



DEMOCRATIC AND POPULAR REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
UNIVERSITY OF MOHAMED BOUDIAF OF M'SILA
Faculty of Mathematics and computer sciences
Department of Mathematics



In partial fulfillment of the requirement for the degree of Master of Mathematics

Field: Mathematics and computer sciences

Speciality: Mathematics

Option: Algebra and Discrete Mathematics

Submitted by

Imane Merzougui

Title

**Notions about elliptic curves and
their uses in cryptography**

Master's committee:

Mr. N. Ghadbane	Prof. Univ of M'sila	President
Mr. D. Mihoubi	Prof. Univ of M'sila	Advisor
Mr. L. Haboub	Prof. Univ of M'sila	Examiner

Promotion: 2018/2019

ملخص

نقدم في هذه المذكرة مفاهيم أساسية عن المنحنيات الإهليلجية وبعض خصائصها على الحقول المنتهية. ثم بعد ذلك نقدم بعض أنظمة التشفير التي تعتمد على صعوبة حل مشكل اللوغاريتم المنفصل في زمرة المنحنيات الإهليلجية.

كلمات مفتاحية: منحنى إهليلجي، زمرة تبديلية، حقل منتهي، لوغاريتم منفصل، نظام تشفير، تشفير، فك التشفير.

Abstract

In this memory, we present fundamental notions about elliptic curves and some of their properties over the finite fields. Then, we present some cryptosystems that based on the difficulty of solving the discrete logarithm problem in the elliptic curve group.

Keywords: Elliptic curves, abelian group, finite field, discrete logarithm, cryptosystem, encryption, decryption.

Résumé

Dans ce mémoire, nous présentons des notions fondamentales sur les courbes elliptiques et certains de leurs propriétés sur les corps finis. Ensuite, nous présentons quelques cryptosystèmes basés sur la difficulté de résoudre le problème de logarithme discret dans le groupe des courbes elliptiques.

Mot clés : Courbe elliptiques, groupe abélien, corps fini, logarithme discret, cryptosystème, cryptage, décryptage.

Acknowledgement

First and foremost, thanks to **God** almighty for the completion of this work. Only due to his blessings I could finish it.

I would like to express my deepest gratitude to my advisor, Mr : **D.Mihoubi**, for his invaluable advices and suggestions, I also would like to express my thanks to the jury members for their advices.

I would like to thank my **parents** for their encouragement who are so supportive to me throughout my life. My thanks also go to all my friends and everyone who have halped me during my study .

Thanks

Notations

$a b$	a divides b
$a \equiv b \pmod{n}$	a is congruent to b modulo n
\mathbb{Z}_n	The set of integers modulo n
$\varphi(n)$	The Euler's phi function of n
$\bar{a}, [a]$	Equivalence class of a
$ G , \#G$	The order of a group G
$\text{ord}(g)$	The order of a nonzero element g
$\langle g \rangle$	Cyclic group generated by g
$G \oplus G'$	Direct product of groups G and G'
\cong	Isomorphism
$\deg f$	The degree of the polynomial f
$R[X]$	Ring of polynomials in X with coefficients from R
$\text{char}(K)$	The characteristic of a field K
$K F$	K is an extension of F
$[K : F]$	Degree of the field extension K
\bar{K}	Algebraic closure of a field K
$\mathbb{F}_q, GF(q)$	Finite field with q elements
\mathbb{F}_q^*	$\mathbb{F}_q \setminus \{0\}$
$\log_g(h)$	The discrete logarithm of h to the base g
$\mathbb{A}^n(K)$	n -affine space over K
$\mathbb{A}^2(K)$	Plane affine space over K
$\mathbb{P}^2(K)$	Projective plane space over K
\mathcal{O}	Point at infinity
E/K	Elliptic curve over K
$E(K)$	The set of K -rational points of E
$E[n]$	The set of n -torsion points of E
e_k	Encryption function
d_k	Decryption function

Contents

Introduction	1
1 Preliminaries notions	2
1.1 Some notions in number theory	2
1.1.1 Divisibility and primes	2
1.1.2 Euler's phi-function	3
1.1.3 Congruences	4
1.2 Groups theory	6
1.2.1 group	7
1.2.2 Group morphism	10
1.3 Rings theory	11
1.3.1 Ring	11
1.3.2 Polynomial ring	12
1.3.3 Ring morphism	13
1.4 Fields	14
1.4.1 The field characteristic	15
1.4.2 Field Extensions	16
1.4.3 Finite fields	17
1.4.4 The discrete logarithm problem	19

