Elliptic curves over finite fields and the rationals: Determining the underlying group structure

Degree Project in Engineering Physics, First Level
Department of Mathematics
KTH Royal Institute of Technology

Author: Tomas Petkov
Supervisor: Ralph Morrison
Examiner: Mårten Olsson

Abstract

The study of elliptic curves is an important part of the fields of algebraic geometry and number theory, with many applications in areas such as cryptography. While much of the groundwork has already been laid out, the results often times fall short of giving an easily digestible overview of the subject as a whole. The aim of this paper is to condense a number of high-level results into a much more readily accessible version that is better suited for a reader encountering elliptic curves for the first time. Additionally, the paper provides a toolkit for identifying elliptic curve groups, detailing steps to take in order to determine the group behind a given elliptic curve.

Sammanfattning

Studien av elliptiska kurvor är ett viktigt delområde inom algebraisk geometri och talteori, med många tillämpningar inom t.ex. kryptografi. Mycket av grunden har redan lagts, men resultatet lyckas sällan ge en lättillgänglig överblick av ämnet som helhet. Målet med detta arbete är att kondensera ett antal djupgående resultat till en åtkomligare version som är bättre lämpad för en läsare som för första gången stöter på elliptiska kurvor. Dessutom tillhandahåller detta arbete en uppsättning verktyg för att kunna identifiera elliptiska kurvor, samt beskriver de steg som skall tas för att kunna bestämma gruppen bakom en given elliptisk kurva.

Preface

This paper was written as part of the course Degree Project in Engineering Physics, First Level (SA114X) at the Department of Mathematics, KTH Royal Institute of Technology.

Notation The symbols $\mathbb{Z}, \mathbb{F}_q, \mathbb{Q}, \mathbb{R}$ denote the integers, the finite field with q elements, the rational numbers and the real numbers, respectively. The notation $\mathbb{Z}_n$ is used to denote the integers mod n, rather than $\mathbb{Z}/n\mathbb{Z}$. When working with Z_p as a field (rather than as a group), with p being prime, this paper uses the notation $\mathbb{F}_p$ so as to remain consistent with the notation $\mathbb{F}_q$. If K is a field, then $\overline{K}$ denotes an algebraic closure of K, while $K^\times$ denotes the multiplicative group of non-zero elements of K.

Acknowledgements I would like to extend my sincerest gratitude to my supervisor Ralph Morrison for introducing me to the fascinating subject of elliptic curves, as well as for his extensive help and guidance throughout the course of this project. I would also like to thank my coursemates Emil, Erika, Isak, Jonas and Patric for proofreading and providing feedback for the paper.

Contents

1 Introduction

Elliptic curves are an interesting subject of study, owing to the fact that the set of points on such a curve can be equipped with a binary operation ($\star$) that induces a natural, albeit unintuitive, group structure on the set of points on the curve. Elliptic curves have numerous applications in e.g. number theory, and have lately been on the receiving end of many mathematician's attentions — they were used in proving Fermat's Last Theorem [9] and are intimately connected with the Birch and Swinnerton-Dyer conjecture [10], one of the seven Millenium Prize Problems.

Many tools are available in order to determine the properties of the resulting group $(E, \star)$. The goal of this paper is to provide an easily accessible first lesson in dealing with elliptic curves, as well as to synthesize some of the most important results into a beginner's toolkit for working with elliptic curves.

In Chapter 1, we will introduce elliptic curves and define the group operation both geometrically and algebraically. Chapter 2, the main focus of the paper, will explore elliptic curves when defined over finite fields, while Chapter 3 will deal with elliptic curves over the rationals.

1.1 Defining elliptic curves

An elliptic curve E over a field K, denoted by $E(K)$, is a non-singular smooth plane cubic curve, defined by an equation of the form

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

with variables and coefficients in K. While this expression is rather unwieldy, we can impose the following conditions on K which allow for significant simplification — assuming the characteristic of K is not 2, the change of variables

$$y_1 = y + \frac{a_1x}{2} + \frac{a_3}{2}$$

produces

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

Assuming further that the characteristic is also not 3, the substitution

$$x_1 = x + \frac{a_2'}{3}$$

yields the **Weierstrass equation**

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

where we require the discriminant $D = 4A^3 + 27B^2 \neq 0$ to avoid singular curves.

1.2 The point at infinity

We define a **point at infinity**, denoted by ∞, satisfying the condition that all vertical lines pass through ∞. The reasoning behind this definition, as well as the point's purpose, will become apparent later on.

1.3 Defining the group law.

We are now ready to define the group of an elliptic curve. First, we define the set:

$$E(K) = \{\infty\} \cup \{(x, y) \in K \times K | y^2 = x^3 + Ax + B\}.$$

The most intuitive approach to defining the group law is the geometrical one. It is therefore helpful to visualize the elliptic curve as a graph over the real numbers. Different values of the coefficients A, B will yield one of two basic shapes, depending on the sign of $4A^3 + 27B^2$. Figure 1 shows the two shapes.

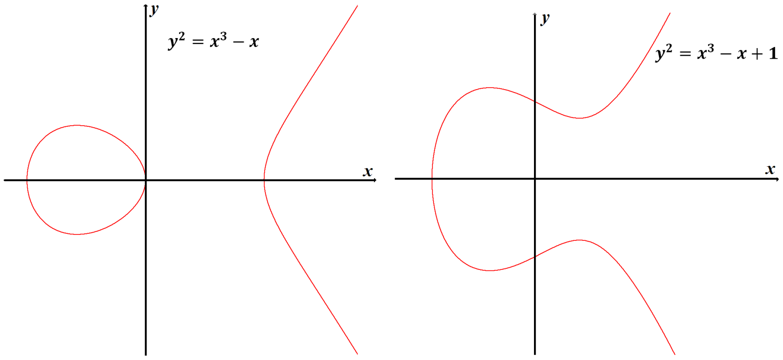

Figure 1: Elliptic curves over $\mathbb{R}$

To define the group law, referred to as addition and denoted by $+$ (not to be confused with addition of coordinates), we begin with two distinct points, different from ∞, on an elliptic curve E:

$$P = (x_1, y_1), \qquad Q = (x_2, y_2).$$

To produce a third point on E, we will draw the line L through P and Q, find its third intersection point with E, and reflect that about the x-axis to obtain a point R. Finally, we define R to be the sum of P and Q — see Figure 2.

