiv {s_2'}^2 \pmod{p^{k-1}}$. It then follows that $s_1^2 = p^2 {s_1'}^2 \equiv p^2 {s_2'}^2 = s_2^2 \pmod{p^{k+1}}$. In the same manner, $s_1^3 \equiv s_2^3 \pmod{p^{k+2}}$ which implies $s_1^3 \equiv s_2^3 \pmod{p^{k+1}}$. As a result we have that

$$s_1 = c^3 + Acs_1^2 + Bs_1^3 \equiv c^3 + Acs_2^2 + Bs_2^3 = s_2 \pmod{p^{k+1}}$$

which completes the induction. Now choosing k such that $p^k > s_1, s_2$ we obtain $s_1 \equiv s_2 \pmod{p^k}$ which implies that $s_1 = s_2$, which is a contradiction. Hence, there exists at

most one point (s,t) of intersection between the line and elliptic curve satisfying $s \equiv 0 \pmod{p}$.

For the second part we begin by finding the slope of the tangent line to the elliptic curve. We obtain this by implicit differentiation of the elliptic curve equation with respect to the variable t (the analogue of x). After rearranging everything we get

$$\frac{ds}{dt} = \frac{3t^2 + As^2}{1 - 2Ast - 3Bs^2}$$

Assume now that the line $t = c$ really is tangent to the curve at (s,t). Since this is a vertical line we must have that $1 - 2Ast - 3Bs^2 = 0$. However $s \equiv t \equiv 0 \pmod{p}$ implies that $1 - 2Ast - 3Bs^2 \equiv 1 \not\equiv 0$ which is a contradiction, and the result follows. ■

Definition 4.4. Let E be an elliptic curve given by $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$. Then for any positive integer r and prime p we define

$$\begin{aligned} \lambda_{p,r} : E_{p,r}/E_{p,5r} &\to \mathbb{Z}_{p^{4r}} \\ (x,y) &\mapsto p^{-r}x/y \pmod{p^{4r}} \\ \infty &\mapsto 0 \end{aligned}$$

where $\mathbb{Z}_{p^r}$ is a group under addition.

Lemma 4.5. *Let E be an elliptic curve given by $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$. If $(x,y) \in E_{p,r}$ but $(x,y) \notin E_{p,r+1}$ we have $\lambda_{p,r}(x,y) \not\equiv 0 \pmod{p}$.*

Proof. Notice that

$$\{(x,y) \in E_{p,r} \mid v_p(x) = -2r, v_p(y) = -3r\} = \{(x,y) \in E_{p,r} \mid v_p(x/y) = r\}.$$

This is the set of points which are in $E_{p,r}$ but not in $E_{p,r+1}$. Therefore $\lambda_{p,r}(x,y) = p^{-r}(p^r x'/y') = x'/y'$ with $p \nmid x'y'$ which implies that $\lambda_{p,r}(x,y) \not\equiv 0 \pmod{p}$. ■

Proposition 4.6. *Let E be an elliptic curve given by $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$. Suppose that P_1, P_2 are points in $E_{p,r}$ and let $P_1 + P_2 = \bar{P_3} = -P_3$, that is, $P_1 + P_2 + P_3 = \infty$. Then $P_3 \in E_{p,r}$ and*

$$\lambda_{p,r}(P_1) + \lambda_{p,r}(P_2) + \lambda_{p,r}(P_3) \equiv 0 \pmod{p^{4r}}$$

Proof. Begin by dividing $y^2 = x^3 + Ax + B$ by y^3 to get

$$\frac{1}{y} = \frac{x^3}{y^3} + A \cdot \frac{x}{y} \cdot \frac{1^2}{y^2} + B \cdot \frac{1^3}{y^3}.$$

Making the substitutions $t = \frac{x}{y}$ and $s = \frac{1}{y}$ we get $s = t^3 + Ats^2 + Bs^2$. Next, suppose that $P_1, P_2, P_3 \in E(\mathbb{Q})$, $P_1, P_2 \in E_{p,r}$ lie on the line given by $ax + by + d = 0$. Dividing by y and making our prior substitution again we obtain $at + b + ds = 0$. The dual of the points $P_i = (x_i, y_i)$ are the $P_i' = (s_i, t_i)$, which lie on the line just obtained.

Using a little projective geometry it can be shown that the order of intersection of the initial line and elliptic curve at a point P_i, is the same as that of the transformed line and transformed elliptic curve at the point P_i'. The order of intersection at a point P is essentially the multiplicity of the root at this point, when the equation for the line and elliptic curve are combined into one. Therefore "clean" intersections and tangent lines in the variables x, y correspond to "clean" intersections and tangent lines respectively in the variables s, t. As a result, we can do apply the addition formulae in the variables s, t instead of x, y.

Next, suppose that the coefficient of s in the line equation is zero, so that it takes the form $t = \frac{-b}{a} = c$, with $c \in \mathbb{Q}$. By hypothesis this line passes through the points $P_1', P_2' \in E_{p,r}$. Turning to Lemma 4.3 we get that $p^{3r} \mid s_1, s_2$ and $p^r \mid t_1, t_2$ which means that $s_i, t_i \equiv 0 \pmod{p}$. Applying Lemma 4.4, there can only be one point with $s_i \equiv 0$ which implies that $P_1 = P_2$. This means that the line is tangent to the curve at this point. A second application of Lemma 4.4 insists that the line cannot be tangent to the curve at such a point, which is a contradiction.

Since $d \neq 0$ we divide across by it to obtain a line of the form $s = \alpha t + \beta$. One can consider the cases $t_1 = t_2$ and $t_1 = t_2$ (applying Lemma 4.4 to the former) to obtain that

$$\alpha = \frac{t_2^2 + t_1 t_2 + t_1^2 + As_2^2}{1 - A\left(s_1 + s_2\right) t_1 - B\left(s_2^2 + s_1 s_2 + s_1^2\right)}$$

By hypothesis, $p^r \mid t_i$, from which it follows that the numerator of α is congruent to zero modulo p^{2r}. However, since we do not know whether the fraction is in it's lowest terms, to secure this result we need to check whether the denominator is divisible by p. Recall that $s_1 \equiv s_2 \equiv 0 \pmod{p}$. As a result the denominator of α is congruent to 1 modulo p, which means it's not divisible by p. Therefore, $\alpha \equiv 0 \pmod{p^{2r}}$ indeed. Combining this with the fact that $p^{3r} \mid s_i$ and $p^r \mid t_i$ we also obtain that $\beta \equiv s_i - \alpha t_i \equiv 0 \pmod{p^{3r}}$.

We now turn our attention to finding the coordinates (s_3, t_3) of the point P_3'. Since this points lies on the intersection of the transformed line with the transformed elliptic curve, we can make the required substitution to obtain

$$t^3 + \frac{2A\alpha\beta + 3B\alpha^2\beta}{1 + B\alpha^3 + A\alpha^2}t^2 + ... = 0.$$

We now reuse the method from Lemma 3.1: the sum of the roots of this equation is equal to negative one times the coefficient of the t^2 term. More explicitly we have that

$$t_1 + t_2 + t_3 = -\frac{2A\alpha\beta + 3B\alpha^2\beta}{1 + B\alpha^3 + A\alpha^2}.$$

The denominator is not divisible by p therefore, as explained above, we need not worry whether the fraction is in it's lowest terms when viewing it modulo any power of p. Since we've just obtained that $p^{2r} \mid \alpha$ and $p^{3r} \mid \beta$, the right hand side is congruent to zero modulo p^{5r}, that is

$$t_1 + t_2 + t_3 \equiv 0 \pmod{p^{5r}}.$$

A consequence of this congruence is $t_1 + t_2 + t_3 \equiv 0 \pmod{p}$. Since $P_1, P_2 \in E_{p,r}$ we have that $p \mid t_1, t_2$ which implies that $t_3 \equiv 0 \pmod{p}$. This now allows us to easily verify the fact that $s_3 = \alpha t_3 + \beta \equiv 0 \pmod{p^{3r}}$, which by a change of coordinates demonstrates that $P_3 \in E_{p,r}$ also.

To prove the last part, we use the fact just obtained (in order to apply the map to P_3) along with the congruence again to get

$$\lambda_r(P_1) + \lambda_r(P_2) + \lambda_r(P_3) \equiv p^{-r}t_1 + p^{-r}t_2 + p^{-r}t_3 \equiv p^{-r}(t_1 + t_2 + t_3) \equiv 0 \pmod{p^{4r}}$$

which demonstrates the required congruence relation. ■

Corollary 4.7. *Let E be an elliptic curve given by $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{Z}$. Then for any positive integer r and prime p, $E_{p,r}$ is a subgroup of $E(\mathbb{Q})$.*

Proof. We check all the group axioms: We have the identity by definition. Associativity follows from the fact that $E_{p,r} \subset E(\mathbb{Q})$. It's also not difficult to see that $-P = (x, -y) \in E_{p,r}$ if and only if $P = (x, y) \in E_{p,r}$. Closure follows immediately from Proposition 4.6. ■

Corollary 4.8. *Let E be an elliptic curve given by $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{Z}$. Then for any positive integer r and prime p the map $\lambda_{p,r}$ is a monomorphism.*

Proof. First notice that

$$\lambda_{p,r}(-(x,y)) = \lambda_r(x,-y) = -p^{-r}x/y = -\lambda_{p,r}(x,y)$$

that is, $\lambda_{p,r}(-P) = -\lambda_{p,r}(P)$. Suppose that P_1, P_2 are points in $E_{p,r}$ and $P_1 + P_2 = P_3' = -P_3$. Then the image of $P_1 + P_2$ is

$$\lambda_{p,r}\left(P_1 + P_2\right) = \lambda_r\left(-P_3\right) = -\lambda_{p,r}\left(P_3\right) = \lambda_{p,r}\left(P_1\right) + \lambda_{p,r}\left(P_2\right)$$

where the last equality follows from Proposition 4.6. This proves that the map is a homomorphism. To show that the homomorphism is injective, note that if $\lambda_{p,r}(x,y) \equiv 0 \pmod{p^{4r}}$, then $v_p(x/y) \geq 5r$, which means that $(x,y) \in E_{p,5r}$. This demonstrates that the kernel of $\lambda_{p,r}$ is trivial. ■

Corollary 4.9. *Let E be an elliptic curve given by $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$ and p be a prime. If $n \neq p^k, k > 0$, then $E_{p,1}$ contains no points of order exactly n.*

Proof. Suppose the contrary. Then there exists a point $P \in E_{p,1}$ of order $n = p^k n'$, where $k \geq 0$ and $p \nmid n'$. If we multiply P by p^k we obtain a point P' whose order is coprime to p. Suppose that r is the largest integer for which $P \in E_{p,r}$. Then

$$n\lambda_{p,r}(P) = \lambda_{p,r}(nP) = \lambda_{p,r}(\infty) \equiv 0 \pmod{p^{4r}}$$

From the congruence above, since $p \nmid n$ we have that $\lambda_{p,r} \equiv 0 \pmod{p^{4r}}$ which by definition of the map implies that $P \in E_{p,5r}$. However since we assumed r was the largest integer, $5r > r$ provides a contradiction and the result follows. ■

Theorem 4.10 (Lutz-Nagell)**.** *Let E be an elliptic curve of the form $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$, and let $P = (x,y)$ be a point on the curve. If P has finite order then $x, y \in \mathbb{Z}$. Moreover, if $y \neq 0$ then y^2 divides the discriminant, that is, $y^2 \mid 4A^3 + 27B^2$.*

Proof. Suppose the first part is false. Then there exists a point $P = (x,y)$ on $E(\mathbb{Q})$ with either x or y not in $\mathbb{Z}$. This means that x or y is in $\mathbb{Q}$, so we can assume that there is some prime p dividing the denominator of one. Consequently, by Lemma 4.2, $P \in E_{p,r}$ for some positive integer r which implies that $P \in E_{p,1}$. Suppose next that q is a prime which divides the order of n of P. This means that the order of the point $Q = \frac{n}{q}P$ is q. Consequently, Q is also a member of the group $E_{p,1}$ since it's a multiple of P. Using Corollary 4.9 we therefore obtain that $q = p$. Now choose an integer j such

that $Q \in E_j, Q \notin E_{j+1}$. This means that $\lambda_{p,j}(Q) \not\equiv 0 \pmod{p}$. However, we also have that $p\lambda_{p,j}(Q) = \lambda_{p,j}(pQ) \equiv 0 \pmod{p^{4j}}$, which means that $\lambda_{p,j}(Q) \equiv 0 \pmod{p^{4j-1}}$ implying that $\lambda_{p,j}(Q) \equiv 0 \pmod{p}$, a contradiction. As a result, we must have that the coordinates of any torsion point on the curve $E(\mathbb{Q})$ are integral.

For the second part, by Lemma 3.1, if $y \neq 0$ then $2P \neq ft$. By hypothesis, $P = (x, y)$ has finite order implies the same for $2P = (x', y')$. By the part proven above, this means that $x', y' \in \mathbb{Z}$. Using Lemma 3.1 again we can obtain x' explicitly in terms of x, y:

$$x' = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4y^2}$$

Since x' is an integer this means that y^2 divides the numerator $x^4 - 2Ax^2 - 8Bx + A^2$. Moreover, since $y^2 = x^3 + Ax + B$ we know that y^2 will divide $c_1(x^4 - 2Ax^2 - 8Bx + A^2) + c_2(x^3 + Ax + B)$ for any integers c_1, c_2. Setting $c_1 = 3x^2 + 4A$ and $c_2 = (-3x^2 + 5Ax + 27B^2)$ yields the result. ■

Example 4.3. We can now retackle the example from Section 4.1 without making any of the previous assumptions. As before, let E be the elliptic curve defined by the equation $y^2 = x(x + 1)(x + 2) = x^3 + 3x^2 + 2x$. To use the theorem above, we first need to transform this into its corresponding Weierstrass equation by effecting the substitution $x = x' - 1$ (given in Section 2.1), to obtain $y^2 = x'^3 - x'$. It is not difficult to show that torsion points on this curve are in bijection with torsion points on the initial curve.

If $y = 0$ we have the points $(0, 0), (1, 0), (-1, 0)$. It can be easily verified that these are torsion points. If $y \neq 0$ then the discriminant is $4(-1)^3 - 27(0)^2 = -4$. The values of y for which $y^2 \mid -4$ are $y = \pm 2$. If we sub these into the equation for the curve and solve for x, we do not obtain any integer values. By Theorem 4.10, since $x' \notin \mathbb{Z}$ it follows that these points are not finite. We've now eliminated all possibilities which means that $E_T(\mathbb{Q}) = \{(0, 0), (1, 0), (-1, 0), \infty\}$.

If we apply the inverse transformation $(x' = x + 1)$ to go back to the original elliptic curve we obtain $E_T(\mathbb{Q}) = \{(0, 0), (-1, 0), (-2, 0), \infty\}$ in accordance with Example 4.1. As we've already worked out: $E_T(\mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. □

Example 4.4. We now find the torsion points for the curve $y^2 = x(x + 5)(x + 10)$. Converting this to its corresponding Weierstrass equation we get $y^2 = x^3 - 25x$. Setting $y = 0$ we obtain the points $(0, 0), (5, 0), (-5, 0)$.

If $y \neq 0$, then by Theorem 4.10 we have $y^2 \mid 4(-25)^3 - 27(0)^2 = -(2 \cdot 5^3)^2$, which then implies that $y \mid 2 \cdot 5^3$. Unfortunately, none of the values yield a point with integer coordinates. After applying the inverse coordinate transformation, this means that $E_T(\mathbb{Q}) = \{(0,0), (0,-5), (0,-10), \infty\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ again. □

Example 4.5. Consider the elliptic curve E defined by $y^2 = x^3 + 1$. If $y = 0$ then we obtain the torsion point $(-1, 0)$. For $y \neq 0$ we must have that $y^2 \mid 4(0)^3 - 27(1)^2 = -27$, that is, $y \mid 3$ so that $y \in \{\pm 1, \pm 3\}$. It turns out that each one of these possibilities corresponds to an integer point on the curve, namely $(0, \pm 1)$ and $(2, \pm 3)$. To check if they are torsion we look at some small multiples and find that $3 \cdot (0, \pm 1) = \infty$ and $6 \cdot (2, \pm 3) = \infty$. Also, after checking the interactions between the points our suspicions concerning the structure of $E(\mathbb{Q})$ are confirmed and we have $E(\mathbb{Q}) = \{(-1, 0), (0, \pm 1), (2, \pm 3), \infty)\} \cong \mathbb{Z}_6$. □

It's not difficult to see that the Lutz-Nagell procedure ensures that $E_T(\mathbb{Q})$ is always finite. We can state this result formally, for any curve E over $E(\mathbb{Q})$:

Lemma 4.11. *Let E be an elliptic curve of the form $y^2 = x^3 + Ax + B$ over $\mathbb{Q}$. Then $E_T(\mathbb{Q})$ is finite.*

Proof. If the coefficients A, B are not integers, a suitable change of coordinates ($x \to x/c^2, y \to x/c^3$ and then multiplying across by c^6) produces new coefficients $A', B' \in \mathbb{Z}$. One can check that torsion points on the initial curve correspond to torsion points on the transformed curve, and vice versa. Therefore, it is sufficient to prove the result for the transformed curve.

If $y = 0$, then there are at most three corresponding x values (by solving for the remaining cubic). By Theorem 4.10, if $y \neq 0$, there are only finitely many values of y such that y^2 divides the discriminant. For each of these, there are again at most three correspoding x values. Therefore, $E_T(\mathbb{Q})$ is finite. ■

4.3 Structure

Although the Lutz-Nagell Theorem provides a deterministic procedure for identifying finite rational points on an elliptic curve, it can benefit from some improvement. If the coefficients A, B are large it can be very time-consuming to search for all possible integral points. However, since $E_T(\mathbb{Q})$ is a group we could take multiples and combinations of points to find new points. Although this extension is much more efficient than the original method, we cannot, at any stage, be certain that we have managed to find

all the torsion points. However, if we deduced the structure of $E_T(\mathbb{Q})$ beforehand, the problem is solved, and the extension becomes viable.

The following theorem places some convenient limits on the structure of $E_T(\mathbb{Q})$. Recall that $E(\mathbb{Q})$ is an abelian group. Consequently, the subgroup $E_T(\mathbb{Q})$ is also an abelian group. Moreover, by Lemma 4.11 it is also finite (see conditions in theorem below). The original proof can be found in [Kro70]:

Theorem 4.12. *Let T be a finite abelian group. Then*

$$T \cong \mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p_n^{k_n}}$$

with each component a cyclic group under addition. ■

The lemma above is extremely useful as it eliminates a sea of possibilities for the structure of $E(\mathbb{Q})$, however, it does not provide us with a method for obtaining the specifics. To obtain this we do a little more supplementary work.

Lemma 4.13. *Let E be an elliptic curve of the form $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$. Assume that p is an odd prime and that it does not divide the discriminant. Define the map*

$$\rho_p : E_T(\mathbb{Q}) \to E(\mathbb{Z}_p)$$

to be the reduction modulo p map. Then $\rho(P) = \infty$ implies that $P = \infty$.

Proof. The first condition ensures that the discriminant is non-zero modulo p, which by Lemma 3.3 guarantees that the curve is non-singular modulo p. If $P \neq \infty$ then by Theorem 4.10 it has integral coordinates and $\rho(P) \neq \infty$. Consequently, it is only possible to have $\rho(\infty) = \infty$. ■

In particular, we have demonstrated that for suitable p, the group homomorphism ρ_p is an injection. As a result, the order of $E_T(\mathbb{Q})$ will have to divide the order of $E(\mathbb{Z}_p)$. We use this fact to our advantage in the example below.

Example 4.6. Suppose we wish to find the torsion subgroup of $y^2 = x^3 - 432x + 8208$. A quick calculation shows that the primes which divide the discriminant are $2, 3$ and 11. We begin with the smallest prime which we can use. Therefore, consider $E(\mathbb{Z}_5)$. A rapid computer search gives $E(\mathbb{Z}_5) = \{(3, 2), (3, 3), (4, 2), (4, 3)\}$. Of course, we must also include the point ∞ by definition, which means that the order of $E(\mathbb{Z}_5)$ is 5. As a result, the order of $E_T(\mathbb{Q})$ must also divide 5, which in turn implies that $E_T(\mathbb{Q})$ is trivial or $E_T(\mathbb{Q}) \cong \mathbb{Z}_5$.

Now that we've found the structure of $E_T(\mathbb{Q})$, we can use Theorem 4.10. If we find at least one non-trivial point we'll be able to generate the rest because of the group structure. Otherwise we'll have to unfortunately search through all possibilities to reach the conclusion that $E_T(\mathbb{Q})$ is trivial.

By the theorem, $y^2 \mid 4(-432)^3 + 27(8202)^2 = (2^4)^2 \cdot (3^6)^2 \cdot 11$. As a result we must have $y \mid 2^4 \cdot 3^6$. Next, running our computer search we obtain the point $P = (-12, 108)$. We calculate $5P = \infty$ which confirms that this point is indeed torsion. We can now use this point to generate the remaining torsion points: $2P = (24, -108), 3P = (24, 108), 4P = (-12, -108)$. Summing everything up, we have

$$E_T(\mathbb{Q}) = \{(-12, 108), (-12, -108), (24, 108), (24, -108), \infty\} \cong \mathbb{Z}_5.$$

□

Theorem 4.12 is a result about finite abelian groups in general, and although it places some helpful constraints on the structure, the number of possible structures are still infinite. However, if we let $G = E(\mathbb{Q})$ one can obtain (after much laborious work) the following useful result [Maz77] [MG78]:

Theorem 4.14 (Mazur's Theorem)**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then $E_T(\mathbb{Q})$ is isomorphic to one of the below:*

$$\mathbb{Z}_n \text{ with } 1 \leq n \leq 10 \text{ or } n = 12;$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_{2n} \text{ with } 1 \leq n \leq 4.$$

In particular, there are only finitely many possibilities for the structure of $E(\mathbb{Q})$. ■

The motivation behind all of our investigations thus far have been borne from the question posed at the beginning, that is, whether the set of rational points on the curve defined by $y^2 = x(x + 5)(x + 10)$ was finite or not. We figured out previously that $(9, -6)$ lies on the curve. However, now that we know all the torsion points (see Example 4.4), we can deduce that $(9, -6) \notin E_T(\mathbb{Q})$. Consequently, adding the point $(9, -6)$ to itself repeatedly will always yield new rational points on the curve, from which it follows that $E(\mathbb{Q})$ is infinite.

Recall that at the beginning of Section 4.1 we anticipated that it would be necessary to study both the torsion and non-torsion parts of $E(\mathbb{Q})$ to answer our initial question. Although the results in this section have demonstrated otherwise, there may be plenty value remaining in studying the non-torsion part of $E(\mathbb{Q})$ also.

5 Points of non-Finite Order

5.1 The Weak Mordell-Weil Theorem

In the previous section we were concerned with finding a list of all the torsion points. Since $E_T(\mathbb{Q})$ turns out to be finite, this was fine. Unfortunately, here we cannot expect to be able to list an infinite number of points. What would be feasible, however, would be to list the generators if they exist. If there are an infinite number of generators then this is unfortunate as well, but we first find out whether this is the case. Also, instead of considering $E(\mathbb{Q}) - E_T(\mathbb{Q})$ it is actually more conventient to just consider $E(\mathbb{Q})$ as a whole, since the latter set is only bigger by a finite number of elements and also has the convenient property of being a group. We first show that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

To begin with, suppose that E is an elliptic curve over $\mathbb{Q}$ of the form $y^2 = (x-e_1)(x-e_2)(x-e_3)$ with $e_1, e_2, e_3 \in \mathbb{Z}$. If we assume more generally that $a, b, c \in \mathbb{Q}$ then a suitable change of coordinates provides a new curve E' with $e_1', e_2', e_3' \in \mathbb{Z}$. Moreover, even if $e_1, e_2, e_3 \notin \mathbb{Q}$ the arguments will still work out, which ensures that the results below hold for all elliptic curves over $\mathbb{Q}$, however, we refrain from describing this case. Supposing then that $x, y \in \mathbb{Q}$ and $e_1, e_2, e_3 \in \mathbb{Z}$. Then we can write

$$\begin{aligned} x - e_1 &= au^2 \\ x - e_2 &= bv^2 \\ x - e_3 &= cw^2 \end{aligned}$$

with $a, b, c \in \mathbb{Q}$. We can now rearrange the original equation to obtain

$$\left(\frac{y}{uvw}\right)^2 = abc.$$

Since abc is a square, we can divide both sides by its denominator to get

$$\left(\frac{y}{u'vw}\right)^2 = a'b'c'$$

with $a', b', c' \in \mathbb{Z}$. Therefore we may make the assumption that a, b, c are square-free integers to begin with.

Definition 5.1. Let E be an elliptic curve of the form $y^2 = (x-e_1)(x-e_2)(x-e_3)$ with $e_1, e_2, e_3 \in \mathbb{Z}$. We define

$$S = \{p \mid p \text{ is prime and } (e_1 - e_2)(e_1 - e_3)(e_2 - e_3) \text{ is divisible by } p\}$$

to be the set of primes which divide the pairwise differences of e_1, e_2, e_3.

Lemma 5.1. *Let E be an elliptic curve of the form $y^2 = (x-e_1)(x-e_2)(x-e_3)$ with $e_1, e_2, e_3 \in \mathbb{Z}$. If $p \mid abc$ then $p \in S$.*

Proof. If $p \mid abc$ then p divides a, b or c. Assume without loss of generality that $p \mid a$. Since a is square-free, we must have that p^k with k odd is the exact power of p dividing $x - e_1$.

If $k = -k' < 0$ then $p^{-k'} \mid x - e_1$. Since e_1, e_2 are integers, we can find an integer n such that $e_1 + n = e_2$. As a result, $x - e_1 - n = x - e_2$. Since $p^{-k'} \mid x - e_1$ we have that $p^{-k'} \mid x - e_1 - \frac{p^{k'}n}{p^{k'}} = x - e_2$. By a similar argument we also have that $p^{-k'} \mid x - e_3$. Putting everything together, we must have that $p^{3k} = p^{-3k'} \mid y^2$ exactly, which is clearly a contradiction. This means that we cannot have $k < 0$.

Assume then that $k > 0$. Then we can write $x \equiv e_1 \pmod{p}$. As a result we have that $x - e_2 \equiv e_1 - e_2 \pmod{p}$ and $x - e_3 \equiv e_3 - e_1 \pmod{p}$. By the argument above, we saw that if one of the factors $x - e_i$ had p in their denominator, then all the factors had p in their denominators. By the contrapositive, since $x - e_1$ does not have p in its denominator, neither do the other two factors. Therefore, if $p \notin S$ then $p \nmid (x-e_2)(x-e_3)$. As a result we must have that $p^k \mid y^2 = (x-e_1)(x-e_2)(x-e_3)$ exactly, which is a contradiction since k is odd. It follows that $p \in S$. ∎

Notice that since $(e_1 - e_2)(e_2 - e_3)(e_3 - e_1)$ has a finite number of prime factors, S is finite and therefore the possible combinations of a, b, c must also be finite.

Definition 5.2. Let E be an elliptic curve given by $y^2 = (x-e_1)(x-e_2)(x-e_3)$ with $e_1, e_2, e_3 \in \mathbb{Z}$. Define

$$\varphi : E(\mathbb{Q}) \to \left(\mathbb{Q}^\times/\mathbb{Q}^{\times 2}\right) \oplus \left(\mathbb{Q}^\times/\mathbb{Q}^{\times 2}\right) \oplus \left(\mathbb{Q}^\times/\mathbb{Q}^{\times 2}\right)$$

$$\begin{aligned}
(x, y) &\mapsto (x - e_1, \quad x - e_2, \quad x - e_3) \qquad \text{when } y \neq 0 \\
\infty &\mapsto (1, \quad 1, \quad 1) \\
(e_1, 0) &\mapsto ((e_1 - e_2)(e_1 - e_3), \quad e_1 - e_2, \quad e_1 - e_3) \\
(e_2, 0) &\mapsto (e_2 - e_1, \quad (e_2 - e_1)(e_2 - e_3), \quad e_2 - e_3) \\
(e_3, 0) &\mapsto (e_3 - e_1, \quad e_3 - e_2, \quad (e_3 - e_1)(e_3 - e_2))
\end{aligned}$$

to be the map which maps point each to a corresponding triple $(x - e_1, x - e_2, x - e_3)$ modulo squares. When $x = e_i$, or equivalently, when $y = 0$, we have to modify the ith component so that interacts well with the rest of the map, in other words, we want to obtain Theorem 5.2.

Theorem 5.2. *Let E be an elliptic curve given by $y^2 = (x - e_1)(x - e_2)(x - e_3)$ with $e_1, e_2, e_3 \in \mathbb{Z}$. Then the map φ defined above is a homomorphism. Moreover, we have $ker(\varphi) = 2E(\mathbb{Q})$.*

Proof. Suppose that $P_i = (x_i, y_i)$ is a triple of points with $y_i \neq 0$, which all lie on E and on the line $y = ax + b$. Subbing the line into the equation for the elliptic curve E we obtain

$$(x - e_1)(x - e_2)(x - e_3) - (ax + b)^2 = 0$$

Since we know that the points P_i lie on both the curve and the line we therefore have that

$$(x - e_1)(x - e_2)(x - e_3) - (ax + b)^2 = (x - x_1)(x - x_2)(x - x_3)$$

Next, letting $x = e_i$ the equation above becomes

$$(x_1 - e_i)(x_2 - e_i)(x_3 - e_i) = (ae_i + b)^2$$

where the right-hand side is clearly an element of $\mathbb{Q}^{\times 2}$. As a result, the above will be congruent to 1 when viewed modulo $\mathbb{Q}^{\times 2}$. Using the definition of the map we obtain

$$\varphi(P_1)\varphi(P_2)\varphi(P_3) = ((ae_1 + b)^2, (ae_2 + b)^2, (ae_3 + b)^2) \equiv (1, 1, 1) = 1.$$

Moreover, notice that for any component φ_i in the triple we have $\varphi_i \equiv \varphi_i^{-1}$ because $\varphi_i = \varphi_i^2 \cdot \varphi_i^{-1}$. As a result $\varphi(P_3) \equiv \varphi(P_3)^{-1}$. Then using the congruence above we have

$$\varphi(P_1)\varphi(P_2) \equiv \varphi(P_3)^{-1} \equiv \varphi(P_3) \equiv \varphi(-(P_1 + P_2)) \equiv \varphi(P_1 + P_2)$$

where the last congruence follows from the assumption that the elliptic curve is in Weierstrass form as usual, before it is factored as per the hypothesis. As a result reflecting across the x-axis has no effect on the x variable and the calculations remain unchanged. We have thus demonstrated the first assertion in the case that $y \neq 0$.

Suppose that P_1, P_2 are points where $y_1, y_2 = 0$. Since there are only a finite number of such possible points (three to be precise), a case by case check confirms the hypothesis under these circumstances.

Lastly, consider the case where P_1, P_2 are points subject to $y_1 = 0$ and $y_2 \neq 0$. Assume without loss of generality that $P_1 = (e_1, 0)$. Considering these two points only, the restriction of the map φ to φ_2, φ_3 is the same for both cases $y = 0$ and $y \neq 0$. Since we have proven the case for $y \neq 0$ above this takes care of φ_2, φ_3. To take care of the remaining case, notice that $\varphi_1(P)\varphi_2(P)\varphi_3(P) = 1$, which implies

$\varphi_2(P)\varphi_3(P) = \varphi_1^{-1}(P) = \varphi_1(P)$. Then using the fact that φ_2, φ_3 are already known to be homomorphisms

$$\varphi_1(P_1 + P_2) = \varphi_2(P_1 + P_2)\varphi_3(P_1 + P_2) = \varphi_2(P_1)\varphi_3(P_1)\varphi_2(P_2)\varphi_3(P_2) = \varphi_1(P_1)\varphi_1(P_2)$$

which completes the first part of the proof.

For the second part of the theorem we prove only the first inclusion: notice that $\varphi(2P) = \varphi(P + P) = \varphi(P)\varphi(P) = \varphi(P)^2 \equiv 1$. As a result we have that for any $P \in E(\mathbb{Q})$, $2P$ belongs to the kernel of φ. ■

Theorem 5.3 (Weak Mordell-Weil Theorem)**.** *Let E be an elliptic curve of the form $y^2 = (x - e_1)(x - e_2)(x - e_3)$. Then $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.*

Proof. As discussed beforehand, we consider the case where $e_1, e_2, e_3 \in \mathbb{Q}$, however, the result holds in general. If $e_1, e_2, e_3 \in \mathbb{Q}$, then a suitable change of coordinates gives us $e_1', e_2', e_3' \in \mathbb{Z}$. Therefore we assume that $e_1, e_2, e_3 \in \mathbb{Z}$ to begin with. Using Theorem 5.2 we have that the $\ker(\varphi) = 2E(\mathbb{Q})$. Consequently, the map

$$E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow \left(\mathbb{Q}^\times/\mathbb{Q}^{\times 2}\right) \oplus \left(\mathbb{Q}^\times/\mathbb{Q}^{\times 2}\right) \oplus \left(\mathbb{Q}^\times/\mathbb{Q}^{\times 2}\right)$$

will be an injection since its kernel is trivial. By Lemma 5.1 there are only finitely many combinations of triples (a, b, c). Since the image is contained in this set of possibilities, it follows that the image of φ is finite and therefore $E(\mathbb{Q})/2E(\mathbb{Q})$ must also be finite. ■

Example 5.1. In the previous section we worked out that $E(\mathbb{Q})$ was infinite for the elliptic curve $y^2 = x(x + 5)(x + 10)$. In particular, since the point $(9, -6) \notin E_T(\mathbb{Q})$ it would generate infinitely many rational points on the curve. We now take a look at what happens when we view the group modulo $2E(\mathbb{Q})$.

The torsion group is unaffected since

$$E_T(\mathbb{Q})/2E(\mathbb{Q}) = E_T(\mathbb{Q})/2E_T(\mathbb{Q}) \cong (\mathbb{Z}_2 \oplus \mathbb{Z}_2)/2(\mathbb{Z}_2 \oplus \mathbb{Z}_2) = (\mathbb{Z}_2 \oplus \mathbb{Z}_2)$$

however, this doesn't matter too much since the torsion subgroup is always finite to begin with. Taking a look at our non-torsion point $P = (9, -6)$ we see that $2nP \equiv \infty$ for all non-zero integers n. As a result we must have that $(2n+1)P \equiv P$ for all integers n, which means that the infinite set of rational points generated by P is reduced to just two points modulo $2E(\mathbb{Q})$.

At this very moment, we don't know whether we've considered all points on the curve E, therefore we cannot draw the desired conclusion just yet. However, as we'll show later, every point in $E(\mathbb{Q})$ is a combination of torsion points and $P = (9, -6)$, which by the procedure just carried out implies that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. □

5.2 Heights and the Mordell-Weil Theorem

Along with the results from Section 5.1, we introduce a new concept referred to as the "height" of a point P on the elliptic curve. Combining the properties of this function with the Weak-Mordell Weil Theorem will provide a path towards proving the desired Mordell-Weil Theorem.

Definition 5.3. Let $Q = a/b$ be a rational number in its lowest terms. We define

$$H(a/b) = \text{Max}(|a|, |b|)$$

to be the height of the rational number Q. Moreover we define, $H(\infty) = 0$.

We now state a very important property of the function H:

Lemma 5.4. *Let $c \in \mathbb{R}$. Then there are only finitely many rational numbers $a/b \in \mathbb{Q}$ for which $H(a/b) \leq c$.*

Proof. If $H(a/b) \leq c$ then $\text{Max}(|a|, |b|) \leq c$. Consequently, we must have that, $-c \leq a, b \leq c$. Since there are only finitely many integers a, b to choose from, this results in finitely many ordered pairs, each corresponding to a possible rational number, from which the result follows. ■

Since we'll be taking the height of points on elliptic curves, we define $H(P) = H(x, y) = H(x)$, that is, we completely disregard the y coordinate. We don't actually lose any information since the x and y coordinates are still related through the equation of the elliptic curve. In our work, it will more convenient to consider an extension of this definition which has nicer properties:

Definition 5.4. Let $Q = a/b$ be a rational number in its lowest terms. We define

$$h(a/b) = \log H(a/b)$$

to be the logarithmic height of the rational number Q. As a result, $h(\infty) = 0$.

We have the following useful result about the logarithmic height h. Readers who wish to examine the proof should refer to [Was08].

Lemma 5.5. *Let E be an elliptic curve over $\mathbb{Q}$. Then there exists an upper bound $k \in \mathbb{R}$ such that*

$$|h(P+Q) + h(P-Q) - 2h(P) - 2h(Q)| \leq k$$

holds for all points P, Q on E. ■

The lemma above indicates that the logarithmic height h is close to being a quadratic form since it nearly obeys the parallelogram law. We can actually deform h to obtain a corresponding function $\hat{h}$ (the canonical height) which obeys the parallelogram law so that it is by virtue a quadratic form. This result along with other convenient properties of $\hat{h}$ will be proven after we define $\hat{h}$ below.

Definition 5.5. Let $Q = a/b$ be a rational number in its lowest terms. We define

$$\begin{aligned} \hat{h} : \mathbb{Q} &\to \mathbb{R} \\ Q &\mapsto \frac{1}{2} \lim_{n\to\infty} \frac{1}{4^n} h\left(2^n Q\right) \end{aligned}$$

to be the *canonical height* of the rational number Q. If $Q = \infty$, then by definition of h we get $\hat{h}(\infty) = 0$.

Lemma 5.6. *Let E be an elliptic curve over $\mathbb{Q}$. Then the function $\hat{h}$ is well-defined over $E(\mathbb{Q})$. Moreover, there exists an upper bound $k \in \mathbb{R}$ such that*

$$\left| \frac{1}{2} h(P) - \hat{h}(P) \right| \leq k$$

for all $P \in E(\mathbb{Q})$.

Proof. For the first part we need to show that the limit exists. We can write

$$\lim_{n\to\infty} \frac{1}{4^n} h\left(2^n P\right) = h(P) + \sum_{j=1}^{\infty} \frac{1}{4^j} \left(h\left(2^j P\right) - 4h\left(2^{j-1} P\right) \right)$$

which is a sort of telescoping series. Taking a look at Lemma 5.5 with $Q = P$ we obtain

$$|h(2P) - 4h(P)| \leq k$$

for all points P on E. Now letting $P \to 2^{j-1}P$ we get

$$\left| \frac{1}{4^j} \left(h\left(2^j P\right) - 4h\left(2^{j-1} P\right) \right) \right| \leq \frac{k}{4^j}$$

for some $k \in \mathbb{R}$. Since the limit of the upper bound on the jth term converges to zero, it follows that the infinite sum must also converge. Therefore $\hat{h}$ is well-defined over $E(\mathbb{Q})$.

For the second part, we continue with the argument above just a little further. Taking the sum on both sides of the inequality above we get

$$\left|\sum_{j=1}^{\infty} \frac{1}{4^j}\left(h\left(2^j P\right) - 4h\left(2^{j-1}P\right)\right)\right| \leq \sum_{j=1}^{\infty}\left|\frac{1}{4^j}\left(h\left(2^j P\right) - 4h\left(2^{j-1}P\right)\right)\right| \leq \sum_{j=1}^{\infty}\frac{k}{4^j}$$

The leftmost term is equal to $2|\frac{1}{2}h(P) - \hat{h}(P)|$ by definition, whereas for the rightmost term we have that

$$\sum_{j=1}^{\infty}\frac{k}{4^j} = \frac{k}{3} = 2k'$$

for some $2k' \in \mathbb{R}$. Putting this all together we obtain that

$$\left|\frac{1}{2}h(P) - \hat{h}(P)\right| \leq k'$$

for some $k' \in \mathbb{R}$ which is the required result. ■

Proposition 5.7. *Let E be an elliptic curve over $\mathbb{Q}$. Then $\hat{h}$ satisfies the following properties:*

1. $\hat{h}(P) \geq 0$ *for all* $P \in E(\mathbb{Q})$.
2. *Given a constant c, there are only finitely many points $P \in E(\mathbb{Q})$ with $\hat{h}(P) \leq c$.*
3. $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$ *for all P, Q.*
4. $\hat{h}(mP) = m^2\hat{h}(P)$ *for all integers m and all P.*
5. $\hat{h}(P) = 0$ *if and only if P is a torsion point.*

Proof. 1. Follows immediately from the definition.

2. Let $\hat{h}(P) \leq c$. Then by Lemma 5.6

$$\left|\frac{1}{2}h(P) - \hat{h}(P)\right| \leq k \implies h(P) \leq 2(\hat{h}(P) + k) \leq 2(c+k) = c'$$

for some $c' \in \mathbb{R}$. By Lemma 5.2, there are only finitely many points $P \in E(\mathbb{Q})$ for which $H(P) \leq c'$. Since the logarithm is monotonic, and $h(P) = \log H(P)$, we can generalize this result to h. Therefore, there can only be finitely many points P for which $h(P) \leq c'$ holds. As a result, there are only finitely many points P for which $\hat{h}(P) \leq c$ holds.

3. Using Lemma 5.5 with $P \to 2^n P$ and $Q \to 2^n Q$, then multiplying across by $\frac{1}{4^n}$ we obtain

$$\frac{1}{4^n} \left| h\left(2^n P + 2^n Q\right) + h\left(2^n P - 2^n Q\right) - 2h\left(2^n P\right) - 2h\left(2^n Q\right) \right| \leq \frac{k}{4^n}$$

Taking the limit as $n \to \infty$ we get

$$\left| \hat{h}\left(P + Q\right) + \hat{h}\left(P - Q\right) - 2\hat{h}\left(P\right) - 2\hat{h}\left(Q\right) \right| = 0$$

which we can rearrange to obtain

$$\hat{h}\left(P + Q\right) + \hat{h}\left(P - Q\right) = 2\hat{h}\left(P\right) + 2\hat{h}\left(Q\right).$$

4. Assuming that the E is in Weierstrass form, for $P = (x, y)$, we can write $P = (x, -y)$, the x-coordinate remaining invariant under reflection through the x-axis. Since the function $\hat{h}$ only takes the x-coordinate as its argument, $\hat{h}(P) = \hat{h}(-P)$. Consequently when considering $\hat{h}(mP)$ we may assume that m is non-negative. If $m = 0, 1$ then $\hat{h}(mP) = m^2 \hat{h}(P)$ holds trivially. We now use a watered-down version of strong induction to prove the claim entirely.

Suppose that the equality holds for $m, m-1$. Then letting $P \to mP$ and $Q \to P$ in (3) we obtain

$$\hat{h}((m+1)P) = -\hat{h}((m-1)P) + 2\hat{h}(mP) + 2\hat{h}(P)$$

By assumption $\hat{h}((m-1)P) = (m-1)^2 \hat{h}(P)$ and $\hat{h}(mp) = m^2 \hat{h}(p)$ so that the right-hand side now becomes

$$\left(-(m-1)^2 + 2m^2 + 2\right) \hat{h}(P) = (m+1)^2 \hat{h}(P)$$

and therefore

$$\hat{h}((m+1)P) = (m+1)^2 \hat{h}(P)$$

completing the induction procedure.

5. If P is torsion then $mP = \infty$. Using (4) we get that

$$m^2\hat{h}(P) = \hat{h}(mP) = \hat{h}(\infty) = 0$$

Since $m \neq 0$ we must have $\hat{h}(P) = 0$. To obtain the other direction assume that $\hat{h}(P) = 0$ to begin with. Then by (4) again, we obtain that $\hat{h}(mP) = m^2\hat{h}(P) = 0$ for arbitrary m. By (2) we know that there are only finitely many points whose height is zero. As a result the set $\{P, 2P, 3P, ...\}$ of points whose height is zero must be finite. Consequently, P must be torsion. ■

Theorem 5.8 (Mordell-Weil Theorem)**.** *$E(\mathbb{Q})$ is finitely generated for any elliptic curve E over $\mathbb{Q}$.*

Proof. By Theorem 5.3 we know that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. Let $R_1, ..., R_n \in E(\mathbb{Q})$ be representatives for the cosets in $E(\mathbb{Q})/2E(\mathbb{Q})$. Now define $c = \text{Max}_i \left\{\hat{h}\left(R_i\right)\right\}$ and let $P_1, P_2, ... \in E(\mathbb{Q})$ be all the points which satisfy $\hat{h}(P_i) \leq c$. By the second property of Proposition 5.7 we may assume that there are only finitely many such points, so that we can write $P_1, P_2, ... = P_1, P_2, ..., P_m$.

Now let G be the subgroup of $E(\mathbb{Q})$ generated by

$$P_1, ..., P_m, R_1, ..., R_n.$$

Suppose that $G \neq E(\mathbb{Q})$. Then there exists a set of points which belong to $E(\mathbb{Q})$ but not to G. Let P be the point with the smallest height in this set. We can assume such a point P exists courtesy of the second property of Proposition 5.7. Now let R_i be the coset to which the point P belongs to. Since $R_i - R_i = \infty$ (viewed as elements of $E(\mathbb{Q})/2E(\mathbb{Q})$), we can write

$$P - R_i = 2P_0$$

for some point $P_0 \in E(\mathbb{Q})$. By the fourth property of Proposition 5.7 we have

$$4\hat{h}\left(P_0\right) = \hat{h}\left(2P_0\right) = \hat{h}\left(P - R_i\right)$$

By the third property this is equivalent to

$$2\hat{h}(P) + 2\hat{h}\left(R_i\right) - \hat{h}\left(P + R_i\right)$$

Applying the first property we get that

$$2\hat{h}(P) + 2\hat{h}\left(R_i\right) - \hat{h}\left(P + R_i\right) \leq 2\hat{h}(P) + 2\hat{h}\left(R_i\right).$$

Next, since $\hat{h}(R_i) \leq c$ and $c < \hat{h}(P)$ we have

$$2\hat{h}(P) + 2\hat{h}\,(R_i) \leq 2\hat{h}(P) + 2c < 2\hat{h}(P) + 2\hat{h}(P) = 4\hat{h}(P)$$

Since the left-most side above is greater than or equal to $4\hat{h}(P_0)$, we obtain the inequality

$$4\hat{h}\,(P_0) < 4\hat{h}(P) \implies \hat{h}\,(P_0) < \hat{h}(P).$$

Now if $P_0 \notin G$ this contradicts our choice of P. Therefore we must have that $P_0 \in G$. Combining this with the fact that $R_i \in G$ also, we obtain $P = R_i + 2P_0 \in G$, which is a contradiction. Consequently we must have $G = E(\mathbb{Q})$. Since G is finitely generated, the result follows. ■

The result above guarantees that $E(\mathbb{Q})$ is finitely generated, which means that we can specify $E(\mathbb{Q})$ by listing its generators instead of all of its (possibly infinite) elements. Moreover, it also provides us with the method for finding these generators. First however, we specify the procedure for determining the structure of $E(\mathbb{Q})$, and then indicate an extension which will provide us with the generators as well.

5.3 Structure

Now that we know that $E(\mathbb{Q})$ is a finitely-generated abelian group we can make use of the following useful Theorem [Sti93]:

Theorem 5.9. *If G is a finitely-generated abelian group then*

$$G \cong T \oplus \mathbb{Z}^r$$

where T is a finite abelian group (see Theorem 4.12), and r is a non-negative integer. ■

Making use of the result above we can now outline a general procedure for determining the structure of the $E(\mathbb{Q})$:

To begin, notice that the image of the injective map

$$\begin{aligned} \varphi : E(\mathbb{Q})/2E(\mathbb{Q}) &\to \left(\mathbb{Q}^\times/\mathbb{Q}^{\times 2}\right) \oplus \left(\mathbb{Q}^\times/\mathbb{Q}^{\times 2}\right) \oplus \left(\mathbb{Q}^\times/\mathbb{Q}^{\times 2}\right) \\ (x, y) &\mapsto (a, b, c) \end{aligned}$$

is finite since the choices for a, b, c are finite (see Lemma 5.1). By Theorem 5.9 above we get that

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong T/2T \oplus (\mathbb{Z}/2\mathbb{Z})^r$$

so that we can consider the latter as the preimage of φ. Calculating T by methods from Section 4, and using the fact that the φ is injective and its image is finite allows us to place an upper bound on the rank r. Unfortunately, the set of possible combinations of triples (a, b, c) is usually quite large so that the determined upper bound is not close to the true value of r at all. The next step is to reduce this bound using congruence relations to eliminate possible triples (a, b, c); more specifically, we consider the natural map from $E(\mathbb{Q})/2E(\mathbb{Q})$ to $E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)$ where $\mathbb{Q}_p$ denotes the p-adic numbers for some $p \leq \infty$, with $\mathbb{Q}_\infty = \mathbb{R}$ for convenience. This then induces the map

$$\varphi' : E(\mathbb{Q}_p)/2E(\mathbb{Q}_p) \to \left(\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}\right) \oplus \left(\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}\right) \oplus \left(\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}\right)$$

from which we see that any possible triple (a, b, c) which does not belong to range of φ' (as we vary over primes p) can discarded. The points which are not eliminated by the process above form a group S_2 called the 2-Selmer group. We regard it a group in the sense of being a subgroup of the larger group $(\mathbb{Q}^\times/\mathbb{Q}^{\times 2}) \oplus (\mathbb{Q}^\times/\mathbb{Q}^{\times 2}) \oplus (\mathbb{Q}^\times/\mathbb{Q}^{\times 2})$.

Backtracking a little, notice that $|T/2T \oplus (\mathbb{Z}/2\mathbb{Z})^r| = 2^{t+r}$. As a result, we reduce (as explained above) until we find an upper bound of the form 2^n, where we expect that $n = t + r$. To check this we run a computer search to find points in $E(\mathbb{Q})$, obtain their corresponding images in $(\mathbb{Q}^\times/\mathbb{Q}^{\times 2}) \oplus (\mathbb{Q}^\times/\mathbb{Q}^{\times 2}) \oplus (\mathbb{Q}^\times/\mathbb{Q}^{\times 2})$ and check whether they form a subgroup of order exactly 2^n. If so, then $n = t + r$ indeed and therefore $r = n - t$. If the bound n is sharp, the computer should eventually find points in $E(\mathbb{Q})$ necessary for creating a group of size 2^n in $(\mathbb{Q}^\times/\mathbb{Q}^{\times 2}) \oplus (\mathbb{Q}^\times/\mathbb{Q}^{\times 2}) \oplus (\mathbb{Q}^\times/\mathbb{Q}^{\times 2})$.

If the bound is not sharp, however, the computer will be stranded searching for non-existent points—or at least points which cannot make $\mathrm{im}(\varphi) \subset (\mathbb{Q}^\times/\mathbb{Q}^{\times 2}) \oplus (\mathbb{Q}^\times/\mathbb{Q}^{\times 2}) \oplus (\mathbb{Q}^\times/\mathbb{Q}^{\times 2})$ any larger. One can try to remedy this by going back and attempting to make the bound sharper, however, this is not always possible. Fortunately, this does not occur too often: it only occurs in the case that $\mathrm{im}(\varphi) \neq S_2$, that is, $Ш_2 = S_2/\mathrm{im}(\varphi) \neq 1$. The symbol Ш denotes the more general *Shafarevich-Tate group* which arises by considering n-descent in general for all $n \geq 1$, in particular, $Ш_2$ denotes the 2-torsion in Ш.

We can now also extend the procedure above, with the help of Theorem 5.8 and the result below [Was08] to obtain a method for finding generators for $E(\mathbb{Q})$.

Theorem 5.10 (Silverman's Theorem)**.** *Let E be an elliptic curve over $\mathbb{Q}$ of the form $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$. Suppose that $P \in E(\mathbb{Q})$. Then P satisfies*

$$-\frac{1}{8}h(j) - \frac{1}{12}h(\Delta) - 0.973 \leq \hat{h}(P) - \frac{1}{2}h(P) \leq \frac{1}{12}h(j) + \frac{1}{12}h(\Delta) + 1.07$$

where $\Delta = -16\,(4A^3 + 27B^2)$ *is the discriminant and* $j = -1728(4A)^3/\Delta$ *is the j-invariant.* ■

So far, the procedure above has yielded the representatives R_i mentioned in Theorem 5.8. Next, we find the canonical height of each R_i. Let c be the maximum height of these representatives. By Theorem 5.8, all that remains to do is to search for rational points with height less than c. Using Theorem 5.10 above we find an upper bound for $h(P)$, in turn leaving us with a finite number of possible integers for both the numerator and denominator (see Lemma 5.4) which we can search through using a computer. The representatives and the set of points found by the computer search can then be combined to form a generating set for $E(\mathbb{Q})$ by Theorem 5.8. However, it must be duly noted that although the last step is a finite search, this "finite" search space can be very large, which makes the method unfeasible at the worst and unattractive at the best.

Assuming, however, that one has obtained a list of the generators, it is desirable—although not necessary—to reduce it to a set of independent generators. The following result enables us to test a set of points for independence:

Lemma 5.11. *Let* E *be an elliptic curve over* $\mathbb{Q}$ *and suppose that* $P, Q \in E(\mathbb{Q})$*. Then the height pairing*

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

is bilinear in each variable. Consequently, if $P_1, ..., P_r \in E(\mathbb{Q})$ *and the* $r \times r$ *determinant* $\det\left(\langle P_i, P_j\rangle\right)$ *is non-zero for all* i, j *then* $P_1, ..., P_r$ *form an independent set of points.*

Proof. We first demonstrate that the pairing is bilinear. Since $\langle P, Q\rangle = \langle Q, P\rangle$ it is sufficient to demonstrate bilinearity in the first variable only. We have that

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

and

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

Using the parallelogram law (Proposition 5.7) we obtain the following four equations:

$$\begin{aligned}
\hat{h}(P+Q+R) + \hat{h}(P+Q-R) - 2\hat{h}(P+Q) - 2\hat{h}(R) &= 0 \\
2\hat{h}(Q-R) - \hat{h}(P+Q-R) - \hat{h}(P-Q+R) &= -2\hat{h}(P) \\
\hat{h}(P+R+Q) + \hat{h}(P+R-Q) &= 2\hat{h}(P+R) + 2\hat{h}(Q) \\
-2\hat{h}(Q-R) &= 2\hat{h}(Q+R) - 4\hat{h}(Q) - 4\hat{h}(R).
\end{aligned}$$

Putting these all together yields

$$\begin{aligned}&2(\hat{h}(P+Q+R)-\hat{h}(P+Q)-\hat{h}(R))\\ =&2(\hat{h}(P+R)-\hat{h}(P)-\hat{h}(R)+\hat{h}(Q+R)-\hat{h}(Q)-\hat{h}(R))\end{aligned}$$

which results in

$$2\langle P+Q,R\rangle = 2(\langle P,R\rangle + \langle Q,R\rangle)$$

by the equations first examined above and bilinearity follows.

For the second part, suppose that there exist integers a_i such that $a_1P_1+...+a_rP_r=\infty$ with some $a_k \neq 0$ so that $a_kP_k = -a_1P_1 + ... + -a_rP_r$. Then a_k times the k-th row of the matrix $\langle P_i, P_j\rangle$ yields a vector with entries $a_k\langle P_k, P_j\rangle$. Using the equation derived above and bilinearity gives

$$\begin{aligned}a_k\langle P_k,P_j\rangle = \langle a_kP_k,P_j\rangle &= \langle -a_1P_1+...+-a_rP_r,P_j\rangle\\ &= -a_1\langle P_1,P_j\rangle + ... + -a_r\langle P_r,P_j\rangle\end{aligned}$$

which demonstrates that a_k times the k-th row of the matrix is a linear combination of the other rows so that the determinant is zero. The contrapositive then provides the result. ■

Example 5.2. Let E be the elliptic curve given by $y^2 = x(x+5)(x+10)$. We want to find the structure of E and its generators using the method just described above.

We first find the image of the obvious points in $E(\mathbb{Q})$. We have $\infty \in E(\mathbb{Q})$ with

$$\varphi(\infty) = (1,1,1)$$

If $y = 0$ then the images of the corresponding points are

$$\begin{aligned}\varphi(0,0) &= (2,5,10)\\ \varphi(-5,0) &= (-5,-1,5)\\ \varphi(-10,0) &= (-10,-5,2)\end{aligned}$$

Our task at hand now is finding the remainder of the points contained in $\mathrm{im}(\varphi)$, that is, the non-obvious points of $\mathrm{im}(\varphi)$ which have $y \neq 0$. We do this by elimination.

The map φ for $y \neq 0$ is given by

$$(x,y) \mapsto (x, x+5, x+10) = (au^2, bv^2, cw^2).$$

From the discussion at the beginning of Section 5.1 one may recall that a, b, c are square-free integers. By Lemma 5.1 we have that $a, b, c \mid (0+5)(-5+10)(-10+0) = -2 \cdot 5^3$ which implies that $a, b, c \in \{\pm 1, \pm 2, \pm 5, \pm(2 \cdot 5)\}$.

Before we begin eliminating possibilities, it is useful to notice one more thing: since abc is a square and a, b, c are each individually square-free, then specifying a, b determines c uniquely. As a result, we only need to focus on eliminating possibilities for a and b. There are currently 8 possibilities for both a and b resulting in 64 total possibilities. Since we know that $T = E_T(\mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ we obtain $T/2T \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ which has order 2^2. We must have $2^{2+r} \leq 2^6 = 64$, therefore $r \leq 4$ at the moment.

To begin the eliminations, notice that

$$x < x + 5 < x + 10$$

implies

$$au^2 < bv^2 < cw^2.$$

If $b < 0$ then the above implies $a < 0$ also. On the other hand, if $b > 0$ the above implies $c > 0$. Since abc is a square this means $abc > 0$ which then implies $a > 0$. Therefore a and b must share the same sign, leaving us with $64/2 = 32$ remaining possibilities. Notice that in terms of our procedure above what we've just done is eliminated possible triples (a, b, c) which do not belong to $(\mathbb{Q}_\infty^\times/\mathbb{Q}_\infty^{\times 2}) \oplus (\mathbb{Q}_\infty^\times/\mathbb{Q}_\infty^{\times 2}) \oplus (\mathbb{Q}_\infty^\times/\mathbb{Q}_\infty^{\times 2})$. The elimination lowers the bound on the rank by a power of two, which means that $r \leq 3$ now.

Suppose $(a, b) = (2, 1)$. Then we can combine

$$\begin{aligned} x &= 2u^2 \\ x + 5 &= v^2 \\ x + 10 &= 2w^2 \end{aligned}$$

to obtain

$$2u^2 - v^2 = -5 \quad 2w^2 - 2u^2 = 10.$$

A little algebra shows that $v_2(v^2) < 0$ if and only if $v_2(2u^2) < 0$. However, if this is true, it's obvious that $v_2(v^2)$ cannot equal $v_2(2u^2)$. As a result $2u^2 - v^2$ cannot be an integer. This is a contradiction, therefore we assume that the denominators are not divisible by 2, allowing us to work modulo 2^n. By the equation above v is odd, therefore

$$v^2 \equiv 1 \pmod 8 \implies 2u^2 \equiv -4 \pmod 8 \implies u^2 \equiv 2 \pmod 4$$

which cannot be true, since u even implies $u^2 \equiv 0 \pmod 4$. Therefore $(2,1) \notin \mathrm{im}(\varphi)$. Since there are now only 31 possible triples (a,b,c) and $2^{2+r} \leq 31 < 2^5$ we get that $r \leq 2$. Similar considerations for other relevant primes p will actually lower the bound further so that $r \leq 1$ in the end.

We now perform the computer search to try and find a point of infinite order if it exists. It does not take long to find $(-9,6)$, which we know does not belong to $E_T(\mathbb{Q})$. As a result we must have that $r = 1$ and therefore $E(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. For completeness we have that

$$\varphi(-9,6) = (-1,-1,1)$$

We currently have five of the 2^3 points of $E(\mathbb{Q})/2E(\mathbb{Q})$. To obtain the other three we just add our point of infinite order to the three torsion points

$$\begin{aligned}
\varphi((-9,6)+(0,0)) &= \varphi\left(-\frac{50}{9}, -\frac{100}{27}\right) &&= (-1,-1,1)\cdot(2,5,10) &&= (-2,-5,10)\\
\varphi((-9,6)+(-5,0)) &= \varphi\left(\frac{5}{4}, \frac{75}{8}\right) &&= (-1,-1,1)\cdot(-5,-1,5) &&= (5,1,5)\\
\varphi((-9,6)+(-10,0)) &= \varphi(40,-300) &&= (-1,-1,1)\cdot(-10,-5,2) &&= (10,5,2)
\end{aligned}$$

so that

$$\begin{aligned}
\mathrm{im}(\varphi) = \{&(1,1,1),(2,5,10),(-5,-1,5),(-10,-5,2),(-1,-1,1),(-2,-5,10),\\
&(5,1,5),(10,5,2)\}
\end{aligned}$$

and correspondingly

$$E(\mathbb{Q})/2E(\mathbb{Q}) = \{\infty,(0,0),(-5,0),(-10,0),(-9,6),\left(-\frac{50}{9},\frac{100}{27}\right),\left(\frac{5}{4},\frac{75}{8}\right),(40,-300)\}$$

where the points are coset representatives. We now determine a generating set for $E(\mathbb{Q})$. First we reduce the representatives to an independent set using Lemma 5.11 to get $\{(0,0),(-5,0),(-10,0),(-9,6)\}$. We now take a look at the canonical heights of the remaining representatives. The torsion points will have canonical height zero so we don't need to check them (see Proposition 5.7). We have $\hat{h}(-4,6) \approx 1.9$ which means that 1.9 is the maximum canonical height of the representatives. To use Theorem 5.10, however, we first need to transform the curve into Weierstrass form so that $y^2 = x^3 - 25x$. The canonical height is unaffected by this transformation. Using the

theorem we obtain an upper bound for the logarithmic height

$$\begin{aligned} h(P) &< 2(\frac{1}{8}h(j) + \frac{1}{12}h(\Delta) + 0.973 + \hat{h}(P)) \\ &< 2(\frac{1}{8}h(j) + \frac{1}{12}h(\Delta) + 0.973 + \max\{\hat{h}(P)\}) \\ &= 2(\frac{1}{8}h(1728) + \frac{1}{12}h(62,500) + 0.973 + 1.9\}) = 9.45 \end{aligned}$$

The last step is to then search through all rational points $\frac{a}{b}$ for all $-e^{9.45} \leq a, b \leq e^{9.45}$. After this exhaustive search, one can verify that adding any of these newly found points to the current independent set of representatives causes independence to fail. As a result, the generating set is $\{(0,0), (-5,0), (-10,0), (-9,6)\}$. □

Although we've figured out how to determine the rank of $E(\mathbb{Q})$ in general, there are still a multitude of questions that can be asked with regards to its behaivour. We wrap up with a currently unsolved problem.

Conjecture 5.12. *There exist elliptic curves with $E(\mathbb{Q})$ of arbitrarily large rank.*

In other words, it is conjectured that the rank of elliptic curves cannot be bounded. Despite extensive research the answer has proven to be elusive, with the problem still under scrutiny today. The current record for the largest rank is held by Noam Elkies, who in 2006 announced the discovery of an elliptic curve of rank at least 28 [E+06] with the rank determined to be exact afterwards [KSW16]. Although lack of further progress with pushing the bound appears to support the conjecture, it should be noted that the methods which are employed for such purposes are computationally intensive and require resources and much time to conduct, without considering the fact that increasing the bound may not contribute towards any actual progress on the conjecture itself.

Acknowledgements

I'd like to express my appreciation and gratitude towards my supervisor Prof. Nicolas Mascot for his helpful suggestions, explanations and assistance throughout the entire project.

References

[BM02] Ezra Brown and Bruce T Myers. Elliptic curves from mordell to diophantus and back. *The American mathematical monthly*, 109(7):639–649, 2002.

[E+06] Noam D Elkies et al. $\mathbb{Z}^{28}$ in $E(\mathbb{Q})$, etc. *Number Theory Listserver*, 2006.

[Fri17] Stefan Friedl. An elementary proof of the group law for elliptic curves. *Groups Complexity Cryptology*, 9(2):117–123, 2017.

[Kro70] Leopold Kronecker. *Auseinandersetzung einiger Eigenschaften der Klassenzahl idealer complexer Zahlen*. 1870.

[KSW16] Zev Klagsbrun, Travis Sherman, and James Weigandt. The elkies curve has rank 28 subject only to grh. *Mathematics of Computation*, 88(316):837–846, 2016.

[LMF22] The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2022. [Online; accessed 19 March 2022].

[Maz77] Barry Mazur. Modular curves and the eisenstein ideal. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 47(1):33–186, 1977.

[MG78] Barry Mazur and Dorian Goldfeld. Rational isogenies of prime degree. *Inventiones mathematicae*, 44(2):129–162, 1978.

[RB12] Adrian Rice and Ezra Brown. Why ellipses are not elliptic curves. *Mathematics Magazine*, 85(3):163–176, 2012.

[Spe96] Phillip Spencer. Understanding Projective Geometry. `https://www.math.toronto.edu/mathnet/questionCorner/projective.html`, 1996. Accessed: March 19, 2022.

[ST92] Joseph H Silverman and John Torrence Tate. *Rational points on elliptic curves*, volume 9. Springer, 1992.

[Sti93] John Stillwell. *Classical topology and combinatorial group theory*, volume 72. Springer Science & Business Media, 1993.

[The19] The PARI Group, Univ. Bordeaux. *PARI/GP version `2.11.2`*, 2019. available from `http://pari.math.u-bordeaux.fr/`.

[Was08] Lawrence C Washington. *Elliptic curves: number theory and cryptography*. Chapman and Hall/CRC, 2008.

[Wil95] Andrew Wiles. Modular elliptic curves and fermat's last theorem. *Annals of mathematics*, 141(3):443–551, 1995.