2	Introduction to elliptic curves	21
2.1	Weierstrass equation	21
2.2	Affine plane curves	23
2.3	Projective plane curves	25
2.4	Elliptic curves	29
2.4.1	j -invariant and Isomorphisms	30
2.4.2	Group law	32
2.4.3	Torsion points	39
2.4.4	Elliptic curves over finite fields	41
2.4.5	Determining the group order	45
3	Cryptosystems based on elliptic curves	48
3.1	Private and Public key cryptosystems	48
3.1.1	RSA cryptosystem	51
3.2	Elliptic curve cryptosystems	53
3.2.1	The Elliptic Curves Discrete Logarithm Problem	53
3.2.2	Elliptic Curve Diffie –Hellman key exchange	57
3.2.3	Elliptic ElGamal public key cryptosystem	59
3.2.4	The Elliptic Curve Digital Signature Algorithm	63
3.2.5	Comparing ECC with RSA public key cryptosystem	67
	Conclusion	69

Introduction

Elliptic curves have been a well-studied mathematical object, fascinating many renowned mathematicians, as these curves offer a rich and insightful structure.

Elliptic curves discovered in the middle of nineteenth century. They have been playing an important role in different branches of mathematics especially in number theory and in related fields such as cryptography.

In 1984, Hendrik Lenstra, Jr. described a new factorization method using elliptic curves.

Elliptic curves play an important role in the proof of Fermat's last theorem and they are used in the primality proofs.

In 1985, Neal Koblitz and Victor Miller independently proposed using elliptic curves to create cryptosystems. The security of these cryptosystems relies on the difficulty of the discrete logarithm problem in the group formed from the points on elliptic curves over finite fields.

The purpose of this memory is briefly present some basic properties of elliptic curves and how do we use them in cryptography.

This work is divided into three chapters:

In the first chapter, we begin with some elementary concepts in number theory, groups, rings and fields.

In the second chapter, we briefly discuss algebraic and projective plane curves, then we give important notions and results on elliptic curves.

In the third chapter, we present cryptosystems based on elliptic curves including key exchanges, encryption and digital signature.

Chapter 1

Preliminaries notions

The concepts that used later are presented in this chapter.

1.1 Some notions in number theory

Number theory is an old branch of mathematics and it has many applications in computer sciences.

1.1.1 Divisibility and primes

Definition 1.1.1 *Given integers a and b , we say that a divides b (or b is divisible by a) and we write $a|b$ if there exists an integer d such that $b = ad$. In this case we call a a **divisor** of b .*

Example 1.1.1 *Since $-12 = -3 \cdot 4$, then $-3|-12$. Since $30 = 2 \cdot 15$, then $2|30$.*

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

- (i) *If $a|b$ and $a|c$, then $a|(b + c)$.*
- (ii) *If $a|b$ and $b|c$, then $a|c$.*
- (iii) *If $a|b$ and $b|a$, then $a = \pm b$.*
- (iv) *If $a|b$, then $a|kb$ for all integers k .*

(v) For any nonzero integer k , $a|b$ if and only if $ka|kb$.

(vi) If $a|b$ and $a|c$, then $a|kb + \ell c$ whenever k and ℓ are integers.

Theorem 1.1.2 (Division Algorithm). *Given integers a and b , with $b > 0$, there exist unique integers q and r satisfying*

$$a = qb + r \quad \text{and} \quad 0 \leq r < b.$$

The integers q and r are called, respectively, the quotient and remainder in the division of a by b . **Primes**

The study of primes has always been an important part of number theory.

Definition 1.1.2 *An integer $p > 1$ is called a **prime number**, or simply a **prime**, if its only positive divisors are 1 and p . An integer greater than 1 that is not a prime is termed **composite**.*

Example 1.1.2 *Among the first 10 positive integers, 2, 3, 5, 7 are primes and 4, 6, 8, 9, 10 are composite numbers.*

- *Note that the integer 2 is the only even prime.*
- *The integer 1 plays a special role, being neither prime nor composite.*

Theorem 1.1.3 (Fundamental Theorem of Arithmetic). *Every positive integer $n > 1$ is either a prime or a product of primes; this representation is unique.*

Example 1.1.3 $100 = 2^2 \cdot 5^2$; $641 = 641$; $999 = 3^3 \cdot 37$.

1.1.2 Euler's phi-function

Euler's phi-function play important roles in RSA cryptosystem that discribed in chapter 3.

Before introducing the definition of Euler's phi-function, we first recall the greatest common divisor of two integers.

Definition 1.1.3 Let a and b be integers, not both zero. The greatest common divisor of a and b , denoted by $\gcd(a, b)$ (or simply (a, b)) is the natural number g such that $g|a$, $g|b$, and g is divisible by any common divisor of a and b .

- If $\gcd(a, b) = 1$, then a and b are said to be **relatively prime** or **coprime**.

Example 1.1.4 The divisors of 12 are 1, 2, 3, 4, 6, 12, whereas those of 30 are 1, 2, 3, 5, 6, 10, 15, 30. Because 6 is the largest of the common divisors, it follows that $\gcd(12, 30) = 6$.

Definition 1.1.4 Let n be a positive integer. The Euler phi-function $\varphi(n)$ is defined to be the number of nonnegative integers b less than n which are prime to n .

$$\varphi(n) = |\{1 \leq b < n \mid \gcd(b, n) = 1\}|.$$

- It is easy to see that $\varphi(1) = 1$, and that $\varphi(p) = p - 1$ for any prime p .
- If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where p_i are distinct primes, then

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Example 1.1.5

- Since 23 is a prime number, then $\varphi(23) = 23 - 1 = 22$.
- Since $9 = 3^2$, then $\varphi(9) = \varphi(3^2) = 3^2 - 3 = 6$.

1.1.3 Congruences

Congruences are an other notion of division, invented by Gauss in 1801. In this section we will focus on the definition and some properties of them.

Definition 1.1.5 If $n \in \mathbb{N}$, then we say that a is **congruent** to b modulo n if $n|(a - b)$, denoted by

$$a \equiv b \pmod{n}.$$

- The integer n is the modulus of the congruence.

- When $n \nmid (a - b)$, we say that a is **incongruent** to b modulo n , or that a is not congruent to b modulo n . and in this case we write

$$a \not\equiv b \pmod{n}.$$

and we say that a and b are **incongruent** modulo n , or that a is not congruent to b modulo n .

Example 1.1.6

- Since $11 \mid (16 - (-6))$, then $16 \equiv -6 \pmod{11}$.
- For any $a, b \in \mathbb{Z}$, $a \equiv b \pmod{1}$, since $1 \mid (a - b)$.

Theorem 1.1.4 Let $n \in \mathbb{N}$.

- (i) The integers a and b are congruent modulo n if and only if there is an integer k such that $a = b + kn$.
- (ii) For arbitrary integers a and b , $a \equiv b \pmod{n}$ if and only if a and b have the same nonnegative remainder when divided by n .

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

- (i) $a \equiv a \pmod{n}$. called the reflexive property.
- (ii) If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$, called the symmetric property.
- (iii) If $a \equiv b \pmod{n}$, and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$, called the transitive property.
- (iv) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a \pm c \equiv b \pm d \pmod{n}$.
- (v) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.
- (vi) If $a \equiv b \pmod{n}$, then $am \equiv bm \pmod{n}$.
- (vii) If $a \equiv b \pmod{n}$, then $a^m \equiv b^m \pmod{n}$;
- (viii) If $a \equiv b \pmod{n}$ and m divides n , then $a \equiv b \pmod{n}$.

Proof. The proof follows directly from the definition of congruence. ■

Remark 1.1.1 (i) – (iii) mean that congruence modulo n is an equivalence relation over \mathbb{Z} which partitions the integers \mathbb{Z} into disjoint subsets.

Definition 1.1.6 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 \bar{a} or $[a]$ is defined as follows

$$\bar{a} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\}$$

in other words, the set of all elements b such that $a \equiv b \pmod{n}$.

- Since $a \equiv r \pmod{n}$ such that $a = kn + r$ and $0 \leq r < n$, $k \in \mathbb{Z}$ (r is the remainder in the eucliden division of a by n), then $\bar{a} = \bar{r}$.
- 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

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$$

Theorem 1.1.6 (Fermat's little theorem) If $a \in \mathbb{Z}$, and p is a prime such that $\gcd(a, p) = 1$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

In the next sections we briefly discuss a few basic concepts about some algebraic structures.

1.2 Groups theory

Definition 1.2.1 A **binary operation** on a set S is really just a particular function from $S \times S$ to S . We denote the image of the pair (a, b) under this function by $a \circ b$. In other words, the binary operation assigns to any two elements a and b of S the element $a \circ b$ of S .

- Many symbols are used for binary operations; the most common are $+$, \cdot , $-$, \circ , $*$, \star , \cup , \cap , \wedge , and \vee .

- A binary operation is also called a composition law.

1.2.1 group

Definition 1.2.2 A **group** (G, \cdot) is a set together with a binary operation " \cdot " satisfying the following axioms

- (i) G is **closed** under the operation " \cdot "; that is,

$$a \cdot b \in G \text{ for all } a, b \in G.$$

- (ii) the operation " \cdot " is **associative**; that is

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \text{ for all } a, b, c \in G.$$

- (iii) there is an **identity element** $e \in G$ such that

$$e \cdot a = a \cdot e = a \text{ for all } a \in G.$$

- (iv) each element $a \in G$ has an **inverse element** $a^{-1} \in G$ such that

$$a \cdot a^{-1} = a^{-1} \cdot a = e.$$

- If the operation is commutative, the group is called commutative or abelian.
- The number of elements in a group G is written $|G|$ or $\#G$ and is called the **order of the group**. G is called a **finite group** if $|G|$ is finite, and G is called a **infinite group** otherwise.

Example 1.2.1

- The set of all rational numbers, \mathbb{Q} , forms an abelian group $(\mathbb{Q}, +)$ under addition. The identity is 0, and the inverse of each element is its negative. Similarly, $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are all an abelian groups under addition.

- Let $n \in \mathbb{N}$, the set \mathbb{Z}_n together with the addition of congruence classes defined as follows

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

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

Remark 1.2.1 the identity element of a group is a unique element and we can denote it by e_G or 1_G . If the element g has an inverse, this inverse is a unique element.

Definition 1.2.3 The order of an element $g \in G$ is the smallest natural number k such that $g^k = e$, denoted by $\text{ord}(g)$.

Example 1.2.2 Let be the group $(\mathbb{Z}_6, +)$ with identity element $\bar{0}$.

- Since $\bar{2}^3 = \bar{2} + \bar{2} + \bar{2} = \bar{0}$, $\bar{2}^4 = \bar{2}^3 + \bar{2} = \bar{2}$, then $\text{ord}(\bar{2}) = 3$.
- Since $\bar{3}^2 = \bar{3} + \bar{3} = \bar{0}$, $\bar{3}^3 = \bar{3}^2 + \bar{3} = \bar{3}$, then $\text{ord}(\bar{3}) = 2$.

Theorem 1.2.1 Let G be a finite group. Then for every $g \in G$ it holds that:

- (i) $g^{|G|} = e_G$.
- (ii) $\text{ord}(g)$ divides $|G|$.

Definition 1.2.4 A group (G, \cdot) is called **cyclic** if there exists an element $g \in G$ such that

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

The element g is called a **generator** of the cyclic group.

Example 1.2.3 The group $(\mathbb{Z}, +)$ is an infinite cyclic group with generator 1 or -1 . The group $(\{1, -1, i, -i\}, \cdot)$ is a cyclic group of order 4 generated by i .

Definition 1.2.5 Let $(G_1, *)$ and (G_2, \cdot) be groups and let $G = G_1 \times G_2$ be their cartesian product. On G we define an operation \circ

via

$$(g_1, g_2) \circ (h_1, h_2) = (g_1 * h_1, g_2 \cdot h_2).$$

Then (G, \circ) is again a group, called the **direct product** of G_1 and G_2 , and is denoted by

$$G = G_1 \times G_2 \text{ or } G = G_1 \oplus G_2.$$

The neutral element is (e_1, e_2) , where e_i is neutral in G_i ($i = 1, 2$). The inverse of (g_1, g_2) is (g_1^{-1}, g_2^{-1}) .

Subgroup

Definition 1.2.6 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 .

Theorem 1.2.2 If (G, \cdot) is a group and H is non empty subset of G , then (H, \cdot) is a **subgroup** of (G, \cdot) if and only if

- (i) $a \cdot b \in H$ for all $a, b \in H$ (closure).
- (ii) $a^{-1} \in H$ for all $a \in H$ (existence of inverses).

And we will denote this by $H \leq_G G$.

- $\{e\}$ and G are called trivial subgroups of (G, \cdot) .

Example 1.2.4

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

1.2.2 Group morphism

A morphism (or homomorphism) between two algebraic structures is a function that preserves their operations.

Definition 1.2.7 *If (G, \cdot) and $(H, *)$ are two groups, the function $f : G \longrightarrow H$ called a group morphism if*

$$f(g_1 \cdot g_2) = f(g_1) * f(g_2) \text{ for all } g_1, g_2 \in G.$$

- A group morphism $f : G \longrightarrow G$ will be called an **endomorphism**, the set of all endomorphism of a group will be denoted by $\text{End}(G)$.
- A **group isomorphism** is a bijective group morphism. if there is an isomorphism between the groups (G, \cdot) and $(H, *)$, we say that (G, \cdot) and $(H, *)$ are **isomorphic** and write

$$(G, \cdot) \cong (H, *).$$

Theorem 1.2.3 *All cyclic groups are, up to isomorphism, given by $\mathbb{Z}_1, \mathbb{Z}_2, \mathbb{Z}_3 \dots$, and \mathbb{Z} (all with respect to addition).*

Theorem 1.2.4 (Principal theorem on finite abelian groups) *Every finite abelian group is isomorphic to the direct product of groups of the type \mathbb{Z}_{p^k} (p prime).*

By rearranging the direct factors properly this principal theorem can be written in a different form.

Definition 1.2.8 *Let G be a finite abelian group $\neq \{e\}$. Then there are natural numbers s, d_1, d_2, \dots, d_s with $d_1 > 1$ and $d_i | d_{i+1}$ for $1 \leq i < s$ such that*

$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \dots \times \mathbb{Z}_{d_s}.$$

*These numbers are uniquely determined by G and are called the **elementary divisors** of G .*

1.3 Rings theory

1.3.1 Ring

Definition 1.3.1 A **ring** $(R, +, \cdot)$ is a set R , together with two binary operations $+$ and \cdot on R satisfying the following axioms

- a. $(R, +)$ is an abelian group.
- b. For any elements $a, b, c \in R$,
 - (i) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. (Associativity of multiplication)
 - (ii) there exists $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$. (Existence of multiplicative identity)
 - (iii) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$. (Distributivity)
- The identity element in $(R, +)$ will be denoted by 0 and called **zero of the ring**.
- If the operation \cdot is commutative, the ring $(R, +, \cdot)$ is called a **commutative ring**.
- If there is no confusion about the operations, we write only R for the ring $(R, +, \cdot)$.
- A ring is called an **integral domain** if it is a commutative ring with nonzero identity in which $ab = 0$ implies $a = 0$ or $b = 0$.
- A ring is called a **division ring** (or skew field) if the nonzero elements of R form a group under \cdot .

Example 1.3.1

1. The integers under the usual addition and multiplication satisfy all of the axioms above, so that $(\mathbb{Z}, +, \cdot)$ is a commutative ring. Also, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, and $(\mathbb{C}, +, \cdot)$ are all commutative rings.
2. The set of all $n \times n$ square matrices with real coefficients forms a ring $(M_n(\mathbb{R}), +, \cdot)$, which is not commutative if $n \geq 1$, because matrix multiplication is not commutative.

3. Show that $(\mathbb{Z}_n, +, \cdot)$ is a commutative ring, where addition and multiplication defined by the equation

$$\overline{a} + \overline{b} = \overline{a + b} \quad \text{and} \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

When the context is clear and no confusion can arise when talking about elements of \mathbb{Z}_n we will eliminate the overline bars.

Subring

Definition 1.3.2 If $(R, +, \cdot)$ is a ring, a nonempty subset S of R is called a subring of R if S itself a ring with respect to the operations on R .

Example 1.3.2 \mathbb{Z} and \mathbb{Q} are subrings of \mathbb{R} .

1.3.2 Polynomial ring

Definition 1.3.3 If R is a commutative ring, a polynomial $P(X)$ in the indeterminate X over the ring R is an expression of the form

$$P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n.$$

Where $a_0, a_1, a_2, \dots, a_n \in R$ and $n \in \mathbb{N}$. The element a_i is called the coefficient of X^i in $P(X)$.

- If n is the largest integer for which $a_n \neq 0$, we say that $P(X)$ has **degree** n and write $\deg P(X) = n$.
- If all the coefficients of $P(X)$ are zero, then $P(X)$ is called the **zero polynomial**, and its degree is not defined.
- The zero polynomial and the polynomials of degree 0 are called **constant polynomials** because they contain no X terms.

- The set of all polynomials in X with coefficients from the commutative ring R is denoted by $R[X]$. That is,

$$R[X] = \{a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \mid a_i \in R, n \in \mathbb{N}\}.$$

This forms a ring $(R[X], +, \cdot)$ called a polynomial ring with coefficients from R when addition and multiplication of the polynomials

$$P(X) = \sum_{i=0}^n a_i X^i \text{ and } Q(X) = \sum_{i=0}^m b_i X^i$$

are defined by

$$P(X) + Q(X) = \sum_{i=0}^{\max(m,n)} (a_i + b_i) X^i$$

and

$$P(X) \cdot Q(X) = \sum_{k=0}^{m+n} c_k X^k \text{ where } c_k = \sum_{i+j=k}^m a_i b_j.$$

It is easy to verify that $(R[X], +, \cdot)$ satisfies all the axioms for a commutative ring. The zero is the zero polynomial, and the multiplicative identity is the constant polynomial 1.

Remark 1.3.1 The set $R[X_1][X_2]$ is the ring of polynomials in the indeterminates X_1 and X_2 over the ring R and we can write $R[X_1][X_2] = R[X_1, X_2]$. Similarly, $R[X_1, X_2, \dots, X_n]$ where $n \in \mathbb{N}^*$, is the ring of polynomials with indeterminates X_1, X_2, \dots, X_n .

1.3.3 Ring morphism

A morphism (or homomorphism) between two rings is a function between their underlying sets that preserves the two operations of addition and multiplication and also the element 1.

Definition 1.3.4 Let $(R, +, \cdot)$ and $(S, \circ, *)$ be two rings. The function $f : R \longrightarrow S$ is called a ring morphism if for all $a, b \in R$

(i) $f(a + b) = f(a) \circ f(b)$.

(ii) $f(a \cdot b) = f(a) * f(b)$.

(iii) $f(1_R) = 1_S$. Where 1_R and 1_S are respectively the identities of R and S .

- A **ring isomorphism** is a bijective ring morphism. If there is a ring isomorphism between the rings R and S , we say R and S are **isomorphic rings** and we write $R \cong S$.

Example 1.3.3 Let R be a commutative ring and let $m \in \mathbb{Z}$. Then

$$\begin{aligned} f : R &\longrightarrow R \\ x &\longmapsto mx \end{aligned}$$

is a ring morphism.

1.4 Fields

Definition 1.4.1 A field is a nonempty set F with two operations ‘+’ (called addition) and ‘ \cdot ’ (called multiplication) satisfying the following conditions:

- $(F, +, \cdot)$ is a commutative ring.
- If $a \in F$, and $a \neq 0$, there exists $b \in F$ such that $a \cdot b = b \cdot a = 1$. (The element b is called the multiplicative inverse of a).

Example 1.4.1

1. The rings \mathbb{Q} , \mathbb{R} , \mathbb{C} are all fields but the ring \mathbb{Z} is not a field.
2. The ring $R[X]$ is not a field.
3. The ring \mathbb{Z}_p is a field for any prime p .

Proposition 1.4.1 Every field F is an integral domain.

Definition 1.4.2 A subset S of a field F is a subfield of F if S is itself a field with respect to the operations on F .

- If also $S \neq F$, then $(S, +, \cdot)$ is called a **proper** subfield of F .
- A field F is called a **prime field** if it has no proper subfields.

Example 1.4.2 \mathbb{Q} and \mathbb{R} are subfields of \mathbb{C} .

Definition 1.4.3 Let E and F be fields. A morphism, (resp. an isomorphism) of fields is a ring morphism (resp. isomorphism) between E and F .

1.4.1 The field characteristic

For a ring R , an integer $n \geq 1$ and $a \in R$, we denote by na or $n \cdot a$ the element

$$\sum_{i=1}^n a = a + a + \cdots + a.$$

Definition 1.4.4 Let F be a field. **The characteristic** of F denoted by $\text{char}(F)$ is the least positive integer p such that $p \cdot 1 = 0$, where 1 is the multiplicative identity of F . If no such p exists, we define the characteristic to be 0 .

Example 1.4.3

1. The characteristics of \mathbb{Q} , \mathbb{R} , \mathbb{C} are 0 .
2. The characteristic of the field \mathbb{Z}_p is p for any prime p .

It follows from the following result that the characteristic of a field cannot be composite.

Theorem 1.4.1 The characteristic of a field is either 0 or a prime number.

Proof. It is clear that 1 is not the characteristic as $1 \cdot 1 = 1 \neq 0$.

Let p be the characteristic of a field F .

Suppose that p is composite, then $p = nm$ for some positive integers $1 < n, m < p$.

Since $\text{char}(F) = p$, then $p \cdot 1 = 0$.

This implies that $(mn) \cdot 1 = 0$. Hence, $(m \cdot 1)(n \cdot 1) = 0$.

Therefore $m \cdot 1 = 0$ or $n \cdot 1 = 0$, which means that $\text{char}(F) = m$ or $\text{char}(F) = n$. This contradicts the definition of the characteristic. ■

Remark 1.4.1 *Let F be a field such that $\text{char}(F) = p$. Then $p \cdot x = 0$ for any element $x \in F$.*

Lemma 1.4.1 (*Freshman's Dream*) *Let p be prime and F is a field of characteristic p . Then*

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}.$$

for all positive integers n .

1.4.2 Field Extensions

Definition 1.4.5 *Let F and K be fields, we say that K is an extension of F if $F \subseteq K$, and we write $K|F$.*

- *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 1.4.4 $\mathbb{C}|\mathbb{R}$ is a finite extension and $\mathbb{C}|\mathbb{Q}$ is infinite extension.

Definition 1.4.6 *An element α lying in some extension field of a field F is called a **root** (or a **zero**) of $g \in F[x]$ if $g(\alpha) = 0$.*

Definition 1.4.7 *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 1.4.8 *An extension K of a field F is called **algebraic** if each element of K is algebraic over F .*

Definition 1.4.9 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 $K[x]$, that is if there exist elements $\alpha_1, \alpha_2, \dots, \alpha_n \in K$ such that

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

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

Definition 1.4.10 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 1.4.11 A field \bar{F} is called an **algebraic closure** of a field F , if F is algebraically closed and is an algebraic extension of F .

1.4.3 Finite fields

Definition 1.4.12 A finite field is a field has a finite number of elements, this number is called the **order** of the field.

- A finite field of q elements is denoted by \mathbb{F}_q or $GF(q)$ (Galois field of order q).
- \mathbb{Z}_p is a finite field for any prime p and it is isomorphic to the field \mathbb{F}_p .
- Every finite field F of a prime characteristic p is an extension of the field \mathbb{F}_p ($\cong \mathbb{Z}_p$).

Example 1.4.6 $\mathbb{Z}_2 = \{0, 1\}$ and $\mathbb{Z}_3 = \{0, 1, 2\}$ are finite fields, the operations on these fields are described by the tables below.

			$+$	$\begin{array}{c cc} 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 2 \end{array}$				\cdot	$\begin{array}{c cc} 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$			
$\mathbb{Z}_2 :$					$\mathbb{Z}_3 :$							
						$+$	$\begin{array}{c ccc} 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \end{array}$			\cdot	$\begin{array}{c ccc} 0 & 1 & 2 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 \\ 2 & 0 & 2 & 1 \end{array}$	

Proposition 1.4.2 the characteristic of a finite field is a prime number.

Theorem 1.4.2 *Let \mathbb{F}_q be a finite field of characteristic p . Then \mathbb{F}_q contains p^n elements, where $n = [\mathbb{F}_q : \mathbb{F}_p]$.*

For the proof we refer to any textbook of abstract algebra (e.g. see [22]).

Theorem 1.4.3 *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.*

This result can be proved using the uniqueness of the splitting field of $X^q - X$ in the algebraic closure of \mathbb{F}_p (see [22]).

Remark 1.4.2 *Finite field of order 2^n are called binary field or characteristic two finite field.*

Theorem 1.4.4 *Let \mathbb{F}_q be a finite field with q elements.*

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

Definition 1.4.13 *A generator of the cyclic group of a finite field \mathbb{F}_q is called a **primitive element**.*

Theorem 1.4.5 *Let a be a primitive element for the finite field \mathbb{F}_q . then*

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

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

Throughout the later chapters when we write \mathbb{F}_q , we always mean a finite field of characteristic p .

1.4.4 The discrete logarithm problem

Generally the discrete logarithm problem is defined over any cyclic group, but in this section we will define it over \mathbb{F}_p^* as a particular case.

Definition 1.4.14 *Let g be a primitive root in \mathbb{F}_p and let h be a nonzero element of \mathbb{F}_p . The discrete logarithm problem (DLP) is the problem of finding an exponent x such that*

$$g^x \equiv h \pmod{p}.$$

The number x is called the discrete logarithm of h to the base g and is denoted by $\log_g(h)$.

Example 1.4.7

- Since $2^5 \equiv 5 \pmod{11}$. Then $\log_2(5) = 5$.
- Since $2^8 \equiv 3 \pmod{11}$. $\log_2(3) = 8$.

Remark 1.4.3 *An older term for the discrete logarithm is the **index**, denoted by $\text{ind}_g(h)$. The index terminology is still commonly used in number theory. It is also convenient if there is danger of confusion between ordinary logarithms and discrete logarithms.*

Theorem 1.4.6 *For any $a, b \in \mathbb{F}_p^*$ each of the following holds.*

- (i) $\log_g(ab) \equiv \log_g(a) + \log_g(b) \pmod{p}$.
- (ii) For any $t \in \mathbb{N}$, $\log_g(a^t) \equiv t \cdot \log_g(a) \pmod{p}$.
- (iii) $\log_g(1) = 0$.
- (iv) $\log_g(g) = 1$.

Proof. Let $\log_g(a) = x$, $\log_g(b) = y$, $\log_g(ab) = z$.

- (i) Since $g^x \equiv a \pmod{p}$, $g^y \equiv b \pmod{p}$ and $g^z \equiv ab \pmod{p}$, then

$$g^{x+y} \equiv ab \pmod{p}.$$

Therefore, $\log_g(ab) = x + y = \log_g(a) + \log_g(b)$.

(ii) Since $g^x \equiv a \pmod{p}$, then $g^{tx} \equiv a^t \pmod{p}$.

Therefore, $\log_g(a^t) = tx$. i.e., $\log_g(a^t) = t \cdot \log_g(a)$.

(iii) If $\log_g(1) = \omega$, then $g^\omega \equiv 1 \pmod{p}$.

Since g is a primitive element of \mathbb{F}_p , and $0 \leq \omega < p$, then $\omega = 0$.

(iv) Let $\log_g(g) = v$, so $g^v \equiv g \pmod{p}$.

Since g is a primitive root of \mathbb{F}_p , then $v = 1$.

■

Remark 1.4.4

- If there is one solution of the DLP, then there are infinitely many. In other words, if x_0 is a solution of $g^x = h$, then $x_0 + k(p-1)$ is also a solution for every value of k . Because Let x_0 be a solution of $g^x = h$. Then, Fermat's little theorem tell us that $g^{p-1} \equiv 1 \pmod{p}$. Therefore, $g^{x_0+k(p-1)} = g^{x_0} \cdot (g^{p-1})^k \equiv h \cdot 1^k \equiv h \pmod{p}$.
- $\log_g(h)$ is defined only up to adding or subtracting multiples of $p-1$. In other words, is really defined modulo $p-1$.
- The discrete logarithm \log_g is a group isomorphism from \mathbb{F}_p^* to \mathbb{Z}_{p-1} .

$$\begin{aligned} \log_g : \mathbb{F}_p^* &\longrightarrