DEMOCRATIC AND POPULAR REPUBLIC OF ALGERIA

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

Mohamed Boudiaf University of Msila

Faculty of Mathematics and Computer Sciences

Department of Mathematics

Master memory

Field : Mathematics and Computer Sciences

Branch : Mathematics

Option : Algebra and Discrete Mathematics

Theme

Elliptic curves over finite fields

Presented by :

Sami Guendouz

In front of the jury composed of :

Ladjelat Lahcene	MAA	University of M'sila	**President**.
Douadi Mihoubi	Prof.	University of M'sila	**Supervisor.**
Haboub Lakhdar	MAA	University of M'sila	**Examiner.**

University year 2019/2020

Acknowledgement

I praise Allah the Almighty and I thank him for helping me to complete this humble work
I also extend my sincere thanks to the supervisor professor, Dr **Mihoubi Douadi** for his wise and rational guidance during the completion of this research paper
Thanks also goes to the professors, members of the jury, who kindly read this paper
I also do miss to thank Mr, **Selikh Bilal** who shared me this experience to complete my work
In the end, I would like to thank everyone who, in a way or another, contributed from near or far to the completion of this research paper.

Thanks

Contents

Introduction générale **1**

1 Essential concepts **2**

1.1 Modular Arithmetic 2

1.1.1 Primes 2

1.1.2 The Greatest Common Divisor 3

1.1.3 Congruences Modulo n 5

1.1.4 Euler's Theorem 7

1.2 finite fields 12

1.2.1 Group theory 12

1.2.2 Rings and fields 14

1.2.3 field Extensions 19

2 Elliptic Curves Arithmetic **21**

2.1 Introduction to elliptic curves 21

2.1.1 Weierstrass equations 21

2.1.2 Simplified Weierstrass equations 23

2.2 The Group law 25

2.2.1 Adding Points on an Elliptic Curve 25

2.2.2 Group law 27

2.2.3 Group order 29

2.2.4 Group structure 30

2.3 Elliptic Curves over Finite Fields 31

2.4 The elliptic curve discrete logarithm problem 34

2.4.1 How hard is the ECDLP? 37

2.4.2 The fastest known algorithm to solve ECDLP in $E(\mathbb{F}_q)$ takes about $\sqrt{q}$ steps . 37

2.5 General Attacks on Discrete Logs 38

2.5.1 The Double-and-Add algorithm 38
2.5.2 Baby Step, Giant Step 39
2.5.3 Pohlig-Hellman attack 41

3 Elliptic curve cryptosystems **44**
3.1 Cryptography 44
3.2 Diffie-Hellman Key Exchange 45
3.3 ElGamal Public Key Encryption 49

Conclusion **53**

Bibliographie **54**

Introduction

The public cryptosystems are based on the notion of one way functions with trapdoors. These are functions that are easy to compute $f(x)$ given the plaintext x, but for which , given the cipher y it is computationally infeasible to solve $y = f(x)$. It is possible to use one-way functions with certain properties to construct a public key cryptosystem. Suppose $f(x)$ has a trapdoor, which means that there is an easy way to solve $y = f(x)$ for x, but only with some extra information known to the designer of function. It should be computationally infeasible for someone other than the designer of the function to determine this trapdoor.

In this memory, the one way function is obtained from exponentiation modulo a prime and the problem is the discrete logarithm problem**(DLP)** used in the group of elliptic curve defined in finite fields given h(x), find an integer k such that $h(x) = (g(x))$ power k in **GF**(p power n) finding such k is believed to be very hard in most situations.

This memory is subdivided in three chapters. The first chapter is devoted to algebraic notions used in this memory. The second chapter is about the elliptic curves and an elliptic curves over a finite fields, finally, the third chapter is focused in the uses of an elliptic curves to build a public cryptosystems.

Chapter 1

Essential concepts

In this chapter we present some of the algebraic concepts that we will need in our memory

1.1 Modular Arithmetic

1.1.1 Primes

Definition 1.1.1. ***(Divides)***. *If $a, b \in \mathbb{Z}$ we say that a divides b, written $a \mid b$, if $ac = b$ for some $c \in \mathbb{Z}$. In this case, we say a is a divisor of b. We say that a does not divide b, written $a \nmid b$, if there is no $c \in \mathbb{Z}$ such that $ac = b$.*

Example 1.1.1. *we have $2 \mid 6$ and $-3 \mid 15$. Also, all integers divide 0, and 0 divides only 0. However, 3 does not divide 7 in $\mathbb{Z}$.*

Theorem 1.1.1. *let a ,b , and c be integres , where $a \neq 0$. Then*

a) If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.

b) If $a \mid b$ and $b \mid c$, then $a \mid c$.

c) If $a \mid b$ and $b \mid a$, then $a = \pm b$.

d) If $a \mid b$ then $a \mid kb$ for all integers k.

e) For any nonzero integer k , $a \mid b$ if and only if $ka \mid kb$.

f) If $a \mid b$ and $a \mid c$, then $a \mid (kb + lc)$ wheneverk and l are integers.

Definition 1.1.2. ***(Prime and Composite)***. *An integer $n > 1$ is prime if the only positive divisors of n are 1 and n. We call n composite if n is not prime.*
The number 1 is neither prime non composite. The first few primes of $\mathbb{N}$ are
$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, ...$
and the first few composites are
$4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28, 30, 32, 33, 34, ...$

Theorem 1.1.2. ***(Fundamental Theorem of Arithmetic)***. *Every natural number can be written as a product of primes uniquely up to order. Note that primes are the products with only one factor and 1 is the empty product.*

Example 1.1.2. $2017 = 2017$ *,*$2020 = 2^2 \cdot 5 \cdot 101$*,* $100 = 2^2 \cdot 5^2$

1.1.2 The Greatest Common Divisor

Definition 1.1.3. ***(Greatest Common Divisor)***. *Let*

$$gcd(a, b) = max\{d \in \mathbb{Z} : d \mid a \; and \; d \mid b\}$$

unless both a and b are 0 in which case $gcd(0, 0) = 0$.

Example 1.1.3. $gcd(1, 2) = 1$*,* $gcd(6, 27) = 3$*, and for any a,* $gcd(0, a) = gcd(a, 0) = a$*.*
If $a \neq 0$, the greatest common divisor exists because if $d \mid a$ then $d \leq |a|$, and there are only $|a|$ positive integers $\leq |a|$. Similarly, the gcd exists when $b \neq 0$.

Lemma 1.1.1. *For any integers a and b, we have*

$$gcd(a, b) = gcd(b, a) = gcd(\pm a, \pm b) = gcd(a, b - a) = gcd(a, b + a)$$

Proof 1.1.1. *We only prove that $gcd(a, b) = gcd(a, b - a)$, since the other cases are proved in a similar way. Suppose $d \mid a$ and $d \mid b$, so there exist integers c_1 and c_2 such that $dc_1 = a$ and $dc_2 = b$. Then $b - a = dc_2 - dc_1 = d(c_2 - c1)$,*
so $d \mid b - a$. Thus $gcd(a, b) \leq gcd(a, b - a)$, since the set over which we are taking the max for $gcd(a, b)$ is a subset of the set for $gcd(a, b - a)$. The same argument with a replaced by $-a$ and b replaced by $b - a$, shows that $gcd(a, b - a) = gcd(-a, b - a) \leq gcd(-a, b) = gcd(a, b)$, which proves that $gcd(a, b) = gcd(a, b - a)$.

Lemma 1.1.2. *Suppose $a, b, n \in \mathbb{Z}$. Then $gcd(a, b) = gcd(a, b - an)$.*

Proposition 1.1.1. *By repeated application of Lemma 1.1.1, we have*

$$gcd(a, b) = gcd(a, b - a) = gcd(a, b - 2a) = ... = gcd(a, b - an)$$

Proposition 1.1.2. *Suppose that a and b are integers with $b \neq 0$. Then there exists unique integers q and r such that $0 \leq r < |b|$ and $a = bq + r$.*

Proof 1.1.2. *For simplicity, assume that both a and b are positive (we leave the general case to the reader). Let Q be the set of all nonnegative integers n such that $a - bn$ is nonnegative. Then Q is nonempty because $0 \in Q$ and Q is bounded because $a - bn < 0$ for all $n > a/b$. Let q be the largest element of Q. Then $r = a - bq < b$, otherwise $q + 1$ would also be in Q. Thus q and r satisfy the existence conclusion. To prove uniqueness, suppose that q' and r' also satisfy the conclusion. Then $q \in Q$ since $r' = a - bq' \geq 0$, so $q' \leq q$, and we can write $q' = q - m$ for some $m \geq 0$. If $q' \neq q$, then $m \geq 1$ so*

$$r' = a - bq' = a - b(q - m) = a - bq + bm = r + bm \geq b$$

since $r \geq 0$, a contradiction. Thus $q = q'$ and $r' = a - bq' = a - bq = r$, as claimed.

Theorem 1.1.3. *The greatest common divisor of two integers x and y not both 0 is the smallest positive integer that is a linear combination of x and y.*

Proof 1.1.3. *Let d be the smallest positive integer that is a linear combination of x and y. Write $d = ax + by$ for integers a and b. We need to see that $d \mid x$ and $d \mid y$.*
Using the division algorithm (Proposition 1.1.2) we write $x = qd + r$ for $0 \leq r < d$. Then we have

$$r = x - qd = x - q(ax + by) = (1 - qa)x - qby.$$

Thus, r is a linear combination of x and y. Since d is the smallest positive linear combination and $0 \leq r < d$, we must have $r = 0$. Since r is the remainder of x after division by d, $r = 0$ implies that $d \mid x$. Similarly, we can show $d \mid y$. Therefore, $d \mid gcd(x, y)$.

Lemma 1.1.3. *For any integers a, b, n, we have*

$$gcd(an, bn) = gcd(a, b) \cdot \mid n \mid$$

Lemma 1.1.4. *Suppose $a, b, n \in \mathbb{Z}$ are such that $n \mid a$ and $n \mid b$. Then $n \mid gcd(a, b)$.*

Proof 1.1.4. *Since $n \mid a$ and $n \mid b$, there are integers c_1 and c_2, such that $a = nc_1$ and $b = nc_2$. By Lemma 1.1.3 $gcd(a, b) = gcd(nc_1, nc_2) = ngcd(c_1; c_2)$, so n divides $gcd(a, b)$.*

Theorem 1.1.4. ***(Euclid)**. Let p be a prime and $a, b \in \mathbb{N}$. If $p \mid ab$ then $p \mid a$ or $p \mid b$.*

Proof 1.1.5. *If $p \mid a$ we are done. If $p \nmid a$ then $gcd(p, a) = 1$, since only 1 and p divide p. By Lemma 1.1.3, $gcd(pb, ab) = b$. Since $p \mid pb$ and, by hypothesis, $p \mid ab$, it follows (using Lemma 1.1.3) that*

$$p \mid gcd(pb, ab) = bgcd(p, a) = b \cdot 1 = b$$

1.1.3 Congruences Modulo n

Definition 1.1.4. *Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$, we say that a is congruent to b modulo n if $n \mid a - b$, and write $a \equiv b \ (mod\ n)$.*

Example 1.1.4.

- *Since $10 \mid (14 - (-6))$, then $14 \equiv -6 \ (mod\ 10)$.*
- *For any $a, b \in \mathbb{Z}$, $a \equiv b \ (mod\ 1)$, since $1 \mid (a - b)$.*

Theorem 1.1.5. *Let $n, m \in \mathbb{N}$, For each $a, b, c, d \in \mathbb{Z}$ Each of the following holds.*

a) $a \equiv a \ (mod\ n)$. *called the reflexive property.*

b) If $a \equiv b \ (mod\ n)$, *then* $b \equiv a \ (mod\ n)$ *called the symmetric property.*

c) If $a \equiv b \ (mod\ n)$ *and* $b \equiv c \ (mod\ n)$, *then* $a \equiv c \ (mod\ n)$, *called the transitive property.*

d) If $a \equiv b \ (mod\ n)$ *and* $c \equiv d \ (mod\ n)$, *then* $a \pm c \equiv b \pm d \ (mod\ n)$.

e) If $a \equiv b \ (mod\ n)$ *and* $c \equiv d \ (mod\ n)$, *then* $ac \equiv bd \ (mod\ n)$.

f) If $a \equiv b \ (mod\ n)$, *then* $ma \equiv mb \ (mod\ n)$.

g) If $a \equiv b \ (mod\ n)$, *then* $a^m \equiv b^m \ (mod\ n)$.

Remark 1.1.1. $(a) - (c)$ *mean that congruence modulo n is equivalence relation over $\mathbb{Z}$ which partitions the integer $\mathbb{Z}$ into disjoint subsets.*

Definition 1.1.5. *For fixed $n \in \mathbb{N}$, and let $a \in \mathbb{Z}$. The congruence class of a with respect to congruence modulo n denoted by $\overline{a}$ or $[a]$ is defined as folows*

$$\overline{a} = \{b \in \mathbb{Z} \mid a \equiv b \ (mod\ n)\}.$$

- *Since $a \equiv r \ (mod\ n)$ such that $a = kn + r$ and $0 \leq r < n-1$,$k \in \mathbb{Z}$ (r is the remaider in the euclidien division of a by n), then $\overline{a} = \overline{r}$.*
- *The set of congruence classes for each $n \in \mathbb{N}$ is denoted by $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$, and it has exactly n elements because of $0 \leq r < n$, then we write*

$$\mathbb{Z}_n = \left\{\overline{0}, \overline{1}, ..., \overline{n-1}\right\}.$$

Example 1.1.5.

$$\begin{aligned} \mathbb{Z}/3\mathbb{Z} &= \{\{..., -3, 0, 3, ...\}, \{..., -2, 1, 4, ...\}, \{..., -1, 2, 5, ...\}\} \\ &= \left\{\overline{0}, \overline{1}, \overline{2}\right\} \end{aligned}$$

Proposition 1.1.3. *If $gcd(c, n) = 1$ and*

$$ac \equiv bc \ (mod\ n)$$

then $a \equiv b \ (mod\ n)$.

Proof 1.1.6. *By definition*

$$n \mid ac - bc = (a - b)c$$

Since $gcd(n, c) = 1$, it follows from Theorem 1.1.4 that $n \mid a - b$, so

$$a \equiv b \ (mod\ n)$$

as claimed.

1.1.4 Euler's Theorem

Definition 1.1.6. ***(Order of an Element)***. *Let $n \in \mathbb{N}$ and $x \in \mathbb{Z}$ and suppose that $gcd(x, n) = 1$. The order of x modulo n is the smallest $m \in \mathbb{N}$ such that*

$$x^m \equiv 1 \ (mod\ n)$$

To show that the definition makes sense, we verify that such an m exists. Consider $x, x^2, x^3, ...$ modulo n. There are only finitely many residue classes modulo n, so we must eventually find two integers i, j with $i < j$ such that

$$x^j \equiv x^i \ (mod\ n)$$

Since $gcd(x, n) = 1$, Proposition 1.1.3 implies that we can cancel $x's$ and conclude that

$$x^{j-i} \equiv 1 \ (mod\ n).$$

Definition 1.1.7. ***(Euler's φ-function)***. *For $n \in \mathbb{N}$, let*

$$\varphi(n) = \#\left\{a \in \mathbb{N} : a \leq n \ \ and \ \ gcd(a, n) = 1\right\}$$

Example 1.1.6.

$$\begin{aligned} \varphi(1) &= \#\{1\} = 1 \\ \varphi(2) &= \#\{1\} = 1 \\ \varphi(5) &= \#\{1, 2, 3, 4\} = 4 \\ \varphi(12) &= \#\{1, 5, 7, 11\} = 4 \end{aligned}$$

Also, if p is any prime number then

$$\varphi(p) = \#\{1, 2, ..., p-1\} = p - 1$$

Theorem 1.1.6. ***(Euler's Theorem)***. *If $gcd(x, n) = 1$, then*

$$x^{\varphi(n)} \equiv 1 \ (mod\ n)$$

Inverses and Fermat's Little Theorem

An important use of division is to solve linear equations of the form

$$ax = b.$$

Unless a is zero, dividing both sides by a allows us to solve for x. Notice that dividing by a is the same as multiplying both sides by the inverse of a,$\frac{1}{a}$. When trying to generalize to modular arithmetic, the key property to keep in mind is that

$$a \cdot \frac{1}{a} = 1.$$

Thus, division by a number is the same as multiplying by its inverse. Even though we do not have fractions in modular arithmetic, we sometimes have inverses.

Definition 1.1.8. *We say that a is the inverse of* b *modulo* m *if*

$$a \cdot b \equiv 1 \ (mod \ m).$$

Example 1.1.7. *Working modulo* 15 *we see that*

$$2 \cdot 8 \equiv 1 \ (mod \ 15).$$

so 2 is the inverse of 8 modulo 15. We could also turn this around and say that 8 is the inverse of 2 modulo 15.

As another example

$$4 \cdot 4 \equiv 1 \ (mod \ 15).$$

so 4 is its own inverse modulo 15.

However, inverses modulo m do not always exist.

Example 1.1.8. *We can check that* 2 *does not have an inverse modulo* 4 *by trying every possible residue class* $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. *Since modular arithmetic depends only on the residue class, we need to consider just one representative from each class. So we can easily check this claim by checking*

whether any of $\{0, 1, 2, 3\}$ *are inverses of* 2*:*

$$\begin{aligned} 2 \cdot 0 &\equiv 0 \,(mod\, 4), \\ 2 \cdot 1 &\equiv 2 \,(mod\, 4), \\ 2 \cdot 2 &\equiv 0 \,(mod\, 4), \\ 2 \cdot 3 &\equiv 2 \,(mod\, 4), \end{aligned}$$

Since none of the multiplications results in 1 and we have tried every possible residue class, 2 does not have an inverse modulo 4.

Theorem 1.1.7. *Given a positive integer* n *and an integer a relatively prime to* n *(i.e,*$gcd(a, n) = 1$*), there is* a *unique residue class* b *modulo* n *such that* $ab \equiv 1 \,(mod\, n)$*.*

Proof 1.1.7. *We know from Theorem 1.1.3 that the greatest common divisor of two integers can be written as a linear combination. Thus, if* $gcd(a, n) = 1$*, there are integers* s *and* t *such that*

$$sa + tn = 1.$$

Since $tn \equiv 0 \,(mod\, n)$*, we have*

$$sa \equiv 1 \,(mod\, n).$$

and s *is the inverse of* a *modulo* n*.*
To prove uniqueness, assume that x *and* y *are both inverses of* a *modulo* n*. Then we have*

$$ax \equiv ay \,(mod\, n).$$

Since $gcd(a, n) = 1$*, we have from Proposition* $1.1.3$

$$x \equiv y \,(mod\, n).$$

Note that the previous theorem states the existence of an inverse but does not give a value. However, from the proof, we see that the extended Euclidean algorithm can be used to find the inverse. We describe the process in Algorithm 2.1.

Algorithm 2.1. Inverses from the Euclidean Algorithm

Input: two positive integers (n, a) that are relatively prime
Output: the inverse of a modulo n
Algorithm:
1: Find x, y from the Euclidean algorithm such that
xa + yn = 1.
2:Return x.

Example 1.1.9. *Consider* $n = 14$ *and* $a = 9$*. We compute*

$$2 \cdot 14 - 3 \cdot 9 = 1$$

so that the inverse of 9 *modulo* 14 *is* -3 *and*

$$-3 \equiv 11 \ (mod \ 14).$$

Theorem 1.1.8. ***(Fermat's Little Theorem)****. If* $a \in \mathbb{Z}$ *and* p *is a prime such that* $gcd(a, p) = 1$*, then*

$$a^{p-1} \equiv 1 \ (mod \ p).$$

Chinese Remainder Theorem

Theorem 1.1.9. *Let* $n_1, ..., n_r$ *be positive integers such that any pair is relatively prime. Then the system of linear congruences*

$$\begin{aligned} x &\equiv a_1 \ (mod \ n_1) \\ &\vdots \\ x &\equiv a_k \ (mod \ n_k) \end{aligned}$$

has a unique solution modulo $N = \prod_{i=1}^{k} n_i$*. The solution is given by*

$$x = a_1 \frac{N}{n_1} y_1 + a_2 \frac{N}{n_2} y_2 + ... + a_k \frac{N}{n_k} y_k$$

where y_i *is the inverse of* $\dfrac{N}{n_i}$ *modulo* n_i*.*

Example 1.1.10. *We are trying to solve*

$$\begin{aligned} x &\equiv 2\ (mod\ 3) \\ x &\equiv 3\ (mod\ 5) \\ x &\equiv 2\ (mod\ 7) \end{aligned}$$

The three moduli are pairwise relatively prime, that is,

$$gcd(3,5) = gcd(3,7) = gcd(5,7) = 1.$$

so the Chinese Remainder Theorem gives a solution modulo $N = 3 \cdot 5 \cdot 7 = 105$*. Using the notation from the theorem, we have*

$$\begin{aligned} a_1 &= 2, \quad n_1 = 3 \\ a_2 &= 3, \quad n_2 = 5 \\ a_3 &= 2, \quad n_3 = 7 \end{aligned}$$

and

$$\begin{aligned} N &= 3 \cdot 5 \cdot 7 = 105, \\ m_1 &= \frac{N}{n_1} = 5 \cdot 7 = 35, \\ m_2 &= \frac{N}{n_2} = 3 \cdot 7 = 21, \\ m_3 &= \frac{N}{n_3} = 3 \cdot 5 = 15, \end{aligned}$$

We need the inverses of the m_i *modulo* n_i*, which we call* y_i*:*

$$\begin{aligned} 2 \cdot 35 &\equiv 1\ (mod\ 3) \ \Rightarrow\ y_1 = 2, \\ 1 \cdot 21 &\equiv 1\ (mod\ 5) \ \Rightarrow\ y_2 = 1, \\ 1 \cdot 15 &\equiv 1\ (mod\ 7) \ \Rightarrow\ y_3 = 1. \end{aligned}$$

So we have

$$\begin{aligned} x &\equiv a_1 m_1 y_1 + a_2 m_2 y_2 + a_3 m_3 y_3, \\ x &\equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \equiv 233 \equiv 23\ (mod\ 105). \end{aligned}$$

1.2 finite fields

1.2.1 Group theory

We begin by recalling the definition of a group.

Definition 1.2.1. *A group is a set G, together with a binary operation $*$, such that the following axioms hold:*

1. ***Closure:*** *G is closed under the operation $*$:*

$$x, y \in G \Longrightarrow x * y \in G;$$

2. ***Associativity:***

$$(x * y) * z = x * (y * z) \; for \; all \; x, y, z \in G;$$

3. ***Identity:*** *there exists an element $e \in G$ (called the identity of G) such that*

$$x * e = e * x = x \; for \; all \; x \in G;$$

4. ***Inverses:*** *for every element $x \in G$ there exists an element $x^{-1} \in G$ (called the inverse of x) such that*

$$x * x^{-1} = x^{-1} * x = e.$$

Remark 1.2.1. *We often write $(\cdot)$ instead of $(*)$ or leave it out completely.*

Definition 1.2.2. ***(Abelian Group)*** *A group G is said to be abelian if the binary operation $*$ is commutative, i.e. if $x * y = y * x$ for all $x, y \in G$. The operation $*$ is often replaced by $+$ for abelian groups, i.e. $x * y$ is written $x + y$ We then say that the group is "written additively" (as opposed to being "written multiplicatively").*

Example 1.2.1.

- *$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are commutative groups. Here $+$ is the addition usual.*
- *Let $n \in \mathbb{N}$, the set $\mathbb{Z}_n$ together with the addition of congruence classes defined as follows*

$$\overline{a} + \overline{b} = \overline{a + b}$$

is an abelian group. The identity element is $\overline{0}$, and the inverse of each element $\overline{a}$ is $-\overline{a} = \overline{-a}$

- *Let G be the set of remainders of all the integers on division by n, e.g. $G = \{0, 1, ..., n-1\}$. Let $a * b$ be the operation of taking the integer sum $a + b$ and reducing it modulo n. Then $(G, *)$ is a group (this is abelian).*

Definition 1.2.3. ***Subgroup*** *A non empty subset H of a group G is called a subgroup of G if H is itself a group with respect to the operation on G:*

Example 1.2.2.

- *$(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ are subgroups of $(\mathbb{R}, +)$.*
- *The set $\{-1, 1\}$ with multiplication is a subgroup of $\mathbb{Z}$.*

Definition 1.2.4. *A group is called finite (respectively, infinite) if it contains finitely (respectively, infinitely) many elements. The number of elements of a finite group G is called its order, written $\mid G \mid$.*

Definition 1.2.5. *Let G be a group, $g \in G$. The order of g is the smallest positive integer n such that $g^n = 1$. If there is no positive integer n such that $g^n = 1$, then g has* ***infinite order****.*

In the case of an abelian group with $+$ as the operation and 0 as the identity, the order of g is the smallest positive integer n such that $ng = 0$.

Example 1.2.3.

- *In $(\mathbb{Z}, +)$, all integers are of infinite order except 0 which is of order 1.*
- *In $(\mathbb{Z}/6\mathbb{Z}, +)$ we have $\overline{2} + \overline{2} + \overline{2} = \overline{0}$ and $\overline{2} + \overline{2} = \overline{4} \neq \overline{0}$ which shows that 2 is of order 3.*
- *In $(\mathbb{Z}/20\mathbb{Z}, +)$ we have $ord(12) = card(< 12 >) = 5$.*

Definition 1.2.6. *If G is a group and $g \in G$, then the subgroup generated by g is*

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}.$$

If the group is abelian and I'm using $+$ as the operation, then

$$\langle g \rangle = \{ng \mid n \in \mathbb{Z}\}.$$

Definition 1.2.7. ***cyclic group*** *A group G is cyclic if $G = \langle g \rangle$ for some $g \in G$. g is a* ***generator*** *of $\langle g \rangle$.*
If a generator g has order n, $G = \langle g \rangle$ is ***cyclic of order*** *n. If a generator g has infinite order, $G = \langle g \rangle$ is* ***infinite cyclic****.*

Example 1.2.4.

- *The group $(Z, +)$ is an infinite cyclic group with generator 1 or -1.*
- *The group $\{1, -1, i, -i\}$ is a cyclic group of order 4 generated by i.*

Theorem 1.2.1. *Let $n \in \mathbb{N}$. The set $\left\{\overline{0}, \overline{1}, ..., \overline{n-1}\right\}$ of equivalence classes modulo n forms a group under the operation $+$ given by $\overline{a} + \overline{b} = \overline{a+b}$. It is called the group of integers modulo n and is denoted $\mathbb{Z}_n$. It is cyclic with $\overline{1}$ as a generator.*

Definition 1.2.8. *The index of H in G (denoted by* ***[G : H]****) is the number of left cosets of H in G, and is equal to the number of right cosets of H in G.*

Theorem 1.2.2. *The order of a finite group G is equal to the product of the order of any subgroup H and the index of H in G. In particular, the order of H divides the order of G and the order of any element $a \in G$ divides the order of G.*

Corollary 1.2.1. *Let $(G, *)$ be a finite group, and let g be any element of G, the order of g divides the cardinal of G. In particular $g^{|G|} = e$ for all $g \in G$.*

1.2.2 Rings and fields

Definition 1.2.9. *A ring $(\mathbb{R}, +, *)$ is a set R, together with two binary operations, denoted by $+$ and $*$, such that*

1. *R is an abelian group with respect to $+$;*
2. *R is closed under $*$;*
3. *$*$ is associative, that is $(a * b) * c = a * (b * c)$ for all $a, b, c \in R$;*
4. *the distributive laws hold, that is, for all $a, b, c \in R$ we have $a * (b + c) = (a * b) + (a * c)$ and $(b + c) * a = (b * a) + (c * a)$.*

Typically, we use 0 to denote the identity element of the abelian group R with respect to addition, and $-a$ to denote the additive inverse of $a \in R$.

Definition 1.2.10.

1. *A ring is called a ring with identity if the ring has a multiplicative identity (usually denoted* e *or* 1*).*
2. *A ring is called commutative if* $*$ *is commutative*
3. *A ring is called an integral domain if it is a commutative ring with identity* $e \neq 0$ *in which* $ab = 0$ *implies* $a = 0$ *or* $b = 0$ *(i.e. no zero divisors).*
4. *A ring is called a division ring (or skew field) if the non-zero elements form a group under* $*$*.*
5. *A commutative division ring is called a field.*

Example 1.2.5.

- *the integers* $(\mathbb{Z}, +, *)$ *form an integral domain but not a field;*
- *the rationals* $(\mathbb{Q}, +, *)$*, reals* $(\mathbb{R}, +, *)$ *and complex numbers* $(\mathbb{C}, +, *)$ *form fields;*
- *the group* $\mathbb{Z}_n$ *with addition as before and multiplication defined by* $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$ *is a commutative ring with identity* $\overline{1}$*.*

So, a field is a set $\mathbb{F}$ on which two binary operations, called addition and multiplication, are defined, and which contains two distinguished elements e and 0 with $e \neq 0$. Moreover, F is an abelian group with respect to addition, having 0 as the identity element, and the non-zero elements of $\mathbb{F}$ (often written $\mathbb{F}^*$) form an abelian group with respect to multiplication having e as the identity element. The two operations are linked by the distributive laws.

Theorem 1.2.3. *Every finite integral domain is a field.*

Proof 1.2.1. *Let* R *be a finite integral domain, and let its elements be* $r_1, r_2, ..., r_n$*. Consider a fixed non-zero element* $r \in R$*. Then the products* $rr_1, rr_2, ..., rr_n$ *must be distinct, since* $rr_i = rr_j$ *implies* $r(r_i - r_j) = 0$*, and since* $r \neq 0$ *we must have* $r_i - r_j = 0$*, i.e.* $r_i = r_j$ *. Thus, these products are precisely the* n *elements of* R*. Each element of* R *is of the form* rr_i*; in particular, the identity* $e = rr_i$ *for some* $1 \leq i \leq n$*. Since* R *is commutative, we also have* $r_i r = e$*, and so* r_i *is the multiplicative inverse of* r*. Thus the non-zero elements of* R *form a commutative group, and* R *is a field.*

Definition 1.2.11.

1. *A subset S of a ring R is called a subring of R if S is closed under $+$ and $*$ and forms a ring under these operations.*

2. *A subset J of a ring R is called an ideal if J is a subring of R and for all $a \in J$ and $r \in R$ we have $ar \in J$ and $ra \in J$.*

3. *Let R be a commutative ring with an identity. Then the smallest ideal containing an element $a \in R$ is $\langle a \rangle = \{ra \mid r \in R\}$. We call $\langle a \rangle$ the principal ideal generated by a.*

Definition 1.2.12. *An integral domain in which every ideal is principal is called a principal ideal domain **(PID)**.*

Example 1.2.6. *$\mathbb{Z}$ is a PID. An ideal J of R defines a partition of R into disjoint cosets (with respect to $+$), residue classes modulo J. These form a ring w.r.t. the following operations:*

$$\begin{aligned} (a+J)+(b+J) &= (a+b)+J; \\ (a+J)(b+J) &= ab+J. \end{aligned}$$

This ring is called the residue class ring and is denoted R/J.

Example 1.2.7. *The residue class ring $\mathbb{Z}/\langle n \rangle$ Here, $\langle n \rangle$ is the principal ideal generated by the integer n (same set $n\mathbb{Z}$ as the subgroup $\langle n \rangle$ but now with two operations). As in the group case, we denote the residue class of a modulo n by $\overline{a}$, as well as by $a + \langle n \rangle$. The elements of $\mathbb{Z}/\langle n \rangle$ are $\overline{0} = 0 + \langle n \rangle$, $\overline{1} = 1 + \langle n \rangle$,..., $\overline{n-1} = n - 1 + \langle n \rangle$.*

Theorem 1.2.4. *$\mathbb{Z}/\langle q \rangle$, the ring of residue classes of the integers modulo the principal ideal generated by a prime q, is a field.*

Proof 1.2.2. *By Theorem $(1.2.3)$, it is enough to show that $\mathbb{Z}/\langle q \rangle$ is an integral domain. Now, $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{0}$ if and only if $ab = kq$ for some $k \in \mathbb{Z}$. Since q is prime, q divides ab if and only if q divides one of the factors. So, either $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$, so $\mathbb{Z}/\langle q \rangle$ contains no zero divisors.*

Example 1.2.8. *Here are the addition and multiplication tables for the field $\mathbb{Z}/\langle 3 \rangle$:*

$+$	$0+\langle 3\rangle$	$1+\langle 3\rangle$	$2+\langle 3\rangle$
$0+\langle 3\rangle$	$0+\langle 3\rangle$	$1+\langle 3\rangle$	$2+\langle 3\rangle$
$1+\langle 3\rangle$	$1+\langle 3\rangle$	$2+\langle 3\rangle$	$0+\langle 3\rangle$
$2+\langle 3\rangle$	$2+\langle 3\rangle$	$0+\langle 3\rangle$	$1+\langle 3\rangle$

$*$	$0+\langle 3\rangle$	$1+\langle 3\rangle$	$2+\langle 3\rangle$
$0+\langle 3\rangle$	$0+\langle 3\rangle$	$0+\langle 3\rangle$	$0+\langle 3\rangle$
$1+\langle 3\rangle$	$0+\langle 3\rangle$	$1+\langle 3\rangle$	$2+\langle 3\rangle$
$2+\langle 3\rangle$	$0+\langle 3\rangle$	$2+\langle 3\rangle$	$1+\langle 3\rangle$

Definition 1.2.13. *A mapping $\phi : R \to S$ (R, S rings) is called a ring homomorphism if for any $a, b \in R$ we have*

$$\phi(a+b) = \phi(a) + \phi(b) \text{ and } \phi(ab) = \phi(a)\phi(b).$$

A ring homomorphism preserves both $+$ and $*$ and induces a homomorphism of the additive group of R into that of S. Concepts such as kernel and image are defined analogously to the groups case. We have a ring version of the First Isomorphism Theorem:

Theorem 1.2.5. *If ϕ is a ring homomorphism from a ring R onto a ring S then the factor ring $R/ker\phi$ and the ring S are isomorphic by the map*

$$r + ker\phi \mapsto \phi(r).$$

We can use mappings to transfer a structure from an algebraic system to a set without structure. Given a ring R, a set S and a bijective map $\phi : R \to S$, we can use ϕ to define a ring structure on S that converts ϕ into an isomorphism. Specifically, for $s_1 = \phi(r_1)$ and $s_2 = \phi(r_2)$, define

$$s_1 + s_2 \text{ to be } \phi(r_1 + r_2), \text{ and } s_1 s_2 \text{ to be } \phi(r_1)\phi(r_2).$$

This is called the ring structure induced by ϕ, any extra properties of R are inherited by S. This idea allows us to obtain a more convenient representation for the finite fields $\mathbb{Z}/\langle q\rangle$.

Definition 1.2.14. *For a prime q, let $\mathbb{Z}_q$ be the set $\{0, 1, ..., q-1\}$ of integers, and let $\phi : \mathbb{Z}/(q) \to \mathbb{F}_q$ be the mapping defined by $\phi(\overline{a}) = a$ for $a = 0, 1, ..., q-1$. Then $\mathbb{F}_q$ endowed with the field structure induced by ϕ is a finite field, called the Galois field of order q.*

From above, the mapping ϕ becomes an isomorphism, so $\phi(\overline{a} + \overline{b}) = \phi(\overline{a}) + \phi(\overline{b})$ and $\phi(\overline{a}\overline{b}) = \phi(\overline{a})\phi(\overline{b})$. The finite field $\mathbb{F}_q$ has zero element 0, identity element 1 and its structure is that of $\mathbb{Z}/\langle q\rangle$. So, computing with elements of $\mathbb{F}_q$ now means ordinary arithmetic of integers with reduction modulo q.

Example 1.2.9.

- $\mathbb{F}_2$*: the elements of this field are* 0 *and* 1*. The operation tables are:*

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

- *We have* $\mathbb{Z}/\langle 5\rangle$*, isomorphic to* $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$*, where the isomorphism is given by* $\overline{0} \to 0, ..., \overline{4} \to 4$ *The operation tables are:*

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$*$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Definition 1.2.15. *If* R *is an arbitrary ring and there exists a positive integer* n *such that* $nr = 0$ *for every* $r \in R$ *(i.e.* r *added to itself* n *times is the zero element) then the least such positive integer* n *is called the characteristic of* R*, and* R *is said to have positive characteristic. If no such positive integer* n *exists,* R *is said to have characteristic* 0*.*

Example 1.2.10.

- $\mathbb{F}_2$ *and* $\mathbb{F}_5$ *have characteristic* 2 *and* 5 *respectively*
- $\mathbb{Q}$ *and* $\mathbb{R}$ *have characteristic* 0*.*

Theorem 1.2.6. *A ring* $R \neq \{0\}$ *of positive characteristic with an identity and no zero divisors must have prime characteristic.*

Proof 1.2.3. *Since* R *contains non-zero elements,* R *has characteristic* $n \geq 2$*. If* n *were not prime, we could write* $n = km$ *with* $k, m \in \mathbb{Z}$*,* $1 < k, m < n$*. Then* $0 = ne = (km)e = (ke)(me)$*, so either* $ke = 0$ *or* $me = 0$*, since* R *has no zero divisors. Hence either* $kr = (ke)r = 0$ *for all* $r \in R$ *or* $mr = (me)r = 0$ *for all* $r \in R$*, contradicting the definition of* n *as the characteristic*

Corollary 1.2.2. *A finite field has prime characteristic.*

Proof 1.2.4. *From Theorem* $(1.2.6)$*, we need only show that a finite field* $\mathbb{F}$ *has a positive characteristic. Consider the multiples* $e, 2e, 3e, ...$ *of the identity. Since* $\mathbb{F}$ *contains only finitely many elements, there must exist integers* k *and* m *with* $1 \leq k < m$ *such that* $ke = me$*, i.e.* $(k - m)e = 0$*, and thus* $(k - m)f = (k - m)ef = 0f = 0$ *for all* $f \in \mathbb{F}$ *so* $\mathbb{F}$ *has a positive characteristic.*

Example 1.2.11. *The field* $\mathbb{Z}/\langle q\rangle$ *(equivalently,* $\mathbb{F}_q$*) has characteristic* q*.*

1.2.3 field Extensions

Definition 1.2.16. *Let F and K be fields, we say that K is an extension of F if $F \subseteq K$, and we write $K \mid F$.*

- *The extension K is a vector space over F, The dimension of this vector space is called the degree of the extension, noted $[K : F]$.*
- *If $[K : F]$ is finite then we say that K is a finite extension.*

Example 1.2.12. *$\mathbb{C} \mid \mathbb{R}$ is a finite extension and $\mathbb{C} \mid \mathbb{Q}$ is infinite extension.*

Definition 1.2.17. *An element α lying in some extension field of a field F is called a **root** of $g \in F[X]$ if $g(\alpha) = 0$.*

Definition 1.2.18. *Let K be an extension of a field F, An element α of K is called algebraic over F if there is a nonzero polynomial g with coefficients in F such that $g(\alpha) = 0$.*

Definition 1.2.19. *An extension K of a field F is called **algebraic** if each element of K is algebraic over F.*

Definition 1.2.20. *Let $f \in F[X]$ and K an extension field of F, Then f is said to **split** in K if f can be expressed as a product of linear factors in $K[X]$, Then is if there exist elements $\alpha_1, \alpha_2, ..., \alpha_n \in K$ such that*

$$f(X) = a(X - \alpha_1)(X - \alpha_2)...(X - \alpha_n).$$

where a is the leading coefficient of f. The field K is called a splitting field of f over F if f splits in K, but does not split in any proper subfield of K containing F.

Example 1.2.13. *$\mathbb{C}$ is the splitting field of $x^2 + 1 \in \mathbb{R}$.*

Definition 1.2.21. *Let K be an extension field of F, The field K is called **algebraically closed** if any nonconstant polynomial in $K[X]$ splits into linear factors in $K[X]$.*

Definition 1.2.22. *A field $\overline{F}$ is called an **algebraic closure** of a field F, if F is algebraically closed and is an algebraic extension of F.*

Proposition 1.2.1. *The characteristic of a finite field is a prime number.*

Theorem 1.2.7. *Let $\mathbb{F}_q$ be a finite field of characteristic p. Then $\mathbb{F}_q$ contains p^n elements, where $n = [\mathbb{F}_q : \mathbb{F}_p]$.*

Theorem 1.2.8. *For any prime p and any positive integer n there exists a finite field with $q = p^n$ elements. This field is unique up to isomorphism.*

Remark 1.2.2. *Finite field of order 2^n are called binary field or characteristic two finite field.*

Theorem 1.2.9. *Let $\mathbb{F}_q$ be a finite field with q element.*

- *The multiplicative group $\left(\mathbb{F}_q^*, \cdot\right)$ of the nonzero elements of $\mathbb{F}_q$ is cyclic of order $q-1$.*
- *All elements a of $\mathbb{F}_q$ satisfy $a^q - a = 0$.*

Definition 1.2.23. *A generator of the cyclic group of a finite field $\mathbb{F}_q$ is called a **primitive elements**.*

Theorem 1.2.10. *let a be a primitive element for the finite field $\mathbb{F}_q$. Then*

$$\mathbb{F}_q = \left\{0, 1, a, a^2, ..., a^{q-2}\right\}.$$

where $a^{q-1} = 1$. Moreover, a^q is also primitive if and only if $gcd\,(K, q-1) = 1$.

Chapter 2

Elliptic Curves Arithmetic

In this chapter, we introduce the basic concepts of elliptic curves and some of their properties on finite fields and conclude with the definition of a discrete logarithm problem.

2.1 Introduction to elliptic curves

2.1.1 Weierstrass equations

Definition 2.1.1. *An elliptic curve E over a field K is defined by an equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1}$$

where $a_1, a_2, a_3, a_4, a_6 \in K$ and $\Delta \neq 0$, where Δ is the discriminant of E and is defined as follows:

$$\begin{cases} \Delta = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6 \\ d_2 = a_1^2 + 4a_2 \\ d_4 = 2a_4 + a_1a_3 \\ d_6 = a_3^2 + 4a_6 \\ d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{cases} \tag{2.2}$$

If L is any extension field of K, then the set of L-rational points on E is

$$E(L) = \{(x, y) \in L * L : \ y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{\infty\}$$

where ∞ is the point at infinity.

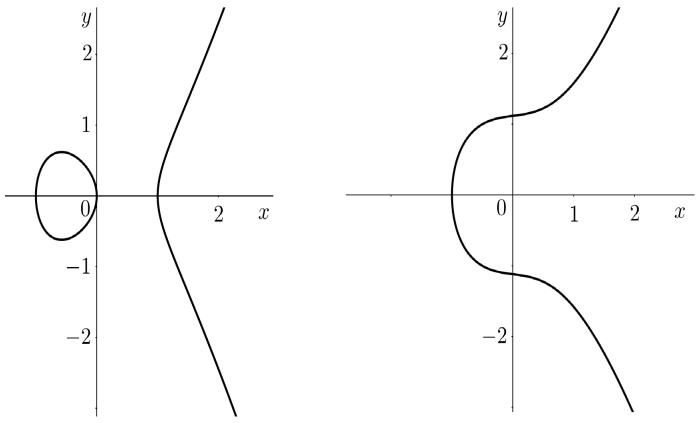
Remark 2.1.1.

1. *Equation* (2.1) *is called a* ***Weierstrass equation****.*
2. *We say that* E*is defined over* K *because the coefficients* a_1, a_2, a_3, a_4, a_6 *of its defining equation are elements of* K*. We sometimes write* E/K *to emphasize that* E *is defined over* K*, and* K *is called the underlying field. Note that if* E *is defined over* K*, then* E *is also defined over any extension field of* K*.*
3. *The condition* $\Delta \neq 0$ *ensures that the elliptic curve is "****smooth****", that is, there are no points at which the curve has two or more distinct tangent lines.*
4. *The point* ∞ *is the only point on the line at infinity that satisfies the projective form of the Weierstrass equation (see figure* 2.1*).*
5. *The* L*-rational points on* E *are the points* (x, y) *that satisfy the equation of the curve and whose coordinates* x *and* y *belong to* L*. The point at infinity is considered an* L*-rational point for all extension fields* L *of* K*.*

Example 2.1.1. ***(elliptic curves over*** $\mathbb{R}$***)*** *Consider the elliptic curves*

$$E_1 : y^2 = x^3 - x$$
$$E_2 : y^2 = x^3 + \tfrac{1}{4}x + \tfrac{5}{4}$$

defined over the field $\mathbb{R}$ *of real numbers. The points* $E_1(\mathbb{R}) \setminus \infty$ *are* $E_2(\mathbb{R}) \setminus \infty$ *graphed in Figure* 2.1*.*



a) $E_1 : y^2 = x^3 - x$ *b)* $E_2 : y^2 = x^3 + \frac{1}{4}x + \frac{5}{4}$

Figure 2.1: Elliptic curves over $\mathbb{R}$.

2.1.2 Simplified Weierstrass equations

Definition 2.1.2. *Two elliptic curves E_1 and E_2 defined over K and given by the Weierstrass equations*

$$E_2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

$$E_2 : y^2 + \overline{a_1}xy + \overline{a_3}y = x^3 + \overline{a_2}x^2 + \overline{a_4}x + \overline{a_6}$$

are said to be isomorphic over K if there exist $u, r, s, t \in K, u \neq 0$, such that the change of variables

$$(x, y) \to (u^2x + r, u^3y + u^2sx + t). \tag{2.3}$$

transforms equation E_1 into equation E_2. The transformation (2.3) is called an admissible change of variables.
A Weierstrass equation

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

defined over K can be simplified considerably by applying admissible changes of variables. The simplified equations will be used throughout the remainder of this memory. We consider separately the cases where the underlying field K has characteristic different from 2 and 3, or has characteristic equal to 2 or 3.

1. *If the characteristic of K is not equal to 2 or 3, then the admissible change of variables*

$$(x, y) \to \left(\frac{x - 3a_1^2 - 12a_2}{36}, \frac{y - 3a_1x}{216} - \frac{a_1^3 + 4a_1a_2 - 12a_3}{24}\right).$$

   transforms E to the curve

$$y^2 = x^3 + ax + b.$$

   where $a, b \in K$. The discriminant of this curve is $\Delta = -16(4a^3 + 27b^2)$.

2. *If the characteristic of K is 2, then there are two cases to consider. If $a_1 \neq 0$, then the admissible change of variables*

$$(x, y) \to \left(a_1^2x + \frac{a_3}{a_1}, a_1^3y + \frac{a_1^2a_4 + a_3^2}{a_1^3}\right).$$

transforms E to the curve

$$y^2 + xy = x^3 + ax^2 + b.$$

where $a, b \in K$. Such a curve is said to be non-supersingular and has discriminant $\Delta = b$. If $a_1 = 0$, then the admissible change of variables

$$(x, y) \to (x + a_2, y).$$

transforms E to the curve

$$y^2 + cy = x^3 + ax + b.$$

where $a, b, c \in K$. Such a curve is said to be supersingular and has discriminant $\Delta = c^4$.

3. *If the characteristic of K is 3, then there are two cases to consider. If $a_1^2 \neq -a_2$, then the admissible change of variables*

$$(x, y) \to \left(x + \frac{d_4}{d_2}, y + a_1 x + a_1 \frac{d_4}{d_2} + a_3\right).$$

where $d_2 = a_1^2 + a_2$ and $d_4 = a_4 - a_1 a_3$, transforms E to the curve

$$y^2 = x^3 + ax^2 + b.$$

where $a, b \in K$. Such a curve is said to be non-supersingular and has discriminant $\Delta = -a^3 b$. If $a_1^2 = -a_2$, then the admissible change of variables

$$(x, y) \to (x, y + a_1 x + a_3).$$

transforms E to the curve

$$y^2 = x^3 + ax + b.$$

where $a, b \in K$. Such a curve is said to be supersingular and has discriminant $\Delta = -a^3$.

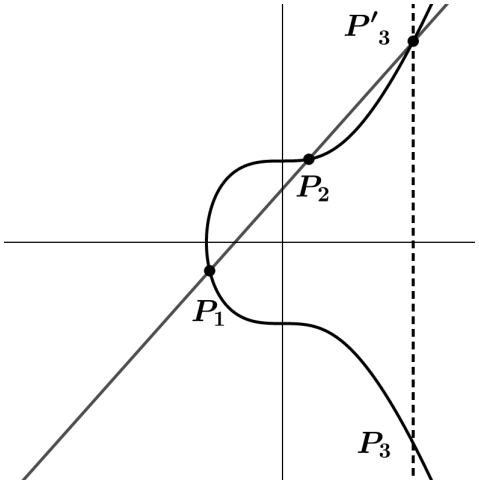


Figure 2.2:

2.2 The Group law

2.2.1 Adding Points on an Elliptic Curve

Start with two points

$$P_1 = (x_1, y_1), \quad P_2 = (x_2, y_2)$$

on an elliptic curve E given by the equation $y^2 = x^3 + Ax + B$ .Define a new point P_3 as follows. Draw the line L through P_1 and P_2. We'll see below that L intersects E in a third point P_3' . Reflect P_3' across the x-axis (i.e., change the sign of the y-coordinate) to obtain P_3. We define

$$P_1 + P_2 = P_3$$

Examples below will show that this is not the same as adding coordinates of the points. It might be better to denote this operation by $P_1 + P_2$, but we opt for the simpler notation since we will never be adding points by adding coordinates.

Assume first that $P_1 \neq P_2$ and that neither point is ∞. Draw the line L through P_1 and P_2 . Its slope is

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

If $x_1 = x_2$, then L is vertical. We'll treat this case later, so let's assume that $x_1 \neq x_2$. The equation of L is then

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

To find the intersection with E, substitute to get

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

This can be rearranged to the form

$$0 = x^3 - m^2x^2 + ...$$

The three roots of this cubic correspond to the three points of intersection of L with E. Generally, solving a cubic is not easy, but in the present case we already know two of the roots, namely x_1 and x_2 , since P_1 and P_2 are points on both L and E. Therefore, we could factor the cubic to obtain the third value of x. But there is an easier way, if we have a cubic polynomial $x^3 + ax^2 + bx + c$ with roots r, s, t, then

$$x^3 + ax^2 + bx + c = (x - r)(x - s)(x - t) = x^3 - (r + s + t)\, x^2 + ...$$

Therefore,

$$r + s + t = -a$$

If we know two roots r,s , then we can recover the third as $t = -a - r - s$. In our case, we obtain

$$x = m^2 - x_1 - x_2$$

and

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

Now, reflect across the x-axis to obtain the point $P_3 = (x_3, y_3)$

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

In the case $x_1 = x_2$ that but $y_1 \neq y_2$, the line through P_1 and P_2 is a vertical line, which therefore intersects E in ∞. Reflecting ∞ across the x-axis yields the same point ∞ (this is why we put ∞ at both the top and the bottom of the y-axis). Therefore, in this case $P_1 + P_2 = \infty$. Now consider the case where $P_1 = P_2 = (x_1, y_1)$. When two points on a curve are very close to each other, the line through them approximates a tangent line. Therefore, when the two points coincide, we take the line L through them to be the tangent line. Implicit differentiation allows us to find the slope m

of L:

$$2y\frac{dy}{dx} = 3x^2 + A, so \quad m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}.$$

If $y = 0$ then the line is vertical and we set $P_1 + P_2 = \infty$ as before. (Technical point:if $y_1 = 0$, then the numerator $3x_1^2 + A \neq 0$) Therefore, assume that $y_1 \neq 0$. The equation of L is

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

as before. We obtain the cubic equation

$$0 = x^3 - m^2x^2 + ...$$

This time, we know only one root, namely X_1, but it is a double root since L is tangent to E at P_1. Therefore, proceeding as before, we obtain

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1.$$

Finally, suppose $P_2 = \infty$. The line through P_1 and ∞ is a vertical line that intersects E in the point P_1' that is the reflection of P_1 across the x-axis. When we reflect P_1' across the x-axis to get $P_3 = P_1 + P_2$, we are back at P_1. Therefore $P_1 + \infty = P_1$ for all points P_1 on E. Of course, we extend this to include $\infty + \infty = \infty$. Let's summarize the above discussion:

2.2.2 Group law

Let E be an elliptic curve defined by $y^2 = x^3 + Ax + B$ Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E with $P_1, P_2 \neq \infty$. Define $P_1 + P_2 = P_3 = (x_3, y_3)$ as follows:

1. If $x_1 \neq x_2$, then

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

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

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

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

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

Moreover, define

$$P + \infty = P.$$

for all points P on E.

Theorem 2.2.1. *The addition of points on an elliptic curve E satisfies the following properties:*

1. *(commutativity) $P_1 + P_2 = P_2 + P_1$ for all P_1, P_2 on E.*
2. *(existence of identity) $P + \infty = P$ for all points P on E.*
3. *(existence of inverses) Given P on E,there exists P' on E with $P + P' = \infty$ .This point P' will usually be denoted $-P$.*
4. *(associativity) $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ for all P_1, P_2, P_3 on E.*

In other words, the points on E form an additive abelian group with ∞ as the identity element.

Proof 2.2.1. *The commutativity is obvious, either from the formulas or from the fact that the line through P_1 and P_2 is the same as the line through P_2 and P_1. The identity property of ∞ holds by definition. For inverses, let P' be the reflection of P across the x-axis. Then $P + P' = \infty$.*
Finally, we need to prove associativity. This is by far the most subtle and nonobvious property of the addition of points on E. It is possible to define many laws of composition satisfying (1), (2),(3) for points on E, either simpler or more complicated than the one being considered. But it is very unlikely that such a law will be associative. In fact, it is rather surprising that the law of composition that we have defined is associative. After all, we start with two points P_1 and P_2 and perform a certain procedure to obtain a third point $P_1 + P_2$. Then we repeat the procedure with $P_1 + P_2$ and P_3 to obtain $(P_1 + P_2) + P_3$. If we instead start by adding$P_2 + P_3$, then computing $P_1 + (P_2 + P_3)$, there seems to be no obvious reason that this should give the same point as the other computation. The associative law can be verified by calculation with the formulas. There are several cases, depending on whether or not $P_1 = P_2$, and whether or not $P_3 = (P_1 + P_2)$, etc.

Definition 2.2.1. *Let n be a positive integer and let P be a point on $E(K)$, The point*

$$nP = \underbrace{P + P + ... + P}_{n\ times}.$$

is called point multiplication or scalar multiplication.
The order of P is the smallest positive integer n such that $nP = \infty$

Example 2.2.1. *Consider the elliptic curve*

$$E : y^2 = x^3 + x + 2.$$

and the point $P = (1, 2)$*. Computing the addition of points, we find*

$$P = (1, 2),\ 2P = (-1, 0),\ 3P = (1, -2),\ 4P = \infty,\ 5P = (1, 2) = P$$

so that the set of points

$$\{nP : n \in \mathbb{Z}\}.$$

is a finite set of points. It turns out that these four points are the only four rational points on E*.*

Example 2.2.2. *Let* $p = 29$*,* $A = 4$*, and* $B = 20$*, and consider the elliptic curve*

$$E : y^2 = x^3 + 4x + 20$$

defined over $\mathbb{F}_{29}$ *. Note that* $\Delta = -16(4A^3 + 27B^2) = -176896 \not\equiv 0\ (mod\ 29)$ *, so* E *is indeed an elliptic curve. The points in* $E(\mathbb{F}_{29})$ *are the following:*

∞	(2,6)	(4,19)	(8,10)	(13,23)	(16,2)	(19,16)	(27,2)
(0,7)	(2,23)	(5,7)	(8,19)	(14,6)	(16,27)	(20,3)	(27,27)
(0,22)	(3,1)	(5,22)	(10,4)	(14,23)	(17,10)	(20,26)	
(1,5)	(3,28)	(6,12)	(10,25)	(15,2)	(17,19)	(24,7)	
(1,24)	(4,10)	(6,17)	(13,6)	(15,27)	(19,13)	(24,22)	

Table 2.1: The points in $E(\mathbb{F}_{29})$

Examples of elliptic curve addition are $(5, 22) + (16, 27) = (13, 6)$, and $2(5, 22) = (14, 6)$.

2.2.3 Group order

Let E be an elliptic curve defined over $\mathbb{F}_q$. The number of points in $E(\mathbb{F}_q)$, denoted $\#E(\mathbb{F}_q)$, is called the order of E over $\mathbb{F}_q$. Since the Weierstrass equation (2.1) has at most two solutions for each $x \in \mathbb{F}_q$, we know that $\#E(\mathbb{F}_q) \in [1, 2q + 1]$. Hasse's theorem provides tighter bounds for $\#E(\mathbb{F}_q)$.

Theorem 2.2.2. *(Hasse) Let* E *be an elliptic curve defined over* $\mathbb{F}_q$*. Then*

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

The interval $\left[q+1-2\sqrt{q}, q+1+2\sqrt{q}\right]$ *. is called the Hasse interval. An alternate formulation of Hasse's theorem is the following: if* E *is defined over* $\mathbb{F}_q$*, then* $\#E(\mathbb{F}_q) = q+1-t$ *where* $|t| \leq 2\sqrt{q}$ *is called the trace of* E *over* $\mathbb{F}_q$*. Since* $2\sqrt{q}$ *is small relative to* q*, we have* $\#E(\mathbb{F}_q) \approx q$*. The next result determines the possible values for* $\#E(\mathbb{F}_q)$ *as* E *ranges over all elliptic curves defined over* $\mathbb{F}_q$

Theorem 2.2.3. *(admissible orders of elliptic curves)*
Let $q = p^m$ *where* p *is the characteristic of* $\mathbb{F}_q$ *. There exists an elliptic curve* E *defined over* $\mathbb{F}_q$ *with* $\#E(\mathbb{F}_q) = q+1-t$ *if and only if one of the following conditions holds:*

1. $t \not\equiv 0 \ (mod\ p)$ *and* $t^2 \leq 4q$*.*
2. m *is odd and either* $t = 0$ *, or* $t^2 = 2q$ *and* $p = 2$ *, or* $t^2 = 3q$ *and* $p = 3$*.*
3. m *is even and either* $t^2 = 4q$*, or* $t^2 = q$ *and* $p \not\equiv 1 \ (mod\ 3)$*, or* $t = 0$ *and* $p \not\equiv 1 \ (mod\ 4)$*.*

A consequence of Theorem 2.2.2 is that for any prime p and integer t satisfying $|t| \leq 2\sqrt{p}$, there exists an elliptic curve E over $\mathbb{F}_P$ with $\#E(\mathbb{F}_p) = p+1-t$.

Example 2.2.3. *(orders of elliptic curves over* $\#E(\mathbb{F}_{37})$*, Let* $p = 37$*. Table 2.2 lists, for each integer* n *in the Hasse interval* $\left[37+1-2\sqrt{37}, 37+1+2\sqrt{37}\right]$*, the coefficients* (A, B) *of an elliptic curve* $E : y^2 = x^3 + Ax + B$ *defined over* $\#E(\mathbb{F}_{37})$ *with* $\#E(\mathbb{F}_{37}) = n$*.*

n	(A,B)	n	(A,B)	n	(A,B)	n	(A,B)	n	(A,B)
26	$(5,0)$	31	$(2,8)$	36	$(1,0)$	41	$(1,16)$	46	$(1,11)$
27	$(0,9)$	32	$(3,6)$	37	$(0,5)$	42	$(1,9)$	47	$(3,15)$
28	$(0,6)$	33	$(1,13)$	38	$(1,5)$	43	$(2,9)$	48	$(0,1)$
29	$(1,12)$	34	$(1,18)$	39	$(0,3)$	44	$(1,7)$	49	$(0,2)$
30	$(2,2)$	35	$(1,8)$	40	$(1,2)$	45	$(2,14)$	50	$(2,0)$

Table 2.2: The admissible orders $n = \#E(\mathbb{F}_{37})$ of elliptic curves $E : y^2 = x^3 + Ax + B$ defined over $\mathbb{F}_{37}$

2.2.4 Group structure

Theorem 2.2.4 describes the group structure of $E(\mathbb{F}_q)$. We use $\mathbb{Z}_n$ to denote a cyclic group of order n.

Theorem 2.2.4. *(group structure of an elliptic curve) Let* E *be an elliptic curve defined over* $\mathbb{F}_q$*. Then* $E(\mathbb{F}_q)$ *is isomorphic to* $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ *where* n_1 *and* n_2 *are uniquely determined positive integers such that* n_2 *divides both* n_1 *and* $q-1$*.*

Note that $\#E(\mathbb{F}_q) = n_1 n_2$. If $n_2 = 1$, then $E(\mathbb{F}_q)$ is a cyclic group. If $n_2 > 1$, then $E(\mathbb{F}_q)$ is said to have rank 2. If n_2 is a small integer (e.g., $n = 2, 3$ or 4), we sometimes say that $E(\mathbb{F}_q)$ is almost cyclic. Since n_2 divides both n_1 and $q - 1$, one expects that $E(\mathbb{F}_q)$ is cyclic or almost cyclic for most elliptic curves E over $\mathbb{F}_q$.

Example 2.2.4. ***(group structure)*** *The elliptic curve $E : y^2 = x^3 + 4x + 20$ defined over $\mathbb{F}_{29}$ has $\#E(\mathbb{F}_{29}) = 37$. Since 37 is prime, $E(\mathbb{F}_{29})$ is a cyclic group and any point in $E(\mathbb{F}_{29})$ except for ∞ is a generator of $E(\mathbb{F}_{29})$. The following shows that the multiples of the point $P = (1, 5)$ generate all the points in $E(\mathbb{F}_{29})$.*

$0P = \infty$	$8P = (8, 10)$	$16P = (0, 22)$	$24P = (16, 2)$	$32P = (6, 17)$
$1P = (1, 5)$	$9P = (14, 23)$	$17P = (27, 2)$	$25P = (19, 16)$	$33P = (15, 2)$
$2P = (4, 19)$	$10P = (13, 23)$	$18P = (2, 23)$	$26P = (10, 4)$	$34P = (20, 26)$
$3P = (20, 3)$	$11P = (10, 25)$	$19P = (2, 6)$	$27P = (13, 6)$	$35P = (4, 10)$
$4P = (15, 27)$	$12P = (19, 13)$	$20P = (27, 27)$	$28P = (14, 6)$	$36P = (1, 24)$
$5P = (6, 12)$	$13P = (16, 27)$	$21P = (0, 7)$	$29P = (8, 19)$	
$6P = (17, 19)$	$14P = (5, 22)$	$22P = (3, 28)$	$30P = (24, 7)$	
$7P = (24, 22)$	$15P = (3, 1)$	$23P = (5, 7)$	$31P = (17, 10)$	

Table 2.3:

2.3 Elliptic Curves over Finite Fields

Previously section we developed the theory of elliptic curves geometrically. For example, the sum of two distinct points P and Q on an elliptic curve E is defined by drawing the line L connecting P to Q and then finding the third point where L and E intersect, in order to apply the theory of elliptic curves to cryptography, we need to look at elliptic curves whose points have coordinates in a finite field $\mathbb{F}_q$. This is easy to do. We simply define an elliptic curve over $\mathbb{F}_q$ to be an equation of the form

$$E : y^2 = x^3 + Ax + B \; with \; A, B \in \mathbb{F}_q \; satisfying \;\; 4A^3 + 27B^2 \neq 0$$

and then we look at the points on E with coordinates in $\mathbb{F}_q$, which we denote by

$$E(\mathbb{F}_q) = \left\{(x, y) : x, y \in \mathbb{F}_q \; satisfy \;\; y^2 = x^3 + Ax + B\right\} \cup \{\infty\}\,.$$

Examples

Example 2.3.1. *Let E be the curve $y^2 = x^3 + x + 1$ over $\mathbb{F}_5$. To count points on E, we make a list of the possible values of x, then of $x^3 + x + 1 \pmod 5$, then of the square roots y of $x^3 + x + 1 \pmod 5$.*

This yields the points on E.

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

Table 2.4:

Therefore, $E(\mathbb{F}_5)$ has order 9.

Let's compute $(3,1)+(2,4)$ on E. The slope of the line through the two points is

$$\frac{4-1}{2-3} \equiv 2 \ (mod\ 5).$$

The line is therefore $y = 2(x-3)+1 \equiv 2x$. Substituting this into $y^2 = x^3+x+1$ and rearranging yields

$$0 = x^3 - 4x^2 + x + 1.$$

The sum of the roots is 4, and we know the roots 3 and 2. Therefore the remaining root is $x = 4$. Since $y = 2x$, we have $y \equiv 3$. Reflecting across the x-axis yields the sum:

$$(3,1)+(2,4) = (4,2).$$

Example 2.3.2. *Consider the elliptic curve*

$$y^2 = x^3 + 3x + 8 \ over\ \mathbb{F}_{13}$$

We can find the points of $E(\mathbb{F}_{13})$ by substituting in all possible values $x = 0,1,2,...,12$ and checking for which x values the quantity x^3+3x+8 is a square modulo 13. For example, putting $x = 0$ gives 8, and 8 is not a square modulo 13. Next we try $x = 1$, which gives $1+3+8 = 12$. It turns out that 12 is a square modulo 13, in fact, it has two square roots,

$$5^2 \equiv 12 \ (mod\ 13) \ \ and \ \ 8^2 \equiv 12 \ (mod\ 13).$$

This gives two points $(1,5)$ and $(1,8)$ in $E(\mathbb{F}_{13})$. Continuing in this fashion, we end up with a

complete list,

$$E(\mathbb{F}_{13}) = \{\infty, (1,5), (1,8), (2,3), (2,10), (9,6), (9,7), (12,2), (12,11)\}.$$

Thus $E(\mathbb{F}_{13})$ consists of nine points.

Suppose now that P and Q are two points in $E(\mathbb{F}_q)$ and that we want to "add" the points P and Q. One possibility is to develop a theory of geometry using the field $\mathbb{F}_q$ instead of R. Then we could mimic our earlier constructions to define $P + Q$. This can be done, and it leads to a fascinating field of mathematics called algebraic geometry. However, in the interests of brevity of exposition, we instead use the explicit formulas given in Theorem 2.2.1 to add points in $E(\mathbb{F}_q)$. But we note that if one wants to gain a deeper understanding of the theory of elliptic curves, then it is necessary to use some of the machinery and some of the formalism of algebraic geometry. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be points in $E(\mathbb{F}_q)$. We define the sum $P_1 + P_2$ to be the point (x_3, y_3) obtained by applying the elliptic curve addition algorithm $(Theorem 2.2.1)$. Notice that in this algorithm, the only operations used are addition, subtraction, multiplication, and division involving the coefficients of E and the coordinates of P and Q. Since those coefficients and coordinates are in the field $\mathbb{F}_q$, we end up with a point (x_3, y_3) whose coordinates are in $\mathbb{F}_q$. Of course, it is not completely clear that (x_3, y_3) is a point in$E(\mathbb{F}_q)$.

Theorem 2.3.1. *Let E be an elliptic curve over $\mathbb{F}_q$ and let P and Q be points in $E(\mathbb{F}_q)$.*

1. *The elliptic curve addition algorithm (Theorem 2.2.1) applied to P and Q yields a point in $E(\mathbb{F}_q)$. We denote this point by $P + Q$.*
2. *This addition law on $E(\mathbb{F}_q)$ satisfies all of the properties listed in Theorem 2.2.1. In other words, this addition law makes $E(\mathbb{F}_q)$ into a finite group.*

Example 2.3.3. *We continue with the elliptic curve*

$$y^2 = x^3 + 3x + 8 \; over \; \mathbb{F}_{13}$$

. from Example 2.3.2, and we use the addition algorithm $(Theorem\ 2.2.1)$ to add the points $P = (9, 7)$ and $Q = (1, 8)$ in $E(\mathbb{F}_{13})$. First we compute

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{8-7}{1-9} = \frac{1}{-8} = \frac{1}{5} = 8$$

Next we compute

$$x_3 = m^2 - x_1 - x_2 = 64 - 9 - 1 = 54 = 2,$$

$$y_3 = m(x_1 - x_3) = 10$$

This completes the computation of

$$P + Q = (1, 8) + (9, 7) = (2, 10) \quad in\ E(\mathbb{F}_{13}).$$

Similarly, we can use the addition algorithm to add $P = (9, 7)$ to itself. Keeping in mind that all calculations are in $\mathbb{F}_{13}$, we find that

$$m = \frac{3x_1^2 + A}{2y_1} = \frac{246}{14} = 1$$

then

$$x_3 = m^2 - x_1 - x_2 = 1 - 9 - 9 = 9 \ \ and \ \ y_3 = m(x_1 - x_3) - y_1 = 1(9 - 9) - 7 = 6,$$

so $P + P = (9, 7) + (9, 7) = (9, 6)$ in $E(\mathbb{F}_{13})$. In a similar fashion, we can compute the sum of every pair of points in $E(\mathbb{F}_{13})$. The results are listed in Table 2.5.

$+$	∞	$(1,5)$	$(1,8)$	$(2,3)$	$(2,10)$	$(9,6)$	$(9,7)$	$(12,2)$	$(12,11)$
∞	∞	$(1,5)$	$(1,8)$	$(2,3)$	$(2,10)$	$(9,6)$	$(9,7)$	$(12,2)$	$(12,11)$
$(1,5)$	$(1,5)$	$(2,10)$	∞	$(1,8)$	$(9,7)$	$(2,3)$	$(12,2)$	$(12,11)$	$(9,6)$
$(1,8)$	$(1,8)$	∞	$(2,3)$	$(9,6)$	$(1,5)$	$(12,11)$	$(2,10)$	$(9,7)$	$(12,2)$
$(2,3)$	$(2,3)$	$(1,8)$	$(9,6)$	$(12,11)$	∞	$(12,2)$	$(1,5)$	$(2,10)$	$(9,7)$
$(2,10)$	$(2,10)$	$(9,7)$	$(1,5)$	∞	$(12,2)$	$(1,8)$	$(12,11)$	$(9,6)$	$(2,3)$
$(9,6)$	$(9,6)$	$(2,3)$	$(12,11)$	$(12,2)$	$(1,8)$	$(9,7)$	∞	$(1,5)$	$(2,10)$
$(9,7)$	$(9,7)$	$(12,2)$	$(2,10)$	$(1,5)$	$(12,11)$	∞	$(9,6)$	$(2,3)$	$(1,8)$
$(12,2))$	$(12,2)$	$(12,11)$	$(9,7)$	$(2,10)$	$(9,6)$	$(1,5)$	$(2,3)$	$(1,8)$	∞
$(12,11)$	$(12,11)$	$(9,6)$	$(12,2)$	$(9,7)$	$(2,3)$	$(2,10)$	$(1,8)$	∞	$(1,5)$

Table 2.5: Addition table for $E : y^2 = x^3 + 3x + 8$ over $\mathbb{F}_{13}$

2.4 The elliptic curve discrete logarithm problem

In order to create a cryptosystem based on the discrete logarithm problem **(PLD)** in the finite field $\mathbb{F}_q^*$, Alice publishes two numbers g and h, and her secret is the exponent x that solves the

congruence

$$h \equiv g^x \ (mod\ q).$$

let's consider how Alice can do something similar with a elliptic curve E over $\mathbb{F}_q$. If Alice views g and h as being elements of the group $\mathbb{F}_q^*$, then the discrete logarithm problem requires Alice's adversary Eve to find an x such that

$$h \equiv \underbrace{g \cdot g \cdot g \cdots g}_{x\ multiplications} (mod\ q)$$

In other words, Eve needs to determine how many times g must be multiplied by itself in order to get to h.
With this formulation, it is clear that Alice can do the same things with the group of points $E(\mathbb{F}_q)$ of an elliptic curve E over a finite field $\mathbb{F}_q$. She chooses and publishes two points P and Q in $E(\mathbb{F}_q)$, and her secret is an integer n that makes

$$Q \equiv \underbrace{P + P + P + ... + P}_{n\ additions\ on\ E} = nP$$

So Eve needs to find out how many times P must be added to itself in order to get Q. Keep in mind that although the **addition law** on an elliptic curve is conventionally written with a plus sign, addition on E is actually a very complicated operation, so this elliptic analogue of the discrete logarithm problem may be quite difficult to solve.

Definition 2.4.1. *Let E be an elliptic curve over the finite field $\mathbb{F}_q$ and let P and Q be points in $E(\mathbb{F}_q)$. The Elliptic Curve Discrete Logarithm Problem **(ECDLP)** is the problem of finding an integer n such that $Q = nP$. By analogy with the discrete logarithm problem in $\mathbb{F}_q^*$, we denote this integer n by*

$$n = log_P(Q)$$

And we call n the elliptic discrete logarithm of Q with respect to P.

Remark 2.4.1. *Our definition of $log_P(Q)$ is not quite precise. The first difficulty is that there may be points $P, Q \in E(\mathbb{F}_q)$ such that Q is not a multiple of P. In this case, $log_P(Q)$ is not defined. However, for cryptographic purposes, Alice starts out with a public point P and a private integer n and she computes and publishes the value of $Q = nP$. So in practical applications, $log_P(Q)$ exists and its value is Alice's secret The second difficulty is that if there is one value of n satisfying $Q = nP$, then there are many such values. To see this, we first note that there exists a positive*

integer s such that $sP = \infty$. Since $E(\mathbb{F}_q)$ is finite, the points in the list $P, 2P, 3P, 4P, ...$Can not all be distinct. Hence there are integers $k > j$ such that $kP = jP$, and we can take $s = k - j$. The smallest such s such that $s \geq 1$ is called the order of P. thus if s is the order of P and if n_0 is any integer such that $Q = n_0P$, then the solutions to $Q = nP$ are the integers $n = n_0 + is$ with $i \in \mathbb{Z}$. This means that the value of $log_P(Q)$ is really an element of $\mathbb{Z}/s\mathbb{Z}$, i.e, $log_P(Q)$ is an integer modulo s, where s is the order of P. For concreteness, we could set $log_P(Q)$ equal to n_0. However, the advantage of defining the values to be in $\mathbb{Z}/s\mathbb{Z}$ is that the elliptic discrete logarithm then satisfies:

$$log_P(Q_1 + Q_2) = log_P(Q_1) + log_P(Q_2) \ \ for\ all\ \ Q1, Q2 \in E(\mathbb{F}_q). \tag{2.4}$$

Notice the analogy with the ordinary logarithm $log(\alpha\beta) = log(\alpha) + log(\beta)$ and the discrete logarithm for $\mathbb{F}_q^*$. The fact that the discrete logarithm for $E(\mathbb{F}_q)$ satisfies (2.4) means that it respects the addition law when the group $E(\mathbb{F}_q)$ is mapped to the group $\mathbb{Z}/s\mathbb{Z}$. We say that the map log_P defines a group homomorphism.

$$log_P : E(\mathbb{F}_q) \longrightarrow \mathbb{Z}/s\mathbb{Z}.$$

Example 2.4.1. *Consider the elliptic curve*

$$E : y^2 = x^3 + 8x + 7 \ \ over\ \mathbb{F}_{73}.$$

The points $P = (32, 53)$ and $Q = (39, 17)$ are both in $E(\mathbb{F}_{73})$, and it is easy to verify that :

$$Q = 11P \ \ so \ \ log_P(Q) = 11.$$

Similarly, $R = (35, 47) \in E(\mathbb{F}_{73})$ and $S = (58, 4) \in E(\mathbb{F}_{73})$, and after some computation, we find that they satisfy $R = 37P$ and $S = 28P$, so

$$Log_P(R) = 37 \ \ and \ \ log_P(S) = 28.$$

Finally, we mention that $\#E(\mathbb{F}_{73}) = 82$, but P satisfies $41P = \infty$. Thus P has the order $41 = 82/2$, so only half of the points in $E(\mathbb{F}_{73})$ are multiples of P. For example, $(20, 65)$ is in $E(\mathbb{F}_{73})$, but it does not equal a multiple of P.

2.4.1 How hard is the ECDLP?

Let be the group of elliptical points $E(\mathbb{F}_q)$. To solve $Q = nP$, Eve chooses random integers $j_1, ..., j_r$ and $k_1, ..., k_r$ between 1 and p and make two lists of points:
List $\#1$:

$$j_1P, j_2P, j_3P, ..., j_rP,$$

List $\#2$:

$$k_1P + Q, k_2P + Q, k_3P + Q, ..., k_rP + Q.$$

As soon as she finds a match (collision) between the two lists, she is done, because if she finds $j_uP = k_vP + Q$, then $Q = (j_u - k_v)P$ provides the solution.
If r is somewhat larger than $\sqrt{p}$, say $r \approx 3\sqrt{q}$, then there is a very good chances that there will be a collision.
This naive collision algorithm requires quite a lot of storage for the two lists. However, it is not hard to adapt **Pollard's ρ method** to devise a storage-free collision algorithm with a similar running time. In any case, there are certainly algorithms that solve the **ECDLP** for $E(\mathbb{F}_q)$ in $\infty(\sqrt{q})$ steps. We have seen that there are much faster ways to solve the discrete logarithm problem for $E(\mathbb{F}_q)^*$. In particular, the index calculus which has a sub-exponential running time, i.e., the running time is $O(q^\epsilon)$ for every $\epsilon > 0$. The principal reason that elliptic curves are used in cryptography is the fact that there are no index calculus algorithms known for the ECDLP, and indeed, there are no general algorithms known that solve the ECDLP in fewer than $\infty(\sqrt{q})$ steps. In other words, despite the highly structured nature of the group $E(\mathbb{F}_q)$, the fastest known algorithms to solve the ECDLP are no better than the generic algorithm that works equally well to solve the discrete logarithm problem in any group. This fact is sufficiently important that it bears highlighting. This fact is sufficiently important that it bears highlighting.

2.4.2 The fastest known algorithm to solve ECDLP in $E(\mathbb{F}_q)$ takes about $\sqrt{q}$ steps .

thus the **ECDLP** appears to be much more difficult than the **DLP**. Recall, however, that there are some primes q for which the DLP in $\mathbb{F}_q^*$ is comparatively easy. For example, if $q1$ is a product of small primes, then the **Pohlig-Hellman** algorithm gives a quick solution to the DLP in $\mathbb{F}_q^*$.
In a similar fashion, there are some elliptic curves and some primes for which the ECDLP in $E(\mathbb{F}_q)$ comparatively easy.

2.5 General Attacks on Discrete Logs

In this section, we discuss attacks that work for arbitrary groups. Since our main focus is elliptic curves, we write our group G additively. Therefore, we are given $P, Q \in G$ and we are trying to solve $nP = Q$ (we always assume that n exists). Let N be the order of G. Usually, we assume N is known. For simplicity, it is usually assumed that P generates G.

2.5.1 The Double-and-Add algorithm

It appears to be quite difficult to recover the value of n from the two points P and $Q = nP$ in $E(\mathbb{F}_q)$,i.e it is difficult to solve the $ECDLP$. We will say more about the difficulty of the $ECDLP$ in the next methods. However, to use the function:

$$\mathbb{Z} \longrightarrow E(\mathbb{F}_q), \quad n \longmapsto nP,$$

for cryptography we need to efficiently compute nP from the known values n and P. If n is large, we do not want to compute nP by computing $P, 2P, 3P, 4P, ...$ The most efficient way to compute nP is very similar to the method for computing powers $a^n(\ mod\ N)$. However, since the operation on an elliptic curve is written as addition instead of as multiplication, we call it **"double-and-add"** instead of **"square-and-multiply."**

The underlying idea is the same as before. We first write n in binary form as

$$n = n_0 + n_1 \cdot 2 + n_2 \cdot 4 + n_3 \cdot 8 + ... + n_r \cdot 2^r \qquad with\ n_0, n_1, ..., n_r \in \{0, 1\}\,.$$

(We also assume that $n_r = 1$.) Next we compute the following quantities:

$$Q_0 = P, Q_1 = 2Q_0, Q_2 = 2Q_1, ..., Q_r = 2Q_{r-1}.$$

Notice that Q_i is simply twice the previous Q_{i-1}, so

$$Q_i = 2^i P$$

These points are referred to as 2-powers of P, and computing them requires r doublings. Finally, we compute nP using at most r additional additions,

$$nP = n_0 Q_0 + n_1 Q_1 + n_2 Q_2 + ... + n_r Q_r.$$

We'll refer to the addition of two points in $E(\mathbb{F}_q)$ as a point operation. Thus the total time to compute nP is at most $2r$ point operations in $E(\mathbb{F}_q)$. Notice that $n \geq 2^r$, so it takes no more than $2log_2(n)$ point operations to compute nP. This makes it feasible to compute nP even for very large values of n. Here is the double-and-add algorithm:

Input. Point $P \in E(\mathbb{F}_q)$ and an integer $n \geq 1$.

1. Set $Q = P$ and $R = \infty$.
2. Loop while $n > 0$.
3. - if $n \equiv 1 \ (mod\ 2)$ then $R = R + Q$
4. - Set $Q = 2Q$ and $n = [n/2]$
5. If $n > 0$, continue with loop at Step 2.
6. Return the point R which equals nP.

Example 2.5.1. *We use the Double-and-Add Algorithm to compute nP in $E(\mathbb{F}_q)$ for:*

$$n = 947, \quad E : y^2 = x^3 + 14x + 19, \quad p = 3623, \quad P = (6, 730).$$

The binary expansion of n is:

$$n = 947 = 1 + 2 + 2^4 + 2^5 + 2^7 + 2^8 + 2^9.$$

The step-by-step calculation, which requires nine doublings and six additions, is given in Table 2.3. *The final result is* $947P = (3492, 60)$.

2.5.2 Baby Step, Giant Step

This method, developed by D. Shanks, requires approximately $\sqrt{N}$ steps and around $\sqrt{N}$ storage. Therefore it only works well for moderate sized N. The procedure is as follows.

1. Fix an integer $m \geq \sqrt{N}$ and compute mP.
2. Make and store a list of iP for $0 \leq i < m$.
3. Compute the points $Q - jmP$ for $j = 0, 1, ..., m - 1$ until one matches an element from the stored list.

Step i	n	$Q = 2^i P$	R
0	947	$(6, 730)$	∞
1	473	$(2521, 3601)$	$(6, 730)$
2	236	$(2277, 502)$	$(2149, 196)$
3	118	$(3375, 535)$	$(2149, 196)$
4	59	$(1610, 1851)$	$(2149, 196)$
5	29	$(1753, 2436)$	$(2838, 2175)$
6	14	$(2005, 1764)$	$(600, 2449)$
7	7	$(2425, 1791)$	$(600, 2449)$
8	3	$(3529, 2158)$	$(3247, 2849)$
9	1	$(2742, 3254)$	$(932, 1204)$
10	0	$(1814, 3480)$	$(3492, 60)$

Table 2.6: Computing $947 \cdot (6, 730)$ *on* $y^2 = x^3 + 14x + 19$ *modulo* 3623

4. If $iP = Q - jmP$, we have $Q = kP$ with $k \equiv i + jm \ (mod\ N)$.

Why does this work? Since $m^2 > N$, we may assume the answer k satisfies $0 \leq k < m^2$. Write $k = k_0 + mk_1$ with $k_0 \equiv k \ (mod\, m)$ and $0 \leq k_0 < m$ and let $k_1 = (k - k_0)/m$. Then $0 \leq k_1 < m$. When $i = k_0$ and $j = k_1$, we have

$$Q - k_1 mP = kP - k_1 mP = k_0 P,$$

so there is a match. The point iP is calculated by adding P (a **"baby step"**) to $(i-1)P$. The point $Q - jmP$ is computed by adding $-mP$ (a **"giant step"**) to $Q - (j-1)mP$. The method was developed by Shanks for computations in algebraic number theory.

Note that we did not need to know the exact order N of G. We only required an upper bound for N. Therefore, for elliptic curves over $\mathbb{F}_q$, we could use this method with $m^2 \geq q + 1 + 2\sqrt{q}$, by **Hasse's theorem**. A slight improvement of the method can be made for elliptic curves by computing and storing only the points iP for $0 \leq i \leq m/2$ and checking whether $Q - jmP = \pm iP$.

Example 2.5.2. *Let $G = E(\mathbb{F}_{41})$, where E is given by $y^2 = x^3 + 2x + 1$. Let $P = (0, 1)$ and $Q = (30, 40)$. By Hasse's theorem, we know that the order of G is at most 54, so we let $m = 8$. The points iP for $1 \leq i \leq 7$ are*

$$(0, 1), (1, 39), (8, 23), (38, 38), (23, 23), (20, 28), (26, 9).$$

We calculate $Q - jmP$ *for* $j = 0, 1, 2$ *and obtain*

$$(30, 40), (9, 25), (26, 9),$$

at which point we stop since this third point matches $7P$*. Since* $j = 2$ *yielded the match, we have*

$$(30, 40) = (7 + 2 \cdot 8)P = 23P.$$

Therefore $k = 23$*.*

2.5.3 Pohlig-Hellman attack

The **Pohlig-Hellman** algorithm efficiently reduces the computation of $l = log_P Q$ to the computation of discrete logarithms in the prime order subgroups of $\langle P \rangle$. It follows that the $ECDLP$ in $\langle P \rangle$ is no harder than the $ECDLP$ in its prime order subgroups. Hence, in order to maximize resistance to the Pohlig-Hellman attack, the elliptic curve parameters should be selected so that the order n of P is divisible by a large prime.We now outline the Pohlig-Hellman algorithm. Suppose that the prime factorization of n is $n = p_1^{e_1} p_2^{e_2} ... p_r^{e_r}$. The Pohlig-Hellman strategy is to compute $l_i \equiv l \; mod \; p_i^{e_i}$ for each $1 \leq i \leq r$, and then solve the system of congruences

$$\begin{aligned} l &\equiv l_1 \; mod \; p_1^{e_1} \\ l &\equiv l_2 \; mod \; p_2^{e_2} \\ &\vdots \\ l &\equiv l_r \; mod \; p_r^{e_r} \end{aligned}$$

for $l \in [0, n-1]$. (The Chinese Remainder Theorem guarantees a unique solution.) We show how the computation of each l_i can be reduced to the computation of e_i discrete logarithms in the subgroup of order p_i of $\langle P \rangle$. To simplify the notation, we write p for p_i and e for e_i . Let the base-p representation of l_i be

$$l_i = z_0 + z_1 p + z_2 p_2 + ... + z_{e-1} p^{e-1}$$

where each $z_i \in [0, p-1]$. The digits $z_0, z_1, ..., z_{e-1}$ are computed one at a time as follows. We first compute $P_0 = (n/p)P$ and $Q_0 = (n/p)Q$. Since the order of P_0 is p, we have

$$Q_0 = \frac{n}{p} Q = l \left(\frac{n}{p} P \right) = l P_0 = z_0 P_0.$$

Hence $z_0 = log_{P_0} Q_0$ can be obtained by solving an ECDLP instance in $\langle P_0 \rangle$. Next,we compute $Q_1 = (n/p^2)(Q - z_0 P)$. We have

$$\begin{aligned} Q_1 &= \frac{n}{p^2}(Q - z_0 P) = \frac{n}{p^2}(l - z_0)P = (l - z_0)\left(\frac{n}{p^2}P\right) \\ &= (z_0 + z_1 p - z_0)\left(\frac{n}{p^2}P\right) = z_1\left(\frac{n}{p}P\right) = z_1 P_0 \end{aligned}$$

Hence $z_1 = log_{P_0} Q_1$ can be obtained by solving an $ECDLP$ instance in $\langle P_0 \rangle$. In general, if the digits $z_0, z_1, ..., z_{t-1}$ have been computed, then $z_t = log_{P_0} Q_t$, where

$$Q_t = \frac{n}{P^{t+1}}\left(Q - z_0 P - z_1 pP - z_2 p^2 P - ... - z_{t-1} p^{t-1} P\right).$$

Example 2.5.3. *(Pohlig-Hellman algorithm for solving the ECDLP) Consider the elliptic curve E defined over $\mathbb{F}7919$ by the equation:*

$$E : y^2 = x^3 + 1001x + 75.$$

Let $P = (4023, 6036) \in E(\mathbb{F}7919)$. The order of P is

$$n = 7889 = 7^3 \cdot 23$$

Let $Q = (4135, 3169) \in \langle P \rangle$. We wish to determine $l = log_P Q$.

a) We first determine $l_1 \equiv l \ (mod\ 7^3)$. We write $l_1 = z_0 + z_1 7 + z_2 7^2$ and compute

$$\begin{aligned} P_0 &= 7^2 \cdot 23P = (7801, 2071) \\ Q_0 &= 7^2 \cdot 23Q = (7801, 2071) \end{aligned}$$

and find that $Q_0 = P_0$, hence $z_0 = 1$. We next compute

$$Q_1 = 7 \cdot 23(Q - P) = (7285, 14)$$

and find that $Q_1 = 3P_0$, hence $z_1 = 3$. Finally, we compute

$$Q_2 = 23(Q - P - 3 \cdot 7P) = (7285, 7905)$$

and find that $Q_2 = 4P_0$*, hence* $z_2 = 4$*. Thus* $l_1 = 1 + 3 \cdot 7 + 4 \cdot 7^2 = 218$.

b) We next determine $l_2 \equiv l \ (mod\ 23)$*. We compute*

$$P_0 = 7^3 P = (7190, 7003) \qquad , Q_0 = 7^3 Q = (2599, 759)$$

and find that $Q_0 = 10P_0$*, hence* $l_2 = 10$.

c) Finally, we solve the pair of congruences

$$\begin{aligned} l &\equiv 218 \ (mod\ 7^3) \\ l &\equiv 10 \ (mod\ 23) \end{aligned}$$

and obtain $l = 4334$.

Chapter 3

Elliptic curve cryptosystems

3.1 Cryptography

In this chapter, we discuss some well-known means by which **Alice** can send a private (i.e. encrypted) message to **Bob**. The information that Alice wants to share with Bob is called the **plaintext**. The encrypted plaintext that Alice actually sends to Bob is called the **ciphertext**. A cryptosystem consists of a finite set of possible plaintexts, a finite set of possible ciphertexts, a finite set of possible keys, an **encryption rule** for encrypting plaintext into ciphertext and a **decryption rule** for decrypting ciphertext back to plaintext. The general idea behind any cryptosystem is that Alice and Bob must share a secret key which is used to encrypt a message, and without which the plaintext cannot be recovered.

Private-key Cryptosystems If there is a way for Alice and Bob to secretly share a key K prior to the transmission of plaintext, they can use encryption and decryption rules defined by their secret value of K. Cryptosystems of this form are called **private-key cryptosystems**. One approach to sharing keys is the **key agree- ment protoco**l whereby Alice and Bob jointly establish the secret key by using values they have sent each other over a public channel. In these systems, the decryption rule is identical to or easily derived from the encryption rule. Hence, exposure of the encryption rule to an eavesdropper will render the system insecure.

Public-key Cryptosystems The security of private-key systems depends on the secret exchange or establishment of keys between Alice and Bob. However, in **public-key cryptosystems** Bob keeps his key (and his decryption rule) to himself, whereas the corresponding encryption rule is publicly known. Therefore, Alice can send encrypted messages without any prior sharing of keys, and Bob will be the only person able to decrypt the messages sent to him.

3.2 Diffie-Hellman Key Exchange

Alice and **Bob** want to agree on a common key that they can use for exchanging data via a symmetric encryption scheme such as **DES** or **AES**. For example, Alice and Bob could be banks that want to transmit financial data. It is impractical and time-consuming to use a courier to deliver the key. Moreover, we assume that Alice and Bob have had no prior contact and therefore the only communication channels between them are public. One way to establish a secret key is the following method, due to Diffie and Hellman (actually, they used multiplicative groups of finite fields).

1. Alice and Bob agree on an elliptic curve E over a finite field $\mathbb{F}_q$ such that the discrete logarithm problem is hard in $E(\mathbb{F}_q)$. They also agree on a point $P \in E(\mathbb{F}_q)$ such that the subgroup generated by P has large order (usually, the curve and point are chosen so that the order is a large prime).
2. Alice chooses a secret integer n_A, computes $Q_A = n_A P$, and sends Q_A to Bob.
3. Bob chooses a secret integer n_B, computes $Q_B = n_B P$, and sends Q_B to Alice.
4. Alice computes $n_A Q_B = n_A n_B P$.
5. Bob computes $n_B Q_A = n_B n_A P$.
6. Alice and Bob use some publicly agreed on method to extract a key from $n_A n_B P$. For example, they could use the last 256 bits of the x-coordinate of $n_A n_B P$ as the key. Or they could evaluate a hash function at the x-coordinate.

Table 3.1 summarizes elliptic Diffie-Hellman key exchange.

Public Parameter Creation	
A trusted party chooses and publishes a (large) prime q, an elliptic curve E over $\mathbb{F}_q$, and a point P in $E(\mathbb{F}_q)$.	
Private Computations	
Alice	Bob
Chooses a secret integer n_A. Computes the point $Q_A = n_A P$	Chooses a secret integer n_B. Computes the point $Q_B = n_B P$.
Public Exchange of Values	
Alice sends Q_A to Bob $\longrightarrow$	Q_A
Q_B $\longleftarrow$	Bob sends Q_B to Alice
Further Private Computations	
Alice	Bob
Computes the point $n_A Q_B$.	Computes the point $n_B Q_A$.
The shared secret value is $n_A Q_B = n_A(n_B P) = n_B(n_A P) = n_B Q_A$.	

Table 3.1: Diffie-Hellman key exchange using elliptic curves

The only information that the eavesdropper Eve sees is the curve E, the finite field $\mathbb{F}_q$, and the points P, n_AP and n_BP . She therefore needs to solve the following:

DIFFIE-HELLMAN PROBLEM

Given P, n_AP and n_BP in $E(\mathbb{F}_q)$, compute n_An_BP.

If Eve can solve discrete logs in $E(\mathbb{F}_q)$, then she can use P and n_AP to find n_A. Then she can compute $n_A(n_BP)$ to get n_An_BP . However, it is not known whether there is some way to compute n_An_BP without first solving a discrete log problem.

DECISION DIFFIE-HELLMAN PROBLEM Given P, n_AP and n_BP in $E(\mathbb{F}_q)$,and given a point $Q \in E(\mathbb{F}_q)$ determine whether or not $Q = n_An_BP$

Example 3.2.1. *Alice and Bob decide to use the Elliptic Diffie-Hellman with the following prime, curve, and point:*

$$q = 17, \quad E : y^2 = x^3 + 2x + 2, \quad P = (5, 1) \in E(\mathbb{F}_{17}).$$

Alice and Bob choose the respective secret values $n_A = 3$ *and* $n_B = 9$*, then*

$$Alice\ computes\ Q_A = 3P = (10, 6) \in E(\mathbb{F}_{17})$$

$$Bob\ computes\ Q_B = 9P = (7, 6) \in E(\mathbb{F}_{17})$$

Alice sends Q_A *to Bob and Bob sends* Q_B *to Alice. Finally,*

$$Alice\ computes\ n_AQ_B = 3(7, 6) = (13, 7) \in E(\mathbb{F}_{17})$$

$$Bob\ computes\ n_BQ_A = 9(10, 6) = (13, 7) \in E(\mathbb{F}_{17})$$

Example 3.2.2. *Alice and Bob decide to use the Elliptic Diffie-Hellman with the following prime, curve, and point:*

$$q = 3851, \quad E : y^2 = x^3 + 324x + 1287, \quad P = (920, 303) \in E(\mathbb{F}_{3851}).$$

Alice and Bob choose the respective secret values $n_A = 1194$ *and* $n_B = 1759$*, then*

$$Alice\ computes\ Q_A = 1194P = (2067, 2178) \in E(\mathbb{F}_{3851})$$

$$Bob\ computes\ Q_B = 1759P = (3684, 3125) \in E(\mathbb{F}_{3851})$$

Alice sends Q_A to Bob and Bob sends Q_B to Alice. Finally,

$$Alice\ computes\ n_A Q_B = 1194(3684, 3125) = (3347, 1242) \in E(\mathbb{F}_{3851})$$

$$Bob\ computes\ n_B Q_A = 1759(2067, 2187) = (3347, 1242) \in E(\mathbb{F}_{17})$$

Bob and Alice have exchanged the secret point $(3347, 1242)$, they should discard the y-coordinate and treat only the value $x = 3347$ as a secret shared value. One way for Eve to discover Alice and Bob's secret is to solve the ECDLP

$$nP = Q_A,$$

since if Eve can solve this problem, then she knows n_A and can use it to compute $n_A Q_B$. Of course, there might be some other way for Eve to compute their secret without actually solving the ECDLP.

Definition 3.2.1. *Let $E(\mathbb{F}_q)$ be an elliptic curve over a finite field and let $P \in E(\mathbb{F}_q)$. The Elliptic Curve Diffie–Hellman Problem is the problem of computing the value of $n_1 n_2 P$ from the known values of $n_1 P$ and $n_2 P$.*

Remark 3.2.1. *Elliptic Diffie–Hellman key exchange requires Alice and Bob to exchange points on an elliptic curve. A point Q in $E(\mathbb{F}_q)$ consists of two coordinates $Q = (x_Q, y_Q)$, where x_Q and y_Q are elements of the finite field $\mathbb{F}_q$, so it appears that Alice must send Bob two numbers in $\mathbb{F}_q$. However, those two numbers modulo p do not contain as much information as two arbitrary numbers, since they are related by the formula*

$$y_Q^2 = x_Q^3 + Ax_Q + B\ in\ \mathbb{F}_q.$$

Note that Eve knows A and B, so if she can guess the correct value of x_Q, then there are only two possible values for y_Q, and in practice it is not too hard for her to actually compute the two values of y_Q.

There is thus little reason for Alice to send both coordinates of Q_A to Bob, since the y-coordinate contains so little additional information. Instead, she sends Bob only the x-coordinate of Q_A. Bob then computes and uses one of the two possible y-coordinates. If he happens to choose the "correct" y, then he is using Q_A, and if he chooses the "incorrect" y (which is the negative of

the correct y), then he is using $-Q_A$. In any case, Bob ends up computing one of

$$\pm n_B Q_A = \pm(n_A n_B)P.$$

Similarly, Alice ends up computing one of $\pm(n_A n_B)P$. Then Alice and Bob use the x-coordinate as their shared secret value, since that x-coordinate is the same regardless of which y they use.

Example 3.2.3. *Alice and Bob decide to exchange another secret value using the same public parameters as in Example* 3.1.2*:*

$$q = 3851, \quad E : y^2 = x^3 + 324x + 1287, \quad P = (920, 303) \in E(\mathbb{F}_{3851}).$$

However, this time they want to send fewer bits to one another. Alice and Bob respectively choose new secret values $n_A = 2489$ and $n_B = 2286$, and as before,

$$Alice\ computes\ Q_A = n_A P = 2489(920, 303) = (593, 719) \in E(\mathbb{F}_{3851})$$

$$Bob\ computes\ Q_B = n_B P = 2286(920, 303) = (3681, 612) \in E(\mathbb{F}_{3851})$$

However, rather than sending both coordinates, Alice sends only $x_A = 593$ to Bob and Bob sends only $x_B = 3681$ to Alice.
Alice substitutes $x_B = 3681$ into the equation for E and finds that

$$y_B^2 = x_B^3 + 324x_B + 1287 = 3681^3 + 324 \cdot 3681 + 1287 = 997.$$

(Recall that all calculations are performed in $\mathbb{F}_{3851}$.) Alice needs to compute a square root of 997 *modulo* 3851*. Therefore,*

$$y_B = 997^{963} \equiv 612\ (mod\ 3851).$$

It happens that she gets the same point $Q_B = (x_B, y_B) = (3681, 612)$ that Bob used, and she computes

$$n_A Q_B = 2489(3681, 612) = (509, 1108)$$

.

Similarly, Bob substitutes $x_A = 593$ into the equation for E and takes a square root,

$$y_A^2 = x_A^3 + 324x_A + 1287 = 593^3 + 324 \cdot 593 + 1287 = 927,$$

$$y_A \equiv 3132 \ (mod\ 3851).$$

Bob then uses the point $Q'_A = (593, 3132)$, which is not Alice's point Q_A, to compute $n_B Q'_A = 2286(593, 3132) = (509, 2743)$. Bob and Alice end up with points that are negatives of one another in $E(\mathbb{F}_q)$, but that is all right, since their shared secret value is the x-coordinate $x = 593$, which is the same for both points.

3.3 ElGamal Public Key Encryption

Bob wants to send a message to Alice. First, Alice establishes his public key as follows. He chooses an elliptic curve E over a finite field v such that the discrete log problem is hard for $E(\mathbb{F}_q)$. He also chooses a point P on E (usually, it is arranged that the order of P is a large prime). He chooses a secret integer n_A and computes $Q_A = n_A P$. The elliptic curve E, the finite field $\mathbb{F}_q$, and the points P and Q_A are Alices public key. They are made public. Alices private key is the integer n_A.

To send a message to Alice, Bob does the following:

1. Downloads Alices public key.
2. Expresses her message as a point $M \in E(\mathbb{F}_q)$.
3. Chooses a secret random integer k and computes $C_1 = kP$.
4. Computes $C_2 = M + kQ_A$.
5. Sends C_1, C_2 to Alice.

Alice decrypts by calculating

$$M = C_2 - n_A C_1.$$

This decryption works because

$$C_2 - n_A C_1 = (M + kQ_A) - n_A(kP) = M + k(n_A P) - n_A kP = M.$$

The elliptic ElGamal public key cryptosystem is summarized in table 3.2

Public Parameter Creation	
A trusted party chooses and publishes a (large) prime q, an elliptic curve E over $\mathbb{F}_q$, and a point P in $E(\mathbb{F}_q)$.	
Alice	Bob
Key Creation	
Chooses a private key n_A. Computes $Q_A = n_A P$ in $E(\mathbb{F}_q)$. Publishes the public key Q_A.	• • •
Encryption	
• • • • • •	Chooses plaintext $M \in E(\mathbb{F}_q)$. Chooses an ephemeral key k. Uses Alice's public key Q_A to compute $C_1 = kP \in E(\mathbb{F}_q)$. and $C_2 = M + kQ_A \in E(\mathbb{F}_q)$. Sends ciphtertext (C_1, C_2) to Alice.
Decryption	
Computes $C_2 - n_A C_1 \in E(\mathbb{F}_q)$. This quantity is equal to M.	• •

Table 3.2: Elliptic ElGamal key creation, encryption, and decryption

The eavesdropper Eve knows Alices public information and the points M_1 and M_2 If she can calculate discrete logs, she can use P and Q_A to find n_A, which she can then use to decrypt the message as $M_2 - n_A M_1$. Also, she could use P and M_1 to find k. Then she can calculate $M = M_2 - kQ_B$. If she cannot calculate discrete logs, there does not appear to be a way to find M.
It is important for Bob to use a different random k each time she sends a message to Alice. Suppose Bob uses the same k for both M and M'. Eve recognizes this because then $M_1 = M_1'$. She then computes $M_2' - M_2 = M' - M$. Suppose M is a sales announcement that is made public a day later. Then Eve finds out M, so she calculates $M' = M - M_2 + M_2'$. Therefore, knowledge of one plaintext M allows Eve to deduce another plaintext M' in this case.

Example 3.3.1. *Let $E : y^2 = x^3 + 4x + 20$ be an elliptic curve over $\mathbb{F}_{29}$ (**example 2.2.4**), $\mathbb{F}_{29}$ is a cyclic group of order $\#\mathbb{F}_{29} = 37$. We put a correspondence between the points of $\mathbb{F}_{29}$ and the english alphabet letters excluding space, Greek letters, etc. as in the following table:*

∞	(1,5)	(4,19)	(20,3)	(15,27)	(6,12)	(17,19)	(24,22)	(8,10)
ϵ	a	b	c	d	e	f	g	h
(14,23)	(13,23)	(10,25)	(19,13)	(16,27)	(5,22)	(3,1)	(0,22)	(27,2)
i	j	k	l	m	n	o	p	q
(2,23)	(2,6)	(27,27)	(0,7)	(3,28)	(5,7)	(16,2)	(19,16)	(10,4)
r	s	t	u	v	w	x	y	z
(13,6)	(14,6)	(8,19)	(24,7)	(17,10)	(6,17)	(15,2)	(20,26)	(4,10)
α	β	γ	δ	λ	θ	ϕ	φ	ψ
(1,24)								
Ω								

Sami wants to send the message **M ="master"** to bilal. So Sami chooses a point $P = (1, 5)$ a random number $n_A = 8$ as his private key and he computes his public key $Q_A = n_A P = (8; 10)$
Encryption: to encrypt the word "master", Bilal converts the letters m, a, s, t, e, r into points on the elliptic curve using the correspondence in the above table as the following $m \leftrightarrow (16, 27)$ $a \leftrightarrow (1, 5)$; $s \leftrightarrow (2, 6)$; $t \leftrightarrow (27, 27)$; $e \leftrightarrow (6, 12)$; $r \leftrightarrow (2, 23)$ and chooses a random ephemral key k then he computes C_1 and C_2 as follows

- Bilal selects a random number $k = 2$ for encrypting the character "m". Then the point $(16, 27)$ is encrypted as
  $C_1 = kP = 2(1, 5) = (4, 19)$ which corresponds to the character "b" in the conversion table.
  $C_2 = M + kQ_A = (16, 27) + 2(8, 10) = (8, 19)$ which corresponds to "γ" in the conversion table. So, the character "m" in the plain text is encrypted to two characters $\{b, \gamma\}$ in the cipher text.

- Let $k = 3$, Then the point $(1, 5)$ is encrypte as
  $C_1 = 3(1, 5) = (20, 3)$ which corresponds to "c" in the table.
  $C_2 = (1, 5) + 3(8, 10) = (19, 16)$, which corresponds to "$y$" in the table:
  So, "a" is encrypted as $\{c, y\}$.

- Let $k = 4$, Then the point $(2, 6)$ is encrypte as
  $C_1 = 4(1, 5) = (15, 27)$ which corresponds to "d" in the table.

$C_2 = (2, 6) + 4(8, 10) = (5, 22)$, which corresponds to "$n$" in the table:
So, "s" is encrypted as $\{d, n\}$.

- Let $k = 5$, Then the point $(27, 27)$ is encrypte as
  $C_1 = 5(1, 5) = (6, 12)$ which corresponds to "e" in the table.
  $C_2 = (27, 27) + 5(8, 10) = (5, 7)$, which corresponds to "$w$" in the table:
  So, "t" is encrypted as $\{e, w\}$.

- Let $k = 6$, Then the point $(6, 12)$ is encrypte as
  $C_1 = 6(1, 5) = (17, 19)$ which corresponds to "f" in the table.
  $C_2 = (6, 12)+6(8, 10) = (0, 22)$, which corresponds to "$p$" in the table, So, "$e$" is encrypted as $\{f, p\}$.

- Let $k = 7$, Then the point $(2, 23)$ is encrypte as
  $C_1 = 7(1, 5) = (24, 22)$ which corresponds to "g" in the table.
  $C_2 = (2, 23) + 7(8, 10) = \infty$, which corresponds to "$\epsilon$" in the table:
  So, "r" is encrypted as $\{g, \epsilon\}$.

Bilal communicates $\{b, \gamma, c, y, d, n, e, w, f, p, g, \epsilon\}$ as the ciphertext to Bilal in public chan- nel.
Decryption: Sami after receiving the cipher text $\{b, \gamma, c, y, d, n, e, w, f, p, g, \epsilon\}$ converts the cipher characters into the points

$$\{(4, 19); (8, 19); (20, 3); (19, 16); (15, 27); (5, 22); (17, 19); (0, 22); (24, 22); \infty\}$$

He decrypts the message taking two points at a time as the points C_1 and C_2 and computing

$$C_2 - n_A C_1 \in E(\mathbb{F}_q).$$

For $(C_1, C_2) = ((4, 19); (8, 19))$, we have $C_2 - n_A C_1 = (8, 19) - 8(4, 19) = (16, 27) \leftrightarrow m$
By the similar way, He continues to obtain the plaintext "$master$".

Conclusion

In this memory, we present mathematical concepts related to elliptic curves and their applications in cryptography, especially in The key to interpersonal exchange, so we've defined the famous problem Discrete logarithm on elliptic curves and its complexity which contributed to Cryptography has evolved through the birth of cryptography on curves Ellipticity **(ECC)**.

Bibliography

[1] **Lawrence C. Washington**, Elliptic Curves Number Theory and Cryptography Second Edition, University of Maryland College Park, Maryland, U.S.A, New York 2008

[2] **Darrel Hankerson, Alfred Menezes and Scott Vanstone**, Guide to Elliptic Curve Cryptography, Springer-Verlag New York 2004

[3] **William Stein**, Elementary Number Theory: Primes, Congruences, and Secrets, January 23, 2017

[4] **I. Merzougui**, Notions about elliptic curves and their uses in cryptography, Memory of master, University of msila, 2019.

[5] **Benjamin Hutz**, An Experimental Introduction to Number Theory, Rhode Island : American Mathematical Society ,2018

[6] **Bouchakour Errahmani Hichem** ,Sur la sécurité de l'information par le biais des courbes elliptiques , University of SIDI BEL ABBÈS , 2019

[7] **I.Blake, G.Seroussi, N.Smart**, Elliptic curves in cryptography, Cambridge University Press, 1999

[8] **Joseph H. Silverman**, The Arithmetic of Elliptic Curves ,Springer New York, 1986

[9] **Neal Koblitz**, Introduction to Elliptic Curves and Modular Forms, Springer US, 1984

[10] **Jeffrey Hoffstein, Jill Catherine Pipher, Joseph H Silverman, and Joseph H Silverman**. An introduction to mathematical cryptography, volume 1. Springer, 2008.

ملخص

كان تطبيق المنحنيات الإهليليجية في مجال التشفير حديثا نسبيا، فقد عرجت هذه الدراسة على جملة من الاحتمالات من حيث الأمان و التشفير وتطبيقات العالم الواقعي. نحن مهتمون على وجه الخصوص بأنظمة تشفير المفتاح العام التي تستخدم مشكلة اللوغاريتم المنفصل لمنحنى إهليليجي لتأسيس الأمان.
الهدف من هذه المذكرة هو تجميع أهم الحقائق والنتائج في نظرة عامة واسعة وموحدة لهذا المجال. ولتوضيح بعض النقاط بشكل أدق فقد تطرق البحث إلى دراسة مجموعة من أنظمة التشفير لتناظرية منحنى إهليليجي مثل مفتاح تبادل التشفير ديفي-هيلمان و الجمال

Abstract

The application of elliptic curves to the field of cryptography has been relatively recent. It has opened up a wealth of possibilities in terms of security, encryption, and real-world applications. In particular, we are interested in public-key cryptosystems that use the elliptic curve discrete logarithm problem to establish security. The objective of this memory is to assemble the most important facts and findings into a broad, unified overview of this field. To illustrate certain points, we also discuss a some cryptosystems of the elliptic curve analogue such as of the exchange key deffie-hellman and El Gamal cryptosystem.

Résumé

L'application de courbes elliptiques dans le domaine de la cryptographie est très récent. cette étude nous offre un certain nombre de possibilités en termes de sécurité, de chiffrement, et d'applications dans le monde réel. nous sommes intéressés notamment aux systèmes de cryptographie à clé publique qui utilisent le problème du logarithme discret de la courbe elliptique pour établir la Sécurité. L'objectif de cette mémoire est de rassembler les réalités les plus importants et les résultats les plus justes possibles dans ensemble plus large de ce domaine. Pour illustrer certains points d'une facon plus précise, nous avons abordé certains cryptosystèmes de l'analogue de la courbe elliptique tels que la clé d'échange deffie-hellman et ElGamal Cryptosystème