UPPSALA
UNIVERSITET

U.U.D.M. Project Report 2019:32

Elliptic Curves
A journey through theory and its applications

Harady Hasan

Examensarbete i matematik, 15 hp
Handledare: Andreas Strömbergsson
Examinator: Martin Herschend
Juni 2019

Department of Mathematics
Uppsala University

Abstract

Back in the 1980's and the years following it, new methods were introduced for primality testing and integer factorization. This thesis aims to present a thorough understanding of the theory behind elliptic curves, especially when they are defined over finite fields, in order to demonstrate their use in these applications. Furthermore, it deals with the application of such curves in the field of cryptography and discusses how and why it supports the art of encryption.

Table of Contents

1 Review

Before starting with the actual subject of this paper, as a help to the reader we give a short review of some basic definitions and results, which play an important role in the subject of elliptic curves. As we will see later,the theory of elliptic curves involves elements from algebra, analysis, number theory and geometry.

Algebra
Definition of a **Group**: A group G is a set of elements with an operation $+$ satisfying the following axioms:
i) addition is associative,
ii) there exists an identity element **0** and
iii) for each element there exists an additive inverse.
- If $a + b = b + a$ for all $a, b \in G$, then G is called commutative(Abelian group)[1].

Definition of a **Field**: A field F is a set of elements together with two operations $+$ and $*$ such that it satisfies:
i) F under $+$ is a commutative group,
ii) the operation $*$ is associative
iii) the operation $*$ is commutative
iv) there exists a multiplicative identity **1**
v) there exists a multiplicative inverse for each non-zero element
vi) the distributive property holds.

- A field F containing a field E as subfield is called an extension field of E. In this situation, if an element $\alpha \in F$ is the root of some polynomial with coefficients in E, then α is called algebraic over E. If all elements of F are algebraic over E, then F is called an algebraic extension of E.
- A field F is called algebraically closed if all non-constant polynomials with coefficients in F have a root in F.
- The algebraic closure of a field F is a field $\overline{F}$ containing F such that.:
i) $\overline{F}$ is an algebraic extension of F,
ii) $\overline{F}$ is algebraically closed.

- The characteristic of a field F, $char(F)$, is the smallest positive integer n such that

$$n\mathbf{1} = \underbrace{\mathbf{1} + \mathbf{1} + \cdots + \mathbf{1}}_{n \text{ times}} = 0.$$

If the characteristic of a field is not finite, then $char(F) = 0$.

Number Theory

- The greatest common divisor of two positive integers is denoted $gcd(a, b)$. If $gcd(a, b) = 1$, then a and b are said to be coprime.
- Fermat's Little theorem: Let p be a prime and a be any positive integer. Let $gcd(a, p) = 1$. Then $a^{p-1} \equiv 1(mod\ p)$.

Geometry

The equation of a straight line is

$$y = kx + m = kx + (y_1 - kx_1) = k(x - x_1) + y_1.$$

2 Introduction

The purpose of this paper is not to answer a specific question or derive some new result: it instead aims to provide a thorough understanding of elliptic curves, how they are defined and in what applications we can benefit from them.

As we will see in this paper, the subject of elliptic curves is a strong combination of abstract algebra and number theory, and two of the main applications of elliptic curves are in integer factorization and cryptography. The first uses elliptic curves to decide whether a given large integer is prime or composite, and if composite, then return one of its proper divisors. In the second application, elliptic curves are used in cryptographic protocols such as Bitcoin or Austrian smart e-ID, just to mention a few[2][3]. Later we will discuss each of these applications carefully and in-depth.

This far we have used the term "elliptic curves" without giving a formal definition of the term. At this point it is very natural to ask what they are. The following example starts from a natural and easy-to-understand problem which leads to a discussion of a specific elliptic curve. After the example we will give a precise definition of the term.

Example 2.1:
Does there exist a positive integer y s.t. its square equals the sum of the squares of the first x positive integers[4]? I.e. we want to find a pair (x,y) such that

$$1^2 + 2^2 + ... + x^2 = y^2 \tag{2.1}$$

This can be simplified in the following way:
We know that

$$\sum_{n=1}^{k} n = \frac{k(k+1)}{2}.$$

Another useful result is the following:

$$n^3 - (n-1)^3 = 3n^2 - 3n + 1.$$

The sum of this equation can be computed as:

$$\sum_{n=1}^{k}(n^3-(n-1)^3)=(1^3-0^3)+(2^3-1^3)+(3^3-2^3)+...+(k^3-(k-1)^3)=k^3.$$

Why? Because when noticing the terms carefully, one will see that all terms wipe each other out except for the second and second to last terms, giving a total of $k^3-0^3=k^3$. Thus we can rewrite the sum of the squared integers as:

$$\sum_{n=1}^{k}(n^3-(n-1)^3)=\sum_{n=1}^{k}(3n^2-3n+1)=3\sum_{n=1}^{k}n^2-3\sum_{n=1}^{k}n+\sum_{n=1}^{k}1=k^3$$
$$\Rightarrow\sum_{n=1}^{k}n^2=\frac{k^3+\frac{3}{2}k(k+1)-k}{3}=\frac{k(k+1)(2k+1)}{6}.$$

Thus we can rewrite equation (2.1) as

$$\sum_{i=1}^{x}i^2=\frac{x(x+1)(2x+1)}{6}=y^2. \tag{2.2}$$

The equation (2.2) is a special case of a much more general family of equations. Now, turning back to our aim with this example, what solutions do there exist? It is obvious, by a simple calculation, that the pairs $(x,y)=(0,0)$ and $(x,y)=(1,1)$ do indeed satisfy equation (2.2). The figure below graphs equation (2.2) where a straight line is drawn through both solution points:

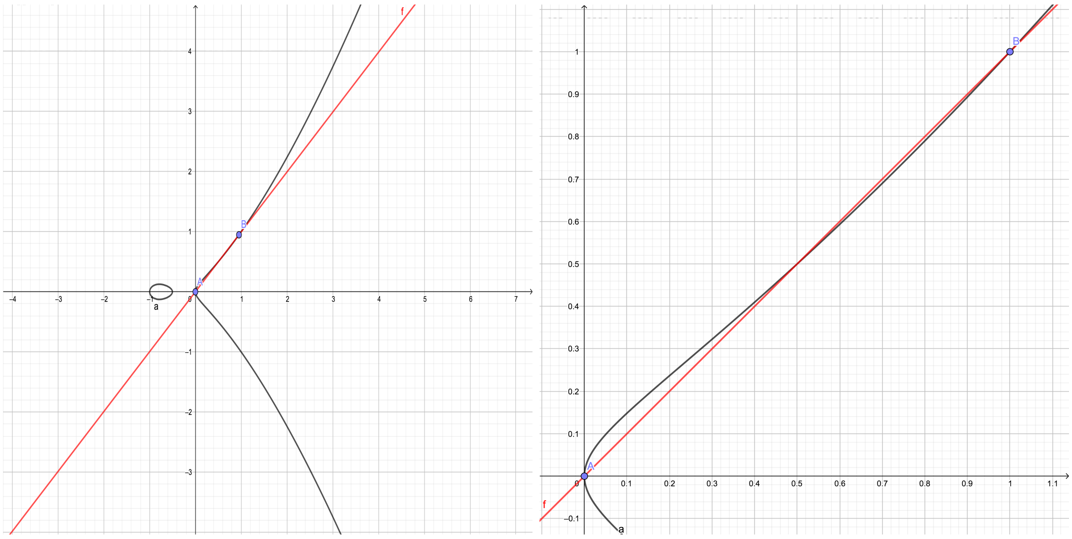


Figure 2.1: Graph of equation (2.2) (left) and zoomed-in version(right)

From this graphical representation it is obvious the line through $(x,y)=(0,0)$ and $(x,y)=(1,1)$ intersects the curve in another point. Thus we would like to know that point of intersection, in the hope to find the solution to our problem. The equation of this line can be found as:

$$y = kx + m$$

where in this case the line has equation(easily checked),

$$y = x.$$

Substituting this into equation (2.2) we obtain

$$y^2 = x^2 = \frac{x(x+1)(2x+1)}{6} \Rightarrow x^3 - \frac{3}{2}x^2 + \frac{1}{2}x = 0.$$

Solving this cubic equation yields another root at

$$x = \frac{1}{2} \Rightarrow y = \frac{1}{2}.$$

Since we know two of the roots $x = 0$ and $x = 1$ already, it is easy to find the third root by factorization, which also implies that this new root is rational. Thus we have found a new point $(\frac{1}{2}, \frac{1}{2})$ on the curve, even though it does not satisfy our aim for integer solutions. But at least the method used to find this point seems to generate new points with rational coordinates on the curve, therefore we continue in a similar manner. Also, the curve of equation (2.2) is symmetric about the x-axis therefore the point $(\frac{1}{2}, -\frac{1}{2})$ also lies on the curve. Cf. the following figure:

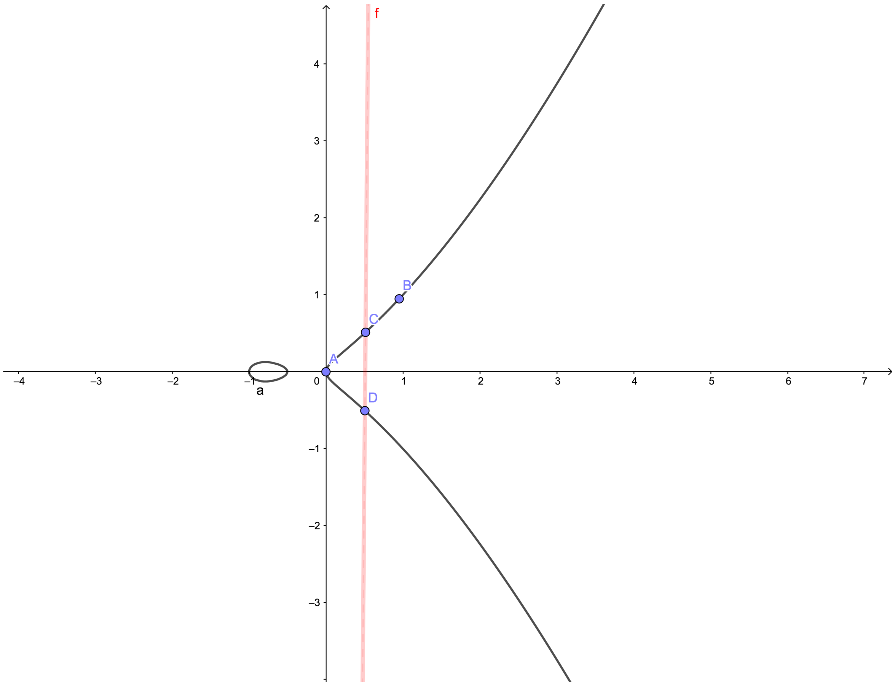


Figure 2.2: Graph of equation (2.2)

Next, we take the points $(1,1)$, $(\frac{1}{2}, \frac{-1}{2})$ and repeat the addition method. We obtain the line

$$y = 3x - 2.$$

Substituting that line into equation (2.2) we obtain

$$y^2 = (3x-2)^2 = \frac{x(x+1)(2x+1)}{6} \Rightarrow x^3 - \frac{51}{2}x^2 + \frac{73}{2}x - 12 = 0.$$

A new root of this equation is at

$$x = 24 \Rightarrow y = 3 \cdot 24 - 2 = 70$$

yielding a new point $(24,70)$ on the curve. Now, we can state that we have found an integer solution to our problem, namely that the sum

$$1^2 + 2^2 + ... + 24^2$$

equals a perfect square, in this case 70^2.□

Having finished **Example 2.1**, it is a perfect time to define the term "elliptic curve". An elliptic curve is not the same thing as an ellipse, there are historical reasons for the name, but the connection between the two curves is quite remote. Notice that our solutions to **Example 2.1** were real valued, since we were working in the real numbers. By [4], given a field F, an elliptic curve is:

$$E : y^2 = x^3 + Ax + B, \ with \ A, B \in F, \tag{2.3}$$

i.e any curve represented by such an equation (2.3) is called an elliptic curve. The set of solutions (x,y) to (2.3) is considered with x,y lying in the field F, or alternatively in some extension field $\overline{F}$ of F . We say that E is defined over the field F, since $A, B \in F$. That field may be $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or a finite field F_p where p is a prime or a prime power.

An equation of the form (2.3) is said to be in the Weierstrass form. It is a special case of the more flexible equation, called generalized Weierstrass form,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.4}$$

A change of variables of the equation (2.4) takes us to equation (2.3). A natural question is why there exist two types of such equations. Indeed, there exist a third type, which also is derived from equation (2.4) through a change of variables, which looks like

$$y^2 = x^3 + a_2'x^2 + a_4'x + a_6' \tag{2.5}$$

for some constants a'_2, a'_4 and a'_6. Equation (2.3) is used when the characteristic of the field, which the curve E is defined over, is not 2 or 3. Equation (2.5) is used when the characteristic of F is distinct from 2. The generalized form (2.4) works well in fields with characteristic of 2 and 3. That the characteristic of the field F is different from 2 or 3 means that we can divide by 2 or 3 in the field, respectively.

The following figure is an example of two more elliptic curves:

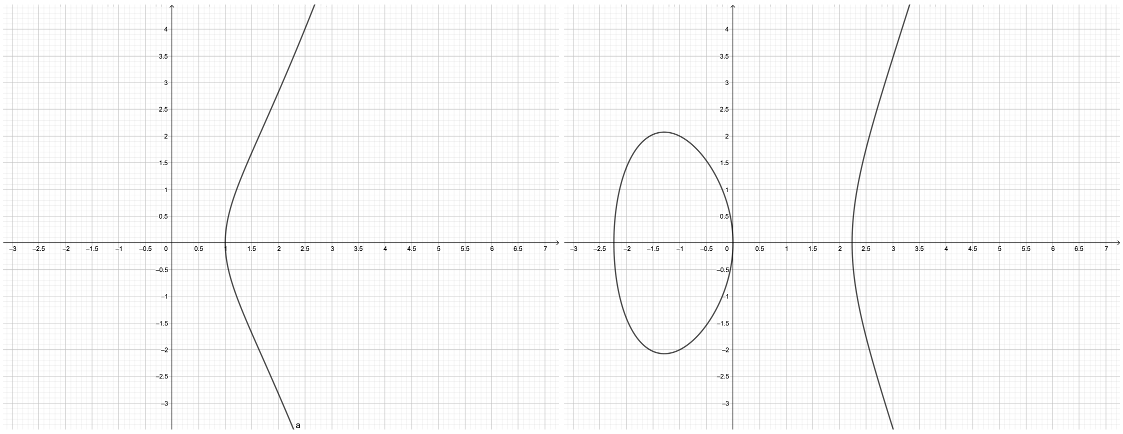


Figure 2.3: Two elliptic curves. Left: $y^2 = x^3 - 1$, Right: $y^2 = x^3 - 5x$

Notice that all the elliptic curves which we have shown share one common property, namely that they are all symmetric about the x-axis.
Why is that so? This is because $(-y)^2 = y^2$, hence the point (x, y) is on the curve if and only if $(x, -y)$ is on the curve.

In the next section we will see how the points on E form the structure of a group.

2.0.1 The Group Law

In the previous section we witnessed that an elliptic curve is nothing more than a set of points, and also we implemented an operation on those elements, to produce new elements. Looking back at the definition of a group, we may see similarities between a group and an elliptic curve. The aim of this section is to show that an elliptic curve indeed possesses the structure of a group. For that purpose, we mention two extra constructions.

The first one is that we create a new element called **point at infinity**, which we denote $\infty = (\infty, \infty)$, where it will be on the top and bottom of any line as well as the y-axis.

What is the reason for that new element? Imagine figure 2.4 where two lines are parallel, where do they meet?

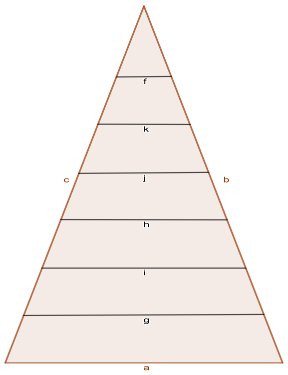


Figure 2.4: Parallel lines intersect at infinity

Intuitively, two parallel lines meet at infinity, therefore we also call that point "point at infinity". If two parallel lines meet at infinity, then each of the lines itself intersect the point at infinity. Thus a vertical line through a point on the curve will intersect the curve at the point ∞. This new point will be the natural identity element in the elliptic curve group, that's why we include it in E, in order to do operations with this and any other element.

The second construction is that we define an operation. That operation, called **addition of points on elliptic curves**, is defined as follows:

Take any two points P and Q on E and draw a straight line through them. That line will intersect the curve in exactly on more point, and that intersection point is found by substituting the equation of the line into equation (2.3) and finding the roots of the cubic. As we already know two of the roots, the third one is easy to find, by factorization. Now we have a new point on the curve, call it $R = (x, y)$. Reflect that point over the x-axis to obtain $-R = (x, -y)$. We have earlier shown that $-R$ lies on the curve if so does R. Thus addition of two points is defined as:

$$P + Q = -R \tag{2.6}$$

as shown in figure 2.5, where S is the reflection of R, i.e. $-R$.

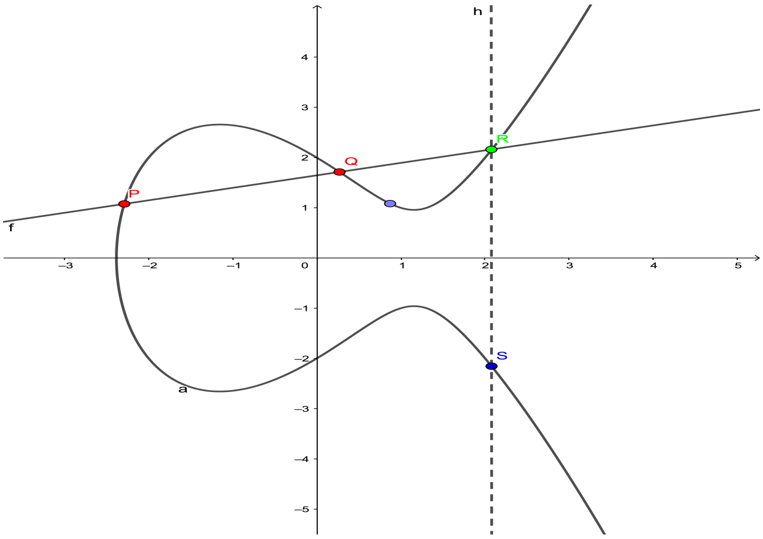


Figure 2.5: Addition of two points on an elliptic curve

Now that we have a notion of addition of two points on an elliptic curve, what kind of points can be added together and what is the result of that operation? There are indeed several cases.

Case I

$P = (x_1,y_1)$ and $Q = (x_2,y_2)$ where $x_1 \neq x_2$ and $y_1 \neq y_2$. Draw a line through them and find the point of intersection with the curve. The equation of the line is

$$y = kx + m = kx + (y_1 - kx_1) = k(x - x_1) + y_1, \tag{2.7}$$

where

$$k = \frac{y_2 - y_1}{x_2 - x_1}.$$

Set

$$y^2 = (k(x - x_1) + y_1)^2 = x^3 + Ax + B \tag{2.8}$$

and rearrange terms to obtain

$$x^3 - k^2x^2 + ... = 0. \tag{2.9}$$

We can write any cubic polynomial as

$$x^3 + ax^2 + bx + x = (x - x_1)(x - x_2)(x - x_3) = x^3 - (x_1 + x_2 + x_3)x^2 + ... = 0 \tag{2.10}$$

Thus having two of the roots x_1, x_2, the third one is found as

$$k^2 = x_1 + x_2 + x_3 \Rightarrow x_3 = k^2 - x_1 - x_2 \Rightarrow y_3 = k(x_3 - x_1) + y_1 \Rightarrow -y_3 = k(x_1 - x_3) - y_1. \tag{2.11}$$

Thus $P + Q = -R = (x_3, -y_3)$.

Case II
What if both points have the same x-coordinate but different y-coordinates? That's $P = (x, y_1)$ and $Q = (x, y_2)$. A line through them will be vertical, and we mentioned about the construction of the point at infinity for this purpose, because that line through P and Q will intersect the curve at ∞, therefore $P + Q = \infty$.

Case III
It can also happen that we want to add a point $P = (x_1, y_1)$ to itself, in fact this is mainly what we will do in applications. Imagine that we add the points P and Q where Q approaches P, so that the distance between them is negligible. Then the line through them also changes as Q moves towards P and becomes the line tangent to the curve at point P. This makes finding the equation of the line easy, as we can use implicit differentiation to obtain the slope of that line. Recall equation (2.3), then

$$\frac{d}{dx}(y^2) = \frac{d}{dx}(x^3 + Ax + B) \Longleftrightarrow 2yy' = 3x^2 + A \Rightarrow y' = \frac{3x_1^2 + A}{2y_1}. \tag{2.12}$$

Thus

$$\frac{dy}{dx} = y' = k \Rightarrow y = k(x - x_1) + y_1. \tag{2.13}$$

The new point is found as in Case I.

Case IV
Finally, it can be the case that we want to add any point P with ∞. Intuitively, any line through P and ∞ will be a vertical line, it will intersect the point $-P$, P's reflection. Reflecting that point takes us back to P. Hence

$$P + \infty = P. \tag{2.14}$$

Remark I
When two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are added, the coordinates of $P + Q = (x_3, -y_3)$ is most easily found by the following two equations:

- $x_3 = k^2 - x_1 - x_2$
- $-y_3 = k(x_1 - x_3) - y_1$

Now that we have a neutral point and also defined what addition of two points on an elliptic curve means, we prove that the set of points on a curve E together with the addition operation define a group.

Theorem I, [4]
Let E be an elliptic curve and $+$ be the operation of addition of two points on E. Then:
i) E has an identity element ∞ s.t. $P + \infty = P, \forall P \in E$.
ii) Each point P has an inverse $-P$, where $P + (-P) = \infty$.
iii) Associativity holds, i.e. $(P + Q) + R = P + (Q + R)$.
- Furthermore, E is commutative, i.e. $P + Q = Q + P, \forall P, Q \in E$.
Thus E is an Abelian group.

Proof
i) $P + \infty = P \ \forall P \in E$. This is Case IV above.
ii) As E is symmetric about the x-axis, for all $P = (x,y)$ on E, also $-P = (x, -y)$ lies on E. A line through them intersects ∞. Again, this is Case IV above.
iii) The associativity property is harder to prove and requires understanding projective and affine geometry, among other things. Therefore it is omitted.
- Commutativity is obvious, as a line through P, Q is the same line through Q, P. Therefore $P + Q = Q + P$.

The reflection $-P = (x, -y)$ of a point $P = (x,y)$ holds only in equation (2.3). If the characteristic of the field is 2 or 3, then we use the more general Weierstrass equations (2.4) and (2.5), thus the inverse of a point also changes into something else. For that reason, we need to be careful with what curve equation we have, since not all of them behave nicely. That is the content of the next section.

2.0.2 Singularities

So far, our use of elliptic curves has assumed that the cubic polynomial in (2.3), i.e. $x^3 + Ax + B$ appearing in (2.3), has three distinct roots, without explicitly stating it. An interesting question is then what happens when the roots are not all distinct? Indeed, quite often that can be the case, especially when the curve is defined over the integers reduced modulo different primes.

Let us first take the case where the polynomial $x^3 + Ax + B$ has a triple root at $x = 0$, that is

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

Thus $(0,0)$ is the only singular point. What's a singular point? It is a point where the curve has a cusp or a self-intersection. Indeed, our curve has a cusp at $(0,0)$, as it can be seen from figure 2.6 Thus excluding $(0,0)$ from (2.3), all the other non-singular points on the curve will create a group as we have explained in the previous section. The reason why we exclude $(0,0)$ is because a line through $(0,0)$ and any other point will not intersect the curve in a third point, therefore addition cannot be performed with $(0,0)$.

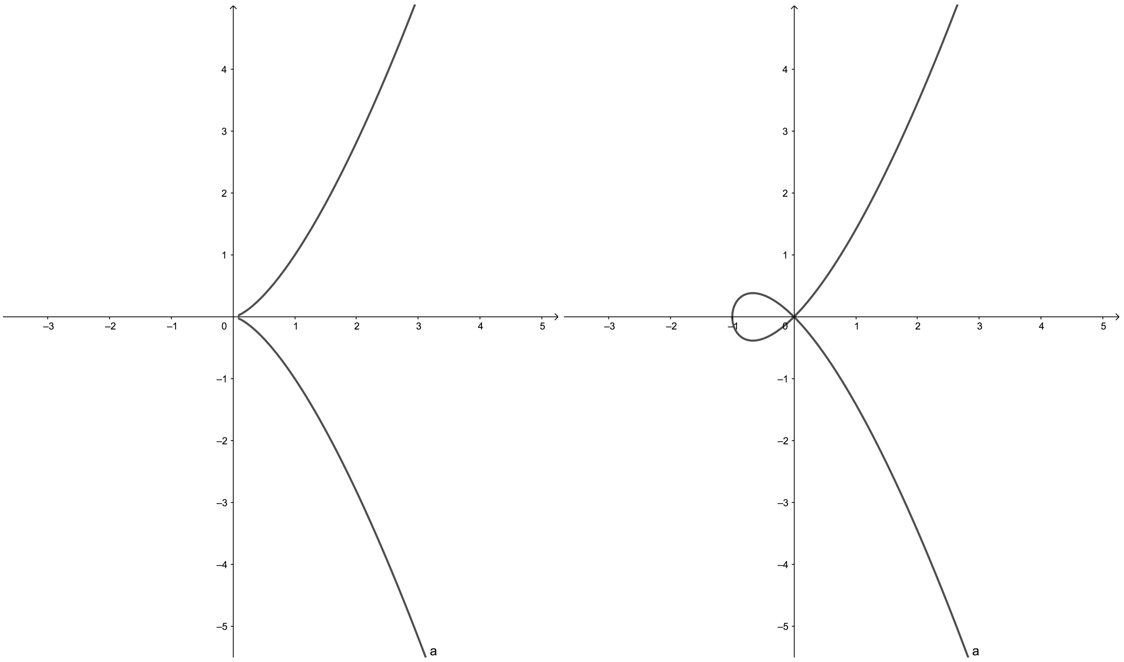


Figure 2.6: Two singular curves. Left: $y^2 = x^3$, Right: $y^2 = x^2(x + 1)$

If the polynomial $x^3 + Ax + B$ appearing in (2.3) has a double root, then the curve E again has a singular point corresponding to this root. This can be seen in the right part of figure 2.6. Note that the polynomial $x^2(x + 1)$ has a double root at $x = 0$. The curve intersects itself at $(0,0)$; therefore this point is called a singular point. In general, if $x^3 + Ax + B$ has a double root at $x = 0$, then the elliptic curve E is of the form $y^2 = x^2(x + a)$ for some non-zero a.

Formalizing the above special cases: An elliptic curve E is called singular if and only if it has some singular point, or equivalently if and only if the polynomial $y^2 = x^3 + Ax + B$ does not have three distinct roots. This is known to hold if and only if the *discriminant* of E is zero. By definition, the discriminant of a curve $E : y^2 = x^3 + Ax + B$ is $\triangle = -(4A^3 + 27B^2)$[5].

Here is an example of how a non-singular curve defined over $\mathbb{R}$ can give rise to singular curves when reducing the integers modulo a prime:

Example 2.2 Let $E : y^2 = x(x+35)(x-55)$ be the equation of a curve. Then
E mod 5: $y^2 = x^3$,
E mod 7: $y^2 = x^2(x+1)$, and
E mod 11: $y^2 = x^2(x+2)$.

2.0.3 Finite Fields

Before proceeding to applications of elliptic curves, there is one more important piece of theory that needs to be covered, namely that of elliptic curves defined over finite fields. When the field is not finite, such as the field of real numbers or rational numbers, the number of points on a curve can be infinitely large, making it difficult to be used in applications. After all, we want to be able to count the number of points on the curve, or even more importantly, to be able to to find the order of any given point on the curve. Therefore, we define elliptic curves over finite fields, which is the basis of applications. The reminder of this section will deal with some examples of elliptic curves over finite fields and relating theorems and an algorithm for fast computation.

Example 2.2
Let F_5 be a finite field and $E : y^2 = x^3 + x + 1 (mod\ 5)$.

$$F_5 = \{0, 1, 2, 3, 4\}.$$

We now determine all points on this curve, by plugging in x into the equation for each x and finding the corresponding y-values if it exists:

- $x = 0 \Rightarrow y = \pm 1 \Rightarrow y = 1, 4 (mod\ 5)$
- $x = 1 \Rightarrow y$ does not exist
- $x = 2 \Rightarrow y = \pm 1$
- $x = 3 \Rightarrow y = \pm 1$

- $x = 4 \Rightarrow y = \pm 2 \Rightarrow y = 2,3(mod\ 5)$

We shall not forget about the point at infinity, which by definition will belong to the set of points on E. Thus we have the following points on E:

$$E = \{\infty, (0,1), (0,4), (2,1), (2,4), (3,1), (3,4), (4,2), (4,3)\}.$$

Let's find the order of the element $(0,1)$:

- $2(0,1) = (0,1) + (0,1)$:

First, we need to find the equation of the line $y = kx + m$ where in this case the slope is: $2yy' = 3x^2 + 1 \Rightarrow y' = \frac{1}{2} \equiv 3(mod\ 5)$.

Notice that we found the residue class representing $\frac{1}{2}(mod\ 5)$ by finding the multiplicative inverse of the denominator, $2^{-1} \equiv 3(mod\ 5)$, and multiplying it by 1, the numerator.

In general, suppose we want to find the residue class of $\frac{a}{b}(mod\ \text{n})$: notice that $\frac{a}{b} = ab^{-1}$ where b^{-1} is the multiplicative inverse of b. b admits a multiplicative inverse if and only if $gcd(b,n) = 1$. Then

$$\frac{a}{b} \equiv ab^{-1}(mod\ n).$$

Following Remark I we find the coordinates of $2(0,1)$ to be:

- $x_3 = k^2 - x_1 - x_2 = 9 \equiv 4(mod\ 5)$
- $-y_3 = k(x_1 - x_3) - y_1 = 3(0-4) - 1 \equiv 2(mod\ 5)$

Thus $2(0,1) = (4,2)$. Similarly, we proceed to find the other multiples of our chosen point:

- $3(0,1) = 2(0,1) + (0,1) = (4,2) + (0,1) \Rightarrow k = 4 \Rightarrow (x_3, -y_3) = (2,1)$
- $4(0,1) = (2,1) + (0,1) \Rightarrow k = 1 \rightarrow (x_3, -y_3) = (3,4)$
- $5(0,1) = (3,4) + (0,1) = (3,1)$
- $6(0,1) = (3,1) + (0,1) = (2,4)$
- $7(0,1) = (2,4) + (0,1) = (4,3)$
- $8(0,1) = (4,3) + (0,1) = (0,4)$
- $9(0,1) = (0,4) + (0,1) = \infty$

Why does that happen? Because $k = \frac{3}{0}$ and 0 does not admit any multiplicative inverse modulo 5.
From this example we can see that the elliptic curve group is cyclic and $(0,1)$, whose order is 9, is a generator of it. This implies that $E(F_5) \cong \mathbb{Z}_9$.

Example 2.3
Let $E : y^2 = x^3 + 2(mod\ 7)$ be an elliptic curve defined over the finite field $F_7 = \{0,1,2,3,4,5,6\}$. Following the method in the previous example we can find the points on the curve E to be:

$$E = \{\infty, (0,3), (0,4), (3,1), (3,6), (5,1), (5,6), (6,1), (6,6)\}.$$

As an example, consider the point $(0,3)$. $2(0,3)$ is computed as follow:

- $k = \frac{3x^2}{2y} = 0 \Rightarrow x_3 = k^2 - 2x_1 = 0$ and $y_3 = k(x_1 - x_3) - y_1 = -3 \equiv 4(mod\ 7)$. Thus $2(0,3) = (0,4)$.
- $3(0,3) = 2(0,3) + (0,4) = \infty$ as both points have the same x-coordinate.

Hence $(0,3)$ has order 3. Similar computations shows that all other points, except the point at infinity, also have order 3. As the elliptic curve group has 9 elements, it is isomorphic to $\mathbb{Z}_3 \oplus \mathbb{Z}_3$.

A theorem that generalizes the two previous results is the following:

Theorem[4]
Let F_q be any finite field and an elliptic curve E be defined over it. Then $E(F_q)$ is either isomorphic to $\mathbb{Z}_n$ for some n or $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ for some n_1, n_2 with n_1 being a divisor of n_2.

Remark II
As we saw in the examples, it is quite tedious to compute nP for an integer n and a point P, therefore we need an algorithm that makes this computation faster.

Algorithm for fast computation
Let n be an integer and P be a point on a curve E. Then nP is most easily computed as:

- $nP = 2(\frac{n}{2}P)$ if n is even
- $nP = P + 2(\frac{n-1}{2}P)$ if n is odd.

This way computations become much faster, instead of adding a point to itself n times. For example $13P$ is computed as:

- $P + P = 2P$
- $2P + 2P = 4P$
- $4P + 4P = 8P$
- $8P + 4P = 12P$
- $12P + P = 13P$

Thus we can compute $13P$ in five steps instead of 13 steps.

Now we have developed the necessary theory of elliptic curves and are ready to discuss the applications of it more thoroughly.

3 Applications In Number Theory

Assume we are given a large number n, for example

$$n = 3^{72} - 10 = 22528399544939174411840147874772631$$

which consists of 35 digits. Is this number prime or not? If it is prime, then a proof is necessary, otherwise how can we be sure of that fact. On the other hand, if this number is not prime, then it did fail to pass a primality test, such as the Fermat's primality test, in which case the number must be composite. It is of interest to find at least one of its prime divisors, or even better, all of its prime divisors $p_1, p_2, ..., p_k$.

This problem has fascinated mathematicians throughout known history, therefore many of them introduced new methods for solving this problem. The easiest one of these methods is to try, by trial and error, to divide n by the numbers $\{2, 3, 4, ..., n-1\}$. A small improvement would be to avoid to divide by the numbers that are multiples of numbers which have already been tested and failed, since if for example n is not divisible by 2, then it cannot be divisible by 4. In this way we are only left with the primes in the list. Even better would be to avoid dividing by primes greater than the square-root of n, since every composite number has a prime divisor less than or equal to the square root of it. Why does that hold? Assume that $n = p_1 \cdot p_2 \cdots p_k$, where $p_1, p_2, \cdots p_k$ are primes and $k \geq 2$, then if $p_1 > \sqrt{n}$ it implies

$$p_2 \leq \frac{n}{p_1} < \frac{n}{\sqrt{n}} = \sqrt{n}.$$

Even though this method feels quite natural to use, it fails to produce any answer in a reasonable amount of time when the number which we are about to factorize has very large prime factors. In fact, the numbers used in cryptography for example, have hundreds of digits.

Another primality test, which is even slower than the previous one is Wilson's theorem, which states that a positive integer n is prime iff $(n-1)! \equiv -1(mod \text{ n})$.

There are also primality tests which are not deterministic as the ones above, but they produce a probability for an integer being prime. Thus higher probability better ensures primality. Fermat's little theorem is one such primality test.

A desired method for primality test would be a deterministic one that for a given input outputs either True or False for the input being prime. A test for integer factorization should output a list of all the prime divisors of its input. The next two sections show how elliptic curves can be used to solve these two problems.

3.0.1 Integer Factorization

The nature of integer factorization is much harder than that of primality testing. There are deterministic tests which can quickly prove that a number is composite without finding a prime divisor of it. According to [4], the largest integers, which are products of two large primes, which could be factorized up to the year 2007 had around 200 digits, while around same time the integers which could be proved to be prime had thousands of digits.

The reason behind elliptic curves being used for integer factorization is that firstly the classical methods were based on multiplicative groups $(\mathbb{Z}_p)^*$ for finding a prime divisor p. As the points on elliptic curves also admits a group structure, these groups can be replaced and we can use elliptic curves to generate a group from which we try to find the prime factors of an integer. Secondly and very importantly, as we can create any elliptic curve we like(non-singularity is required), if a curve does not admit any solutions then we can easily change it to another. In this way we have a very high chance to indeed factor an integer. Let's start with an example to get a feeling of how it all works.

Example 3.1
Let $n = 4453$ be an integer which we would like to factorize. We pick the curve $E : y^2 = x^3 + 10x - 2(mod\ 4453)$ and observe that the point $P = (1,3)$ lies on the curve. How do we find a prime divisor of n from that point? The idea is that we know for some $k > 1, kP = \infty$. Thus $(k-1)P$ and P are inverses of each other which implies that when we try to find the slope of the line passing through them, we can not find the multiplicative inverse of some integer. That is this integer is not coprime with n, hence it may admit a factor of n.Therefore we compute kP for $k = 1,2,3,...$

- $2P = (1,3) + (1,3) \Rightarrow y' = \frac{3x^2+10}{2y} = \frac{13}{6} \equiv 3713(mod\ 4453) \Rightarrow 2P = (4332,3230)$.
- $3P = (4332,3230) + (1,3) \Rightarrow$ the slope of the line passing through P and $2P$ is $k = \frac{3230-3}{4332-1} = \frac{3227}{4331}(mod\ 4453)$ but $gcd(4331,4453) = 61 \neq 1$. Thus 4331 has no multiplicative inverse modulo 4453 but we found a factor of n, namely 61. $4453 = 61 \cdot 73$.

The elliptic curve method, ECM, is due to Hendrik Lenstra which is based on Pollard's $p-1$ method, which we will describe first.

Example 3.2
$35 = 5 \cdot 7$ with 5,7 being prime factors of it. Since $5,7 \leq 7$, 35 is called 7-smooth. Generally, let $n = p_1 p_2 \cdots p_k$ be an integer with prime factors $p_1, p_2, \cdots, p_k$. Then for an arbitrary positive integer B, n is called **B-smooth** if $p_1, p_2, \cdots, p_k \leq B$. That is all prime factors are less than or equal to B. Thus any integer is smooth to its largest prime factor.

$125 = 5^3$, is 125-**power smooth**. In general, let $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$, then n is **B-power smooth** if $p_i^{e_i} \leq B \; \forall i \in \{1,2,...,k\}$. Thus any integer is power smooth to the largest prime power dividing it.

Pollard's $p-1$ method uses the following idea:

Let n be an integer which we want to factorize. We use Fermat's little theorem to find one of the factors. Suppose that p is one of the prime factors of n where $p-1$ is B-power smooth, then choose a random positive integer a where we assume that it is coprime to p. Then since every prime power factor of $p-1$ is less than or equal to B, $p-1$ must divide $B!$, therefore we have that

$$a_1 = a^{B!} \equiv (a^{p-1})^{\frac{B!}{p-1}} \equiv 1^{\frac{B!}{p-1}} \equiv 1(mod\ p).$$

This implies that $a_1 - 1 = a^{B!} - 1 = p \cdot m$ for some integer m, or that $p | a_1 - 1$. If it is the case that n does not divide $a_1 - 1$, then $gcd(a_1 - 1, n) < n$ is a nontrivial factor of n. If for any prime divisor q of n we have that $q-1$ is B-power smooth then this method will not produce any prime factor since we will face $gcd(a_1 - 1, n) = n$, in which case we have to change B or a.

Example 3.3
Let's factor 5917 using Pollard's method with $B = 5$ and $a = 2$. We check that $gcd(2, 5917) = 1$. Then

$$2^{5!} - 1(mod\ 5917) \equiv 1647 \Rightarrow gcd(2^{5!} - 1, 5917) = gcd(1647, 6917) = 61$$

$5917 = 61 \cdot 97$.
Notice that $p = 61$ is a prime factor and $p - 1 = 60 = 2^2 \cdot 3 \cdot 5$ is 5-power smooth, that is why 5 did work as a bound in this example.

This method requires several assumptions, such as the random integer a and a prime factor of n to be coprime as well as that n is not B-power smooth.

The following is Lenstra's modification of Pollard's $p-1$ method:
For a composite integer n, pick a bound B to be around 10^8 and pick around 20 elliptic curves $E(mod\ n)$ with points P on them as follows:

- choose $A\ (mod\ n)$ randomly and a point $P=(r,s)$where $C=s^2-r^3-Ar(mod\ n)$. Thus the elliptic curve is $E: y^2=x^3+Ax+C$ and we have already found a point $P=(r,s)$ on it.
- compute $B!\cdot P$. If this step fails, then a nontrivial factor of n has been found. That is because at some point, when points were added together to compute $B!P$, the line through two points has undefined slope modulo n. This occurs when the difference of the x-coordinates of the points is not coprime with n. Then $gcd(x_1-x_2,n)$ equals a factor of n, for x_1, x_2 being the x-coordinates of the two points respectively.
- If in the above step we manage to find $B!P$, then change E or B and repeat the step above.

We end this section with this final example, which uses Lensta's ECM :

Example 3.4
Let $n=1081$, $A=1$ and $P=(0,1)$. Thus $E: y^2=x^3+x+1(mod\ 1081)$. We choose $B=5 \Rightarrow B!=1\cdot 2\cdots 5=120$.

- $2!(0,1)=(811,134)$
- $3!P=3(2!P)=3(811,134)=2(811,134)+(811,134) \Rightarrow 2(811,134)=(59,430)$ so $(811,134)+(59,430)$ has slope

$$k=\frac{134-430}{811-59}=\frac{-296}{752}\equiv\frac{785}{752}(mod\ 1081)$$

  but 752 admits no multiplicative inverse. Hence $gcd(752,1081)\neq 1$. In fact $gcd(752,1081)=47 \Rightarrow 1081=47\cdot 23$.

3.0.2 Primality testing

Just as Lenstra's EC factorization method is a modification of a classical, more elementary factorization method, also elliptic curve primality testing is a modification of a more classical primality testing method, called *Pocklington-Lehmer Primality Test*. We start by describing this latter method:

Pocklington-Lehmer Primality Test

Let n be a positive odd integer of several hundreds digits. Let $n-1 = pq$ with $\sqrt{n} \leq p = p_1 p_2 \cdots p_k$ where $p_1 p_2 \cdots p_k$ are all prime factors of p. Suppose that for each p_i there exists an integer l_i such that the following two conditions are satisfied:

- $l_i^{n-1} \equiv 1 (mod\ n)$ and
- $gcd(l_i^{\frac{n-1}{p_i}} - 1, n) = 1$.

Then n is prime.

Proof

We prove this proposition by contradiction. What contradiction are we aiming to arrive at? Namely that every prime factor c of n will be greater than $p \geq \sqrt{n}$. But this cannot be the case, as n must have a prime factor $c \leq \sqrt{n}$. Thus n must be a prime number.

Suppose n is not a prime number but composite, that is it has a prime factor $c \leq \sqrt{n}$. Let p_i^e be the highest power of p_i dividing p. Then let

- $b \equiv l_i^{\frac{n-1}{p_i^e}} (mod\ c)$. This means that
- $b^{p_i^e} \equiv l_i^{n-1} \equiv 1 (mod\ c)$, but
- $b^{p_i^{e-1}} \equiv l_i^{\frac{n-1}{p_i}} \not\equiv 1 (mod\ c)$.

The last relation holds because

$$gcd(l_i^{\frac{n-1}{p_i}} - 1, n) = 1$$

and we assumed that c is a prime divisor of n. The last two points tell us that the order of b $(mod\ c)$ is p_i^e. This combined with the fact that

$$b^{c-1} \equiv 1 (modc),$$

we can conclude that

$$p_i^e | c-1.$$

As these statements are true for any prime power factor p_i^e of p, it turns out that

$$p = p_1 p_2 \cdots p_k | c-1$$

Now we have showed that for any prime factor c of n we have

$$c > p \geq \sqrt{n}$$

But this contradicts our assumption that $c \leq \sqrt{n}$. Therefore no such c can exist and hence n is prime.□

Example 3.5
Let $n = 100019$ and we wish to determine whether it is a prime or not. We use the Pocklington-Lehmer test. $n - 1 = 100018 = 2 \cdot 50009 = 2 \cdot 43 \cdot 1163$. Let us take $p = 43 \cdot 1163 \geq \sqrt{n}$. The divisors of p are $43, 1163$. Next, we have that

- $2^{100018} \equiv 1 (mod\ 100019)$ and $gcd(2^{\frac{100018}{43}} - 1, 100019) = 1$. Thus $p_1 = 43$ and $l_1 = 2$.
- $2^{100018} \equiv 1 (mod\ 100019)$ and $gcd(2^{\frac{100018}{1163}} - 1, 100019) = 1$, so $p_2 = 1163$ and $l_2 = 2$.

Thus we have satisfied the proposition and $n = 100019$ is a prime. Of course we have to show that $43, 1163$ are also primes. We can use the same method for that purpose as well and recursively proceed until we reach some number where we "know" it is prime.

Notice that this method for primality testing is quite similar to Pollard's method for factorization, as they both use $n - 1$ to prove something about n and also use the Fermat's little theorem. Also, when n is very large, it can be difficult to find a factor $p \geq \sqrt{n}$ of $n - 1$ and its prime divisors $p_1, p_2, \cdots, p_k$. This is one reason to introduce the elliptic curve version of this method. Notice that $n - 1$(assuming n is prime) is the order of the multiplicative group $(\mathbb{Z}_n)^*$, therefore we can change this group order with the order of an elliptic curve group where that order is around $n - 1$. As we can choose any elliptic curve, this order is not difficult to find. This method was introduced by Joe Killian and Shafi Goldwasser[6].

The detailed discussion of the method requires that one considers $E(\mathbb{Z}_n)$, the points of an elliptic curve over the ring $\mathbb{Z}_n$, for an arbitrary integer $n > 1$. When n is a prime number, $\mathbb{Z}_n$ equals the finite field F_n, and $E(F_n)$ has been defined and used above. However when n is composite, the definition and basic theory of $E(\mathbb{Z}_n)$ is more complicated (cf. [4, Ch. 2.11]). We will not discuss this theory in detail, but we mention that when n is composite, $E(\mathbb{Z}_n)$ has points which are "partially at ∞". However $E(\mathbb{Z}_n)$ still has a unique point "fully at ∞"; we call this point ∞; it is the identity element of the group $E(\mathbb{Z}_n)$, just as for $E(F)$ for a field F. A point in $E(\mathbb{Z}_n)$ which is not partially (or fully) at ∞ is called a finite point; the finite points are exactly the points $P = (x, y)$ with $x, y \in \mathbb{Z}_n$ satisfying the equation (2.3) in $\mathbb{Z}_n$.

EC primality testing
Let $n > 1$ and E be an elliptic curve $(mod\ n)$. Suppose there exist distinct prime num-

bers $q_1, q_2, \cdots q_k$ and finite points $P_i \in E(\mathbb{Z}_n)$ such that the following two conditions are satisfied:

- $q_i P_i = \infty$ for $i \in \{1, 2, .., k\}$ and
- $\Pi^k{}_{i=1} q_i = q_1 \cdot q_2 \cdots q_k > (\sqrt[4]{n} + 1)^2$.

Then n **is prime**.

The proof of this theorem is omitted. It can be found in [4, p.196]. □

4 Applications In Cryptography

Everything we have done so far, including factorization of large numbers and primality testing, are in the first place used in cryptography. Before elliptic curves were introduced in cryptography, the RSA algorithm was heavily used. Nowadays even elliptic curves have started to leave footprints in that domain and many cryptographic algorithms and protocols are implemented based on elliptic curves. Compared to RSA, elliptic curves provide the same level of security for much smaller key sizes. That can mean that when implementing cryptographic tools, much smaller chip sizes, less power consumption, etc.. is required. But what is cryptography anyway?

4.0.1 Cryptography

Cryptography is the art, or science of encrypting data so that no one can see/read that data except those who can decrypt it. In order to encrypt data, one needs to have an encryption key. The same is true for decryption, namely that one needs a decryption key. Usually the data being encrypted is called a plaintext message and its encryption is called ciphertext message. Because the size of such keys is very crucial in applications, new methods are being introduced quite often.

There are two types of encryption: symmetric-key encryption and public-key encryption. The first is the case when the encryption key and decryption key are similar. This system is very strong in terms of speed and its small key size, but it is not an easy task for the sender and receiver to share the keys. On the other hand, public-key encryption consists of two keys, one called public-key and the other is the private-key. Everyone can encrypt data using the public-key, since it is available for the public, hence its name, but only those who have the private key can decrypt the data. There is of course a relation between the public- and private-key. The private one can be derived from the public one, therefore measures must be taken to prevent that. Elliptic curve cryptography is a public-key cryptography, therefore we first need to learn about the measures of prevention of private-key derivation from the public-key. This is treated in the next subsection.

4.0.2 The Discrete Logarithm Problem

This problem, called the discrete logarithm, is the engine of all public-key cryptography. It is the reason why everything works so smoothly. For the integers, it is defined as follows:

Let g, b be integers $(mod\ p)$ for some prime p, where g, b are not multiples of p. Assume there exists an integer k such that

$$g^k \equiv b(mod\ p).$$

Solving the DLP amounts to find such a k. It is very easy to compute b from g and k, but difficult to find k by solving

$$dlog_g(b)(mod\ p)$$

when the integers involved are extremely large. $dlog(x)$ is the discrete log. It is different from the continuous $log(x)$.
As an example, let g be a generator of the multiplicative group $\mathbb{Z}_p^*$, for some prime. Then the group is:

$$G = \{g^0, g^1, g^2, g^3, \cdots, g^{p-2}\} = \mathbb{Z}_p^*.$$

Let $g = 5$ and $p = 277$. Then the cyclic group is $\{1, 5, 25, 125, 71, \cdots, 117, \cdots\}$. Of course, for finding what exponent we did raise 5 to in order to get $117(mod\ p)$, we need to by brute-force generate the group and find that element and its position. For a large prime p this becomes infeasible. Notice that hard problem in this sense means that no polynomial time algorithm exists to solve it.

Since we use multiplicative groups, one can ask why not use an elliptic curve group. Indeed, this is fully possible. The ECDLP is a modification of DLP and works as follow: the integers $g, b \in \mathbb{Z}_p$ are exchanged with elements in an elliptic curve group, which are points on the curve. Thus we pick two points $P, Q \in E(\mathbb{Z}_p)$and try to find an integer k such that

$$kP = Q. \tag{4.1}$$

It is trivial that the heart of the problem has not changed. In order to solve this, one needs to find k that satisfies the equation above. Equation (4.1) constitutes the elliptic curve cryptography and applications are primarily based on it. But here is an interesting question we need to answer, namely how do two persons exchange their keys in a safe way?

4.0.3 Diffie-Hellman Key-Exchange

The last question is answered here in this subsection. This algorithm is due to Whitfield Diffie and Martin Hellman, who were first to introduce it, hence its name.

Suppose two persons A and B want to communicate in an unsecured channel. The idea is that these people can not meet to share similar keys in order to use a symmetric-key system. But instead they try to share those keys publicly in a secure way so that no one can reproduce them, and then use those keys to communicate using a symmetric-key system. Here is how it is done:

- They pick an elliptic curve E modulo some large prime p such that the DLP is hard to solve in the group $E(\mathbb{Z}_p)$ and they also pick a point P on E where that point will generate a cyclic subgroup of $E(\mathbb{Z}_p)$ on its own, such that the order of that subgroup is very large, i.e. close to the order of the group itself.
- A picks a private integer r and computes the point $R = rP$. A sends R to B.
- Similarly, B picks a private integer s and computes the point $S = sP$. B sends S to A.
- Now both A and B can compute the point $Q = r(sP) = s(rP)$.

They have now established a shared key, which is the point Q. Anyone except them who wants to obtain that key must solve r from P and R or solve s from P, S. Thus it is indeed crucial that the DLP is hard to solve. Notice that E, P, R, S are public and anyone can see them. r and s on the other hand are kept secret.

Now it is time to describe a cryptosystem that indeed is based on the ECDLP.

4.0.4 Elgamal's Work With Elliptic Curves

Computer scientist Tahir Elgamal was the one who introduced elliptic curves into cryptography and created the first cryptographic system based on elliptic curves. It is called Elgamal Public-Key Encryption. Not only that, but he also introduced Elgamal Digital Signatures. What is a cryptosystem?
A cryptosystem is a five-tuple (P, C, K, E, D, g) where

- P is the space of plaintext,
- C is the space of ciphertext,
- K is the key space,
- E, D are sets of encryption respective decryption rules, and
- g is a rule that must be satisfied, namely that the decryption of the encryption of a plaintext is the plaintext itself.

Here is how Elgamal Public-Key encryption is used when two persons A, B want to communicate:

- A picks a curve $E(mod\ \mathbb{Z}_p)$ and chooses a point P. A computes the point $R = rP$ by picking the private integer r. A sends $(E, \mathbb{Z}_p, P, R)$, which now becomes public, to B, and keeps r private.
- Now assume that B wants to send the message m to A. B expresses the message as a point M on $E(mod\ \mathbb{Z}_p)$. (There are several ways to do that, but they are all technical, therefore we do not describe them).
- B also picks a private integer s and computes the point $S = sP$. Thereafter, B computes the point $M^* = M + sR = M + s(rP)$.(the message is now well encrypted). B sends S, M^* to A. (S, M^*) becomes now public.

To obtain the message M from S, M^*, A computes

- $rS = r(sP)$ and
- $M = M^* - rS = (M + srP) - (rsP)$.

If anyone else wants to see that message, they need to solve the discrete logs of (P, R) to find r, or of (P, S) to find s. It is very important that each time B sends a message to A they use a different private integer s, otherwise the system can become prone to attacks and the message can be obtained by unauthorized people.

Example 4.1
Let $E : y^2 = x^3 + x + 6(mod\ 11)$. A chooses a random private integer $r = 7$. The point $P = (2,7)$ is the public chosen point on E. A also computes $R = 7(2,7) = (7,2)$.
B receives $(E, \mathbb{Z}_{11}, (2,7), (7,2))$. Now let us assume that B wants to send the message m to A. For example $m = "Hello!"$. Let us assume that the hash value of m is $h(m) = 9$.

A hash is a one way function that for an input of any length it produces an fixed-length output such that it is mathematically hard to obtain the input from the output.

B now expresses the message as a point $M = h(m)P = 9(2,7) = (10,9)$. B also picks a private random integer $s = 3$ and computes $S = sP = 3(2,7) = (8,3)$. B sends $M^* = M + s(R) = (10,2)$ and $S = (8,3)$ to A.
To decrypt the message, A computes

- $rS = r(sP) = 7(8,3) = (3,5)$ and
- $M = M^* - r(S) = (10,2) - (3,5) = (10,9)$.

As we stated earlier, Elgamal not only created a cryptosystem, but also a way to create digital signatures that is based on elliptic curves. Classical digital signature schemes were based on the classical discrete logarithm problem, and the algorithm was developed for the multiplicative group of a finite field. What is a digital signature again? In contrast to encrypting data, digital signatures seek to create a signature, of a document for example, digitally. The idea here is not to hide the document itself, the document is published, but the sign on it is of interest in this context. We want a way to tie a sign to its true signer. No one should be able to forge such a sign in the name of someone else, the receiver of the document must be able to prove for others that the sign is indeed authentic and signed by the claimed signer, and most importantly, the true signer should not be able to deny a sign put by them. All these properties are very crucial and must be respected, in order for the signature scheme to be considered safe. A signature scheme consists the following algorithms:

- A key-generation algorithm: the output of this algorithm is the public- private-key pair.
- A signing algorithm: given a document and the private-key, it outputs the signature.
- A verification algorithm: given the document, signature and public-key, this algorithm either accepts or rejects the authenticity of the signature.

Suppose that A wants to sign a document and send it to B. Elliptic curves is used in the following way to make that possible:

- **key-generation**: A picks a curve E, an integer q, which is typically a large prime number, so that the ECDLP is hard in $E(F_p)$, and a point P on E to generate a subgroup of large order. Furthermore, A picks a private random integer r and computes the point $R = rP$. Finally, a function $f : E(F_p) \to \mathbb{Z}$ is chosen. It may be $f(x,y) = x$ where $0 \leq x < p$. The public information is the five-tuple (E, F_p, f, P, R). A keeps r private.
- **signing**: to sign the document, A expresses the document as an integer m less than the order of P, for example by using a hash function, and picks a random integer k to compute the point $Q = kP$ where $gcd(k, |P|) = 1$. This to ensure that k has a multiplicative inverse modulo P. The signature is

$$s \equiv k^{-1}(m - rf(Q))(mod\ |P|) = k^{-1}(m - rx)(mod\ |P|)$$

  where x is the point Q's x-coordinate. s is an integer modulo $|P|$. A sends (m, Q, s) to B.

The message m(actually its hash value) is public and anyone can see it. From the points Q, P it is infeasible to find the private integer k. If k, r are kept secret then the signature s can not be forged.

- **verification**: To verify the signature, B downloads the public information from A and computes

$$Z_1 = f(Q)R + sQ$$

and

$$Z_2 = mP$$

Notice that

$$Z_1 = f(Q)R + sQ = x(rP) + sQ = x(rP) + kP(k^{-1}(m - rf(Q))(mod|P|))$$

$$\Longleftrightarrow$$

$$x(rP) + mP - (rx)P = mP = Z_2$$

therefore if $Z_1 = Z_2$ then the signature is valid.

Example 4.2
Let E, F_p, P, R be as in example 4.1. Let $m = "Hello!"$ be the message with hash value $h(m) = 9$ that A wants to sign. The public information is $(E, \mathbb{Z}_{11}, f, (2,7), 7(2,7) = (7,2))$. This is the public-key generation.
The private integer k is chosen to be 3 and the point Q is $3P = 3(2,7) = (8,3)$. The signature is

$$s = k^{-1}(m - rf(Q))(mod\ |P|) = 3^{-1}(9 - 7 \cdot 8(mod\ 13) = 9(9 - 56) \equiv 6(mod\ 13)$$

Notice that $gcd(k, |P|) = gcd(3, 13) = 1$. A sends $(m = 9, Q = (8,3), s = 6)$.
B does the verification by computing:

$$Z_1 = f(Q)R + sQ = 8(7,2) + 6(8,3) = 8 \cdot 7(2,7) + 6 \cdot 3(2,7) = 4(2,7) + 5(2,7)(mod\ 13) = 9(2,7)$$

and

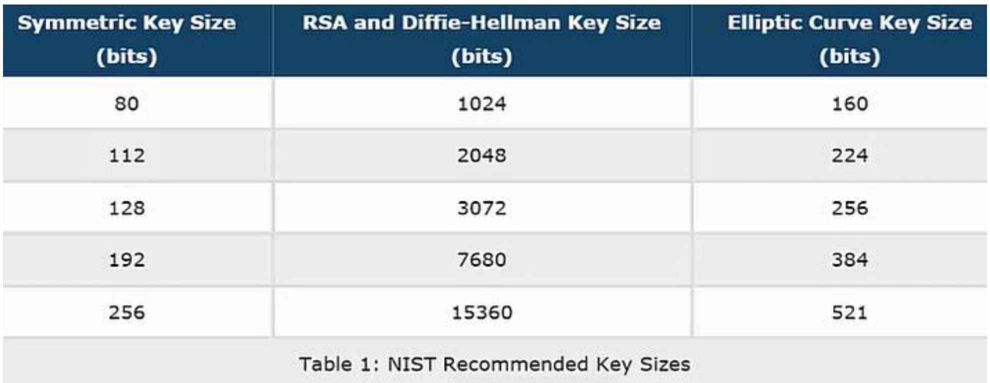
$$Z_2 = mP = 9(2,7).$$

Thus $Z_1 = Z_2$ and the signature is verified and accepted.

As a fact, there is another cryptographic protocol for digital signatures, called the Elliptic Curve Digital Signature Algorithm(ECDSA), based on elliptic curves, which is a modification of the Elgamal digital signatures schemes. But due to the similarities between the two, we choose to not discuss it further.

Another interesting fact is that the digital cryptocurrency Bitcoin uses ECDSA's private-key as a user's account address. Also, the signatures used here are ECDSA signatures which uses the curve , called $secp256k1$, $y^2 = x^3 + 7(mod\ F_{p_{256}})$ where $p_{256} = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$ is a 256-bit prime number[2]. It is approximately equal to $1.15 \cdot 10^{77}$ and is almost as large as the number of atoms in the visible universe[Source: Wolfram alpha].

As a final word, we can cite an article about elliptic curve cryptography[7], where the author states that the fact that elliptic curves uses keys of small sizes is becoming more and more important as we need to implement cryptography on smaller and less powerful devices, such as mobile phones. This is well explained in 4.1. The U.S. government uses elliptic curves to protect internal communications, the Apple iMessage service uses it to provide signatures, Bitcoin uses it for proving ownership. There are of course many other applications of elliptic curves in the everyday life.



Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Table 1: NIST Recommended Key Sizes

Figure 4.1: Key-size comparison[8]

5 Conclusion

At this point, we have reached the end of this thesis. The following is a short conclusion of what we have covered:

- We started by defining what an elliptic curve is, namely that any equation of the form $E : y^2 = x^3 + Ax + B,\ (A.B) \in F$ represents an elliptic curve defined over the field F.
- We showed how the operation of addition of two points on E is defined and described the different cases of addition.
- Also, elliptic curves is shown to form the structure of a group having the point at infinity ∞ as its identity element.
- There are elliptic curves with singular points on them. Such curves have zero discriminant.
- Elliptic curves defined over finite fields F_n have a finite set of points on it. They are the most interesting curves in applications.
- We showed how to use elliptic curves for factorization and primality testing.
- Lastly, we discussed how elliptic curves is gaining importance in the field of cryptography and how they are used for digital signatures.

Literature

[1] T. W. Judson, *Abstract Algebra, Theory and Applications*. 2015.

[2] N. H. Joppe W. Bos J. Alex Halderman, “Elliptic curve cryptography in practice”, 2013.

[3] A. Corbellini. (). ’Elliptic curve cryptography: A gentle introduction’, [Online]. Available: https://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/. (accessed: 01.03.2019).

[4] L. C. Washington, *Elliptic curves: Number Theory and Cryptography, Second Edition*. 2008.

[5] S. Anni, *MA426: Elliptic curves, Lectures by Damiano Testa, Notes by Samuele Anni*. 2014.

[6] S. G. Joe Killian, “Primality testing using elliptic curves”, 1999.

[7] N. Sullivan. (). ’A (relatively easy to understand) primer on elliptic curve cryptography’, [Online]. Available: https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/. (accessed: 13.05.2019).

[8] J. Olenski. (). ’Ecc 101: What is ecc and why would i want to use it?’, [Online]. Available: https://www.globalsign.com/en/blog/elliptic-curve-cryptography/. (accessed: 31.05.2019).