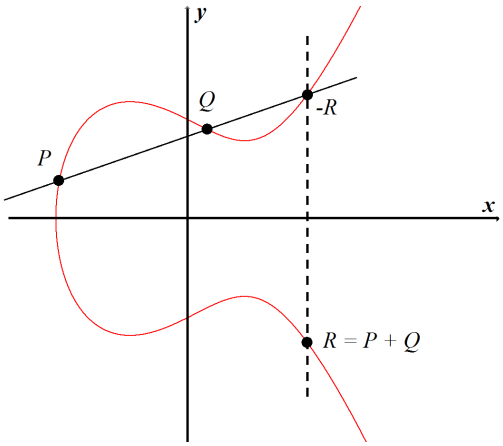

Figure 2: Addition of two distinct points

Remark. The existence of the third intersection is guaranteed by **Bézout's Theorem** [1], which states that the number of intersection points of two distinct smooth plane algebraic curves over a field F is equal to the product of their degrees, provided points are counted with multiplicity, points at infinity are included, and points are allowed to have coordinates in an algebraic closure of F. For an elliptic curve and a straight line, this results in $3 \cdot 1 = 3$ intersection points. The fact that we know the first two intersection points lie in F and not its closure $\overline{F}$, guarantees that the third intersection point is in F as well.

To make the geometric definition more formulaic, we begin by assuming that $P \neq Q, x_1 \neq x_2$, with neither point being ∞, and handle the other cases later. The slope of L is then $m = \dfrac{y_2 - y_1}{x_2 - x_1}$, and we therefore have the following equation for L:

$$y = m(x - x_1) + y_1.$$

The intersection of L and E is obtained by substituting this expression into the equation for E, yielding

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

Rearranging this, we have

$$x^3 - m^2x^2 + Cx + D = 0, \tag{1}$$

for some C and D. To find the roots of this equation, we can use the fact that two of them are already known, x_1 and x_2. Letting the third one be x_3, we have

$$\begin{aligned} 0 &= (x - x_1)(x - x_2)(x - x_3) \\ &= x^3 - (x_1 + x_2 + x_3)x^2 + ... \end{aligned} \tag{2}$$

Identifying the coefficients in expressions (1) and (2), we obtain the relation

$$\begin{aligned} m^2 &= x_1 + x_2 + x_3, \\ x_3 &= m^2 - x_1 - x_2. \end{aligned}$$

To find the y-coordinate of the intersection, y_3', we insert x_3 into the expression for L:

$$y_3' = m(x_3 - x_1) + y_1.$$

Finally, we let y_3 be the reflection of y_3' about the x-axis

$$y_3 = -y_3' = m(x_1 - x_3) - y_1$$

and define $P + Q$ to be the point $R = (x_3, y_3)$.

If on the other hand $P \neq Q, x_1 = x_2$, the line through P and Q is a vertical line, which will intersect E at ∞. Since the reflection of ∞ about the x-axis is still ∞, we have $P + Q = \infty$.

We continue with the case of $P = Q$. We will take the line through P and Q to be the tangent line of E at P. If $y_1 = 0$, the line will again be vertical, so we set $P + Q = \infty$. If $y_1 \neq 0$, we can calculate the slope of L by means of implicit differentiation:

$$\begin{aligned} y^2 &= x^3 + Ax + B, \\ 2y\frac{dy}{dx} &= 3x^2 + A, \\ m = \frac{dy}{dx} &= \frac{3x_1^2 + A}{2y_1}. \end{aligned}$$

Proceeding in the same way as in the case $P \neq Q$, but counting x_1 as a double root, we obtain

$$\begin{aligned} x_3 &= m^2 - 2x_1, \\ y_3 &= m(x_1 - x_3) - y_1. \end{aligned}$$

Finally, we consider the case where one of the points is ∞. The line through any point P and ∞ is vertical, and intersects E in the reflection of P. Reflecting about the x-axis returns us to the point P, so we have

$$P + \infty = P,$$

which we will extend to include

$$\infty + \infty = \infty.$$

We are now ready to show that the set of points on an elliptic curve, together with the addition defined above, form an abelian group:

1. Existence of identity : By definition, $P + \infty = P$ for all points P.

2. Existence of inverses : For any point P, its inverse is its reflection across the x-axis. Using the additive notation, $P = (x, y) \implies -P = (x, -y)$.

3. Associativity : Proving that associativity holds is a very challenging task. The proof is quite extensive, but is not central to this paper, so we omit it and refer to [7, Ch. 2.4]

4. Commutativity : It is evident from the formulas for the addition of points that the operation is commutative. Commutativity can also be concluded from the geometric definition, since the line through P and Q is the same as the line through Q and P.

2 Elliptic curves over finite fields

Defining an elliptic curve E over the finite field with q elements, $\mathbb{F}_q$ introduces an entire new set of challenges. Since there are only q^2 points in the two dimensional plane $\mathbb{F}_q^2$, the group $E(\mathbb{F}_q)$ is obviously going to be finite. What further information can we then obtain about its structure, and what tools are at our disposal to do so?

2.1 Determining the group order

We begin with the simplest approach — counting all the points on the curve.

Example 1 Let E be the curve $y^2 = x^3+2x+1$ over $\mathbb{F}_5$. To find the points on E, we simply list the possible values for x and $x^3+2x+1 \pmod 5$, as well as the corresponding values for y:

x	x^3+2x+1	y	Points
0	1	± 1	(0,1), (0,4)
1	4	± 2	(1,2), (1,3)
2	3	—	—
3	4	± 2	(3,2), (3,3)
4	3	—	—
∞		∞	∞

We can now see that $E(\mathbb{F}_5)$ has order 7 and can therefore conclude that $E(\mathbb{F}_5) \simeq \mathbb{Z}_7$. Additionally, a simple calculation shows that repeated addition of any non-infinite point to itself genererates the entire group.
This method can be formalized by generalizing the **Legendre Symbols**. We begin with the basic definition of the Legendre Symbol $\left(\frac{x}{p}\right)$ for an odd prime p:

$$\left(\frac{x}{p}\right) = \begin{cases} +1 & \text{if } t^2 \equiv x \pmod p \text{ has a solution } t \not\equiv 0 \pmod p, \\ -1 & \text{if } t^2 \equiv x \pmod p \text{ has no solution } t, \\ 0 & \text{if } x \equiv 0 \pmod p, \end{cases}$$

and extend it to any finite field $\mathbb{F}_q$ with q odd by defining

$$\left(\frac{x}{\mathbb{F}_q}\right) = \begin{cases} +1 & \text{if } t^2 = x \text{ has a solution } t \in \mathbb{F}_q^{\times}, \\ -1 & \text{if } t^2 = x \text{ has no solution } t \in \mathbb{F}_q, \\ 0 & \text{if } x = 0 \end{cases}$$

for any $x \in \mathbb{F}_q$.
With this definition, we can state the following theorem:

Theorem 2.1. *Let E be an elliptic curve over $\mathbb{F}_q$ with q odd defined by $y^2 = x^3 + Ax + B$. Then the number of points $\#E(\mathbb{F}_q)$ on the curve is given by*

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + Ax + B}{\mathbb{F}_q}\right).$$

Proof. For any value of x, consider the value of $x^3 + Ax + B$. If it is a non-zero square, then we have two points satisfying $y^2 = x^3 + Ax + B$. If it is zero, there is only one such point, and there are no valid points when $x^3 + Ax + B$ is a non-square. In each of these cases, the number of points is equal to $1 + \left(\frac{x^3 + Ax + B}{\mathbb{F}_q}\right)$, so summing over all $x \in \mathbb{F}_q$ and adding one to account for the point at infinity, we have

$$\begin{aligned} \#E(\mathbb{F}_q) &= 1 + \sum_{x \in \mathbb{F}_q} \left(1 + \left(\frac{x^3 + Ax + B}{\mathbb{F}_q}\right)\right) \\ &= q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + Ax + B}{\mathbb{F}_q}\right). \end{aligned}$$

■

Example 2 Let E be the curve $y^2 = x^3 + 2x + 1$ over $\mathbb{F}_5$ from Example 1. Since the non-zero squares in $\mathbb{F}_5$ are 1 and 4, applying **Theorem 2.1** yields

$$\begin{aligned} \#E(\mathbb{F}_5) &= 5 + 1 + \sum_{x=0}^{4} \left(\frac{x^3 + 2x + 1}{\mathbb{F}_5}\right) \\ &= 6 + \left(\frac{1}{\mathbb{F}_5}\right) + \left(\frac{4}{\mathbb{F}_5}\right) + \left(\frac{3}{\mathbb{F}_5}\right) + \left(\frac{4}{\mathbb{F}_5}\right) + \left(\frac{3}{\mathbb{F}_5}\right) \\ &= 6 + 1 + 1 - 1 + 1 - 1 = 7. \end{aligned}$$

While the method of counting points, either by hand or by using Legendre symbols, clearly works, it can hardly be considered efficient for any but the smallest of fields. For larger fields, we will need more more advanced tools. One such tool is the Frobenius endomorphism.

2.1.1 The Frobenius endomorphism

Let $\mathbb{F}_q$ be a field with algebraic closure $\overline{\mathbb{F}}_q$ and define the **Frobenius map**

$$\begin{aligned} \phi_q \colon \overline{\mathbb{F}}_q &\longrightarrow \overline{\mathbb{F}}_q, \\ x &\mapsto x^q \end{aligned}$$

If E is an elliptic curve over $\mathbb{F}_q$, then ϕ_q has an action on the coordinates of points in $E(\overline{\mathbb{F}}_q)$:

$$\phi_q(x,y) = (x^q, y^q), \quad \phi_q(\infty) = \infty.$$

The Frobenius map can be shown to possess a large number of useful properties, and an in-depth overview would be well beyond the scope of this paper. Instead we will present some of the most important results without proof and refer the interested reader to [7, Ch. 4.2].

Properties of the Frobenius map ϕ_q :

If $E(\mathbb{F}_q)$ is an elliptic curve with $\#E(\mathbb{F}_q) = q + 1 - a$, then

a) ϕ_q is an endomorphism of E of degree q,

b) $\phi_q^n = \phi_{q^n}$,

c) $\#E(\mathbb{F}_{q^n}) = \deg(\phi_q^n - 1)$,

d) $\deg(r\phi_q - s) = r^2 q + s^2 - rsa$ for $r, s \in \mathbb{Z}$,

e) $\phi_q^2 - k\phi_q + q = 0 \iff k = a$.

With these properties at our disposal, we can determine the orders of elliptic curve groups over large fields. We begin with the following theorem, which shows that the order of $E(\mathbb{F}_q)$ determines the order of $E(\mathbb{F}_{q^n})$.

Theorem 2.2. *Let* $\#E(\mathbb{F}_q) = q+1-a$. *Write* $X^2 - aX + q = (X-\alpha)(X-\beta)$. *Then*

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

for all $n \geq 1$*.*

We first need to show that $\alpha^n + \beta^n$ is an integer for all $n \geq 1$.

Lemma 2.2.1. *Let* $s_n = \alpha^n + \beta^n$*. Then* $s_0 = 2$*,* $s_1 = a$ *and* $s_{n+1} = as_n - qs_{n-1}$ *for all* $n \geq 1$*.*

Proof. Write $(\alpha - \alpha)(\alpha - \beta) = \alpha^2 - a\alpha + q = 0$ to obtain

$$\alpha^2 = a\alpha - q. \tag{3}$$

Multiplying (3) by α^{n-1} yields

$$\alpha^{n+1} = a\alpha^n - q\alpha^{n-1}. \tag{4}$$

Similarly, one obtains the relation

$$\beta^{n+1} = a\beta^n - q\beta^{n-1}. \tag{5}$$

Adding expression (4) and (5) produces the wanted result

$$\begin{aligned} s_{n+1} &= \alpha^{n+1} + \beta^{n+1} \\ &= a(\alpha^n + \beta^n) - q(\alpha^{n-1} + \beta^{n-1}) \\ &= as_n - qs_{n-1}, \end{aligned}$$

completing the proof of the lemma. ■

We can now prove **Theorem 2.2**:

Proof. Let

$$f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n.$$

Then $(X^2 - aX + q) = (X - \alpha)(X - \beta)$ divides $f(X)$. Therefore, by property e), we can write

$$(\phi_q^n)^2 - (\alpha^n + \beta^n)\phi_q^n + q^n = f(\phi_q) = Q(\phi_q)(\phi_q^2 - a\phi_q + q) = 0.$$

Applying property b) to the leftmost expression yields

$$(\phi_q^n)^2 - (\alpha^n + \beta^n)\phi_q^n + q^n = 0,$$

$$\phi_{q^n}^2 - (\alpha^n + \beta^n)\phi_{q^n} + q^n = 0$$

Finally, by property e), the only integer k for which $\phi_{q^n}^2 - k\phi_{q^n} + q^n = 0$ is given by $k = q^n + 1 - \#E(\mathbb{F}_{q^n})$, so we conclude that

$$\alpha^n + \beta^n = q^n + 1 - \#E(\mathbb{F}_{q^n}).$$

$\blacksquare$

Example 3 Let E be the curve $y^2 = x^3 + 2x + 1$ over $\mathbb{F}_5$. In examples 1 and 2, we showed that $\#E(\mathbb{F}_5) = 7$, so $a = 5 + 1 - 7 = -1$. We let

$$X^2 + X + 5 = \left(X - \frac{-1 + i\sqrt{19}}{2}\right)\left(X - \frac{-1 - i\sqrt{19}}{2}\right).$$

According to **Theorem 2.2** we then have

$$\#E(\mathbb{F}_{25}) = 25 + 1 - \left(\frac{-1 + i\sqrt{19}}{2}\right)^2 - \left(\frac{-1 - i\sqrt{19}}{2}\right)^2 = 35,$$
$$\#E(\mathbb{F}_{125}) = 125 + 1 - \left(\frac{-1 + i\sqrt{19}}{2}\right)^3 - \left(\frac{-1 - i\sqrt{19}}{2}\right)^3 = 112 \text{ etc.}$$

When q is not a power of a small prime, we need other methods of determining the group order. We begin with **Hasse's Theorem**, which will enable us to put an upper and lower limit to the group order.

Theorem 2.3 (Hasse). *Let E be an elliptic curve over the finite field $\mathbb{F}_q$. Then the order of $E(\mathbb{F}_q)$ satisfies*

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}.$$

Proof. Since $\deg(r\phi_q - s) \geq 0$, by property d) of the Frobenius endomorphism we must have

$$r^2q + s^2 - rsa \geq 0,$$
$$q\left(\frac{r}{s}\right)^2 - a\left(\frac{r}{s}\right) + 1 \geq 0$$

for all values of r, s, which requires the discriminant of the quadratic to be non-positive:

$$a^2 - 4q \leq 0,$$
$$|a| \leq 2\sqrt{q}$$

Letting $r = s = 1$ and applying property c), we obtain

$$\begin{gathered}\#E(\mathbb{F}_q) = \deg(\phi_q - 1) = q + 1 - a, \\ q + 1 - \#E(\mathbb{F}_q) = a, \\ |q + 1 - \#E(\mathbb{F}_q)| = |a| \leq 2\sqrt{q}.\end{gathered}$$

This completes the proof of Hasse's Theorem. ■

Being able to limit the group order to an interval of size $4\sqrt{q}$ proves to be extremely useful when paired with one of the fundamental results of group theory — that the order of a point divides the order of the group. If we are able to find a point whose order is greater than $4\sqrt{q}$, only one of its multiples can be in the interval provided by Hasse's theorem, and must therefore be the group order. If the order is smaller than $4\sqrt{q}$, we still have a short list of possibilities. Using additional points can narrow down that list until only one remains.

Example 4 Let E be the curve $y^2 = x^3 + 7x + 12$ over $\mathbb{F}_{103}$. Applying Hasse's theorem, we obtain

$$103 + 1 - 2\sqrt{103} \leq \#E(\mathbb{F}_{103}) \leq 103 + 1 + 2\sqrt{103},$$

$$84 \leq \#E(\mathbb{F}_{103}) \leq 124.$$

One can show that the points $(-1, 2)$ and $(19, 0)$ on E have orders 13 and 2, respectively, so the group order must be a multiple of 26. The only such possibility in the interval [84,124] is 104, so we conclude that the group order must be 104.
These theorems prove to be sufficient to calculate the number of elements in the group. A question that now arises naturally is which integers can occur as the order of an elliptic curve group. The answer is given by the following theorem, proved in [8]:

Theorem 2.4. *Let $q = p^n$ be a power of a prime p and let $N = q + 1 - a$. There is an elliptic curve E defined over $\mathbb{F}_q$ such that $\#E(\mathbb{F}_q) = N$* ***if and only if*** *$|a| \leq 2\sqrt{q}$ (as per Hasse's Theorem) and a satisfies one of the following:*

1. $\gcd(a, p) = 1$,
2. $a = 0, n$ odd or $p \not\equiv 1 \pmod 4$,

3. $a = \pm\sqrt{q}, n$ even or $p \not\equiv 1 \pmod 3$,
4. $a = \pm 2\sqrt{q}, n$ even,
5. n odd, $p = 2$ or $3, a = \sqrt{pq}$.

2.2 Determining the group structure

After establishing the group order, one last step remains — determining the underlying structure of the group. How does one determine whether a group of 36 elements is isomorphic to $\mathbb{Z}_{36}$, $\mathbb{Z}_2 \oplus \mathbb{Z}_{18}$, $\mathbb{Z}_3 \oplus \mathbb{Z}_{12}$ or $\mathbb{Z}_6 \oplus \mathbb{Z}_6$? This theorem, proved in [4], provides a significant level of insight:

Theorem 2.5. *Let $E(\mathbb{F}_q)$ be the group of an elliptic curve E, with $\#E(\mathbb{F}_q) = q + 1 - a = N$. The possible group structures in cases (2) through (5) in Theorem 2.4 are:*

2. $\mathbb{Z}_2 \oplus \mathbb{Z}_{N/2}$ or $\mathbb{Z}_N$ if $q \equiv 3 \pmod 4$; $\mathbb{Z}_N$ otherwise,
3. $\mathbb{Z}_N$,
4. $\mathbb{Z}_{\sqrt{q}\pm1} \oplus \mathbb{Z}_{\sqrt{q}\pm1}$ (using the positive sign when $a = -2\sqrt{q}$ and vice-versa),
5. $\mathbb{Z}_N$.

In cases (1) and (2), the uncertainty can be resolved by imposing the following restriction, as shown in [3]:

Theorem 2.6. *Let $E(\mathbb{F}_q)$ be the group of an elliptic curve E, with $\#E(\mathbb{F}_q) = q + 1 - a = N$. Let $N = p^e n_1 n_2$, with $p \nmid n_1 n_2$, $n_1 | n_2$ and $n_1 | q - 1$. Then*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}_{p^e} \oplus \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}.$$

Remark. When expressing the group isomorphism, the Chinese Remainder Theorem is usually applied to the expression in **Theorem 2.6** in order to obtain a more succinct expression of the form $E(\mathbb{F}_q) \simeq \mathbb{Z}_n$ or $E(\mathbb{F}_q) \simeq \mathbb{Z}_n \oplus \mathbb{Z}_{mn}$ for integers n, m.

These theorems prove to be sufficient in the vast majority of cases, since **Theorem 2.6** very rarely produces different possible factorizations. When it does, one needs to determine the order of a number of individual elements in order to conclude the final structure.

2.3 Solution algorithm, with examples

As we have now established, determining the group structure has two main components — finding the order, and then deducing the structure from it. We illustrate with a few examples:

Example 5 Let E be the curve $y^2 = x^3 + 4x - 1$ over $\mathbb{F}_7$. We wish to determine its order.
Since $\mathbb{F}_7$ is a small field, we can count the points directly using **Theorem 2.1**. The non-zero squares in $\mathbb{F}_7$ are 1, 2 and 4, so we obtain

$$\begin{aligned}
\#E(\mathbb{F}_7) &= 7 + 1 + \sum_{x=0}^{6} \left(\frac{x^3 + 4x - 1}{\mathbb{F}_7} \right) \\
&= 8 + \left(\frac{6}{\mathbb{F}_7} \right) + \left(\frac{4}{\mathbb{F}_7} \right) + \left(\frac{1}{\mathbb{F}_7} \right) + \left(\frac{3}{\mathbb{F}_7} \right) + \left(\frac{2}{\mathbb{F}_7} \right) + \left(\frac{4}{\mathbb{F}_7} \right) + \left(\frac{1}{\mathbb{F}_7} \right) \\
&= 8 - 1 + 1 + 1 - 1 + 1 + 1 + 1 = 11.
\end{aligned}$$

Example 6 Let E be the curve $y^2 = x^3 + 4x - 1$ over $\mathbb{F}_{343}$. We wish to determine its order.
Since $343 = 7^3$, it is a power of a small prime, so we apply **Theorem 2.2**. We know from Example 5 that $\#E(\mathbb{F}_7) = 11$, $a = 7 + 1 - 11 = -3$. Form the polynomial

$$\begin{aligned}
X^2 - aX + q &= (X - \alpha)(X - \beta) \\
X^2 + 3X + 7 &= \left(X - \frac{-3 + i\sqrt{19}}{2} \right) \left(X - \frac{-3 - i\sqrt{19}}{2} \right) \\
\#E(\mathbb{F}_{343}) &= 343 + 1 - \left(\frac{-3 + i\sqrt{19}}{2} \right)^3 - \left(\frac{-3 - i\sqrt{19}}{2} \right)^3 = 308.
\end{aligned}$$

Example 7 We want to determine the order of the group $E(\mathbb{F}_{17})$ defined by the curve $y^2 = x^3 + 5x - 6$. We could apply **Theorem 2.1** here as well, but it would be very inefficient. Instead we turn to **Hasse's Theorem**, which gives us

$$\begin{gathered}
q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}, \\
10 \leq \#E(\mathbb{F}_q) \leq 26.
\end{gathered}$$

A quick observation shows us that $(2,1) \in E(\mathbb{F}_{17})$. Repeatedly applying the addition formula on (3,9) with itself shows that $6(3,9) = \infty$. Since the order of the point divides the order of the group, we must have $\#E(\mathbb{F}_{19}) = 12$, $\#E(\mathbb{F}_{19}) = 18$ or $\#E(\mathbb{F}_{19}) = 24$. Repeating this with the point $(7,6)$ shows that $18(7,6) = \infty$, so we conclude that $\#E(\mathbb{F}_{17}) = 18$.

Remark. For larger groups, computing the order of a point by repeated addition is very time consuming. The **Baby Step, Giant Step** algorithm, described in detail in [7, Ch. 4.3.4], significantly speeds up the process.

Example 8 We want to find the group structure for the groups in examples 5, 6 and 7.

5) The group in example 5 has order 11, so $E(\mathbb{F}_7) \simeq \mathbb{Z}_{11}$.

6) In example 6, we have $\#E(\mathbb{F}_{343}) = 308 = 343+1-36$. Since $\gcd(343, 36) = 1$, **Theorem 2.5** fails to give any information of value. However, we can apply **Theorem 2.6** and write $\#E(\mathbb{F}_{343}) = 308 = 7^1 \cdot 2 \cdot 2 \cdot 11$, which together with the Chinese Remainder Theorem yields

$$E(\mathbb{F}_{343}) \simeq \mathbb{Z}_7 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{22} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{154}.$$

7) In example 7, we have $\#E(\mathbb{F}_{17}) = 18 = 17 + 1 - 0$. Consulting with **Theorem 2.5**, we see that since $a = 0, n$ is odd and $q \not\equiv 3 \pmod 4$, we must have $E(\mathbb{F}_{17}) \simeq \mathbb{Z}_{18}$.

Example 9 We wish to determine the group structure for an elliptic curve $E(\mathbb{F}_{25})$ with $\#E(\mathbb{F}_{25}) = 36$.
We apply **Theorem 2.5** once again. $\#E(\mathbb{F}_{25}) = 36 = 25 + 1 + 10$, so $a = -10 = -2\sqrt{25}$, which places us in case (4). Using the positive sign because $a < 0$, we obtain

$$E(\mathbb{F}_{25}) \simeq \mathbb{Z}_6 \oplus \mathbb{Z}_6.$$

3 Elliptic curves over the rationals

Determining the group structure of an elliptic curve defined over the rational numbers, $E(\mathbb{Q})$, proves to be a much more challenging endeavor, due in large part to the fact that $\mathbb{Q}$ contains an infinite amount of elements. In fact, completely characterizing $E(\mathbb{Q})$ is as yet an unsolved problem in mathematics [5]. Nevertheless, there is a great deal of information to be obtained about the group's behavior.

3.1 The torsion subgroup.

Many important properties of $E(\mathbb{Q})$ can be deduced by looking at its torsion subgroup, i.e. the subgroup consisting of all points of finite order. The following theorem, proved independently by Lutz and Nagell [7, Ch. 8.1], gives two necessary criteria for torsion points on $E(\mathbb{Q})$:

Theorem 3.1 (Lutz-Nagell)**.** *Let E be the curve given by $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$. Let $P = (x, y) \in \mathbb{Q}$. If P has finite order, then*

1. $x, y \in \mathbb{Z}$,
2. $y = 0$ or $y^2 | 4A^3 + 27B^2$.

This is an immensely powerful result, with one extremely important implication. After noting that any elliptic curve with rational coefficients can made to have integer coefficients via a change of variables, applying the **Lutz-Nagell theorem** we not only obtain a finite torsion subgroup $E(\mathbb{Q})^{\text{tors}}$, whose size depends on the divisors of $4A^3 + 27B^2$, but also a complete list of candidates for torsion points, which are easily checked — we simply need to look at the multiples of each point. For any point P, if $nP = \infty$ (or $nP = mP$ with $n \neq m$) then P is a torsion point. If, on the other hand, any nP has non-integer coordinates, then P has infinite order.

Example 10 Let E be the curve $y^2 = x^3 + 4$. $y = 0$ yields no rational solutions, so in order to find the torsion points, we begin by finding the divisors of $4A^2 + 27B^2 = 432$:

$$y^2 | 432 \implies y = \pm 1,\ \pm 2,\ \pm 3,\ \pm 4,\ \pm 6,\ \pm 12.$$

Checking each of these, we only obtain rational points for $y = \pm 2$, corresponding to $x = 0$, so the only possible torsion points are $(0, 2)$ and $(0, -2)$. A simple calculation shows that $3(0, \pm 2) = \infty$, so we conclude that $E(\mathbb{Q})^{\text{tors}} \simeq \mathbb{Z}_3$.

Example 11 Let E be the curve $y^2 = x^3 + 8$. Setting $y = 0$ yields the point $(-2, 0)$, which has order 2. If $y \neq 0$, we have $4A^3 + 27B^2 = 1728$, meaning we need to have $y^2 | 1728$. Checking the list of possibilities, we obtain $(1, \pm 3)$ and $(2, \pm 4)$ as candidates. However,

$$2(1, 3) = (-7/4, -13/8) \text{ and } 2(2, 4) = (-7/4, 13/8)$$

Those points cannot have finite order since their coordinates are not integers, so $\{\infty, (-2, 0)\} = E(\mathbb{Q})^{\text{tors}} \simeq \mathbb{Z}_2$.

This approach is very similar to the method of counting points over $\mathbb{F}_q$ — both rely on checking finite lists of candidates, and both have the disadvantage of being far too inefficient when that list becomes large. In this case, we have two main issues — points of very large order, which might require us to calculate far too many multiples, and discriminants with many divisors, which yield very large lists of candidates. Both of these can be resolved by the reduction mod p map.

3.2 The reduction map

Theorem 3.2. *Let E be an elliptic curve $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$. Let p be an odd prime with $p \nmid 4A^3 + 27B^2$, and let*

$$\rho_p \colon E(\mathbb{Q})^{tors} \to E(\mathbb{F}_p)$$

be the reduction mod p map. Then

1. ρ_p is injective.

2. If $P \in E(\mathbb{Q})$ has finite order and $\rho_p(P) = \infty$, then $P = \infty$.

Proof. 1. See [6].

2. By the Lutz-Nagell theorem, all torsion points have integer coordinates, and will therefore reduce to well-defined, finite points, and ∞ is the only point that will reduce to ∞.

■

An injection between $E(\mathbb{Q})^{\text{tors}}$ and $\mathbb{F}_p$ means that **Hasse's theorem** can be used to provide an upper bound to the size of $E(\mathbb{Q})^{\text{tors}}$. In other words, if we find an odd prime p such that $p \nmid 4A^3 + 27B^2$, then

$$\#E(\mathbb{Q})^{\text{tors}} \leq \#E(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}.$$

We can show that this is a very narrow restriction by considering what values p can take. Assume we have a curve E given by $y^2 = x^3 + Ax + B$, with $3 \nmid A$. This implies $3 \nmid 4A^3 + 27B^2$, and we can use $p = 3$ as our prime. Thus, in some sense, for two thirds of all elliptic curves, we have

$$\#E(\mathbb{Q})^{\text{tors}} \leq \#E(\mathbb{F}_3) \leq 7,$$

so we only need to compute the first 7 multiples of any given point in order to determine if it has finite order or not.

If $3|A$, a larger prime needs to be used, and there is no obvious candidate. However, we can obtain an estimated upper bound for $E(\mathbb{Q})^{\text{tors}}$ by considering the worst case scenario, in which the discriminant has as many distinct prime divisors as possible. We can base our argument on the *primorial function* $n\#$, defined as the product of all primes $p_i \leq n$:

$$n\# = \prod_{k=1}^{\pi(n)} p_k,$$

where p_k is the k:th prime number, and $\pi(n)$ is the prime counting function. Being a prime number analogue to the factorial, the primorial function also grows very quickly: $5\# = 2 \cdot 3 \cdot 5 = 30$, $13\# = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 30030$ and $23\# > 10^8$.

Applying this concept to the context of the reduction map, the primorial of a prime number p is the smallest number than can be divisible by all primes up to and including p. For example, since $13\# = 30030$, for any values of A, B such that $D = 4A^3 + 27B^2 \leq 30029$, at least one of $2, 3, 5, 7, 11, 13$

does not divide D and we can therefore use $p = 13$ for the reduction map to obtain an upper bound for $E(\mathbb{Q})^{\text{tors}}$. By letting $|A|, |B| \leq C$ for some number C, we can tabulate the corresponding upper bounds on $\#E(\mathbb{F}_p)$ for different values of C:

C	$4C^3 + 27C^2$	p	$\#E(\mathbb{F}_p)$
10	6700	13	≤ 21
100	4270000	19	≤ 28
1000	4027000000	29	≤ 40
10^6	$\approx 4 \cdot 10^{18}$	53	≤ 68

This is, of course, a very crude approximation and the resulting estimates are quite conservative. Nevertheless, the values obtained give reasonable bounds to the size of $E(\mathbb{Q})^{\text{tors}}$ — when $|A|, |B| \leq 100$, we would need to compute less than 30 multiples to check if a point has finite order. (Recall that this assumes $3|A$ — if $3 \nmid A$ we only need 7.)

In fact, one can show it always suffices to compute only the first 12 multiples, since the maximum order of a torsion point is twelve. This was proven by Mazur in [2], who showed that the torsion subgroup can only be one of 15 different groups:

Theorem 3.3. *Let E be an elliptic curve over $\mathbb{Q}$. Then the torsion subgroup $E(\mathbb{Q})^{tors}$ is one of the following:*

$$\begin{aligned} E(\mathbb{Q})^{tors} &\simeq \mathbb{Z}_n, && \text{with } 1 \leq n \leq 10 \text{ or } n = 12; \text{ or} \\ E(\mathbb{Q})^{tors} &\simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{2n}, && \text{with } 1 \leq n \leq 4. \end{aligned}$$

Finally, we need to handle the case where $4A^3 + 27B^2$ has many divisors, and thus yields a large number of candidates. Once again, the reduction map proves to be of great use. By **Theorem 3.2**, we have the injection

$$\rho_p \colon E(\mathbb{Q})^{\text{tors}} \to E(\mathbb{F}_p)$$

when $p \nmid 4A^3 + 27B^2$. This immediately implies that the order of $E(\mathbb{Q})^{\text{tors}}$ must divide the order of $E(\mathbb{F}_p)$. We can therefore use different values of p for the reduction map to find different sizes of $E(\mathbb{F}_p)$ until they only have one common divisor, which must then be the order of $E(\mathbb{Q})^{\text{tors}}$.

Example 12 Let E be the curve $y^2 = x^3 + 18x + 72$. Its discriminant is

$$D = 4A^3 + 27B^2 = 163296 = 2^5 \cdot 3^6 \cdot 7.$$

We could apply the Lutz-Nagell theorem and check all points satisfying $y^2|D$. Instead, we use the reduction map and consider $E(\mathbb{F}_5)$ and $E(\mathbb{F}_{11})$. We can easily show that $\#E(\mathbb{F}_5) = 5$ and $\#E(\mathbb{F}_{11}) = 8$. Consequently, the order of $E(\mathbb{Q})^{\text{tors}}$ must divide both 5 and 8, and $E(\mathbb{Q})^{\text{tors}}$ is thus trivial.

With these tools, we can determine the structure of the torsion subgroup of an elliptic curve over the rationals. How do we then proceed in order to characterize the entire group? Unfortunately, this proves to be an infinitely more difficult task. The most important result is given by the **Mordell-Weil Theorem**:

Theorem 3.4 (Mordell-Weil). *Let E be an elliptic curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is a finitely generated abelian group.*

Proof. A detailed proof, based on showing the finiteness of $E(\mathbb{Q})/2E(\mathbb{Q})$ and applying a variation of the method of infinite descent, can be found in [7, Ch. 8.]

This result, together the fundamental theorem of finitely generated abelian groups, means we can express any elliptic curve group over $\mathbb{Q}$ as the direct sum of a finite number of copies of the integers $\mathbb{Z}$ and the torsion subgroup we have discussed throughout this chapter:

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})^{\text{tors}}.$$

The integer r, called the *rank* of the curve, is the subject matter of much mathematical research, including the Birch and Swinnerton-Dyer conjecture [10]. It is still not known how to compute the rank in the general case, or even if the rank can be arbitrarily large [5].

3.3 Determining the torsion subgroup, with examples

To determine the torsion subgroup $E(\mathbb{Q})^{\text{tors}}$, we first need to determine its order and then use that to deduce the structure. The following examples demonstrate the process:

Example 13 Let E be the curve given by $y^2 = x^3 + 1$. The discriminant for this curve is $D = 27$. Applying the Lutz-Nagell theorem, we need $y = 0$ or $y|27$. Setting $y = 0$ yields the point $(-1, 0)$, while $y^2|27$ yields $y = \pm 1$ and $y = \pm 3$ as candidates. We first check which of those values produce rational points — if $y = \pm 1$ we need to have $x = 0$, while $y = \pm 3$ implies $x = 2$. Consequently, we have 5 candidates for torsion points: $(-1, 0), (0, \pm 1), (2, \pm 3)$. A quick calculation shows that adding the point $(2, 3)$ to itself produces all the other points : $2(2, 3) = (0, 1),\ 3(2, 3) = (-1, 0),\ 4(2, 3) = (0, -1),\ 5(2, 3) = (2, -3),\ 6(2, 3) = \infty$, so we conclude that

$$E(\mathbb{Q}) \simeq \mathbb{Z}_6.$$

Example 14 Let E be the curve given by $y^2 = x^3 - 219x + 1654$. We want to use the reduction map, so we begin by factorizing the discriminant:

$$D = 31850496 = 2^{17} \cdot 3^5.$$

Applying the reduction mod 5 map, we obtain the curve $E_5 \colon y^2 = x^3 + x + 4$. Using the methods of Chapter 2, we can show that $\#E_5(\mathbb{F}_5) = 9$, so the order of $E(\mathbb{Q})^{\text{tors}}$ must be a multiple of 9. However, Theorem 3.3 states that the order of $E(\mathbb{Q})^{\text{tors}}$ can not be larger than 16, so we must have $\#E(\mathbb{Q})^{\text{tors}} = 9$. Additionally, the only group of order 9 allowed by Theorem 3.3 is $\mathbb{Z}_9$, so we must have

$$E(\mathbb{Q})^{\text{tors}} \simeq \mathbb{Z}_9.$$

Example 15 Let E be the curve given by $y^2 = x^3 - x$. Its discriminant is $D = -4$, so according to the Lutz-Nagell theorem we must have $y = 0$, $y = \pm 1$, $y = \pm 2$ or $y = \pm 4$. Checking all of these, the only rational solutions we obtain are $(0, 0)$, $(1, 0)$ and $(-1, 0)$. For the other 3 points, we have $2(0, 0) = 2(1, 0) = 2(-1, 0) = \infty$, so we conclude that

$$E(\mathbb{Q})^{\text{tors}} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

References

[1] Fulton, W., 2008. *Algebraic Curves: An Introduction To Algebraic Geometry* [pdf]. **Available at**: <`http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf`>[Accessed 18 May 2016].

[2] Mazur, B., 1978. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Inventiones Mathematicae*, 44(2), p.129–62.

[3] Rück, H.-G., 1987. A note on elliptic curves over finite fields. *Mathematics of Computation*, 49(179), p.301-04.

[4] Schoof, R., 1985. *Non-singular plane cubic curves over finite fields*, [Ph.D. Thesis], University of Amsterdam.

[5] Silverman, J. H., 2009. *The arithmetic of elliptic curves.* 2nd ed. New York : Springer-Verlag.

[6] Washington, L.C., 1997. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*, 2nd ed. New York : Springer-Verlag.

[7] Washington, L.C., 2008. *Elliptic Curves - Number Theory and Cryptography.* 2nd ed. Boca Raton : Chapman & Hall/CRC.

[8] Waterhouse, W.C., 1969. Abelian varieties over finite fields. *Annales scientifiques de l'École Normale Supérieure*, 4(2), p.521-60.

[9] Wiles, A., 1995. Modular elliptic curves and Fermat's Last Theorem. *Annals of Mathematics* 141(3), p.448

[10] Wiles, A., 2006. The Birch and Swinnerton-Dyer conjecture. In Carlson, J., Jaffe, A., Wiles, A., *The Millenium Prize Problems.* American Mathematical Society, p.31-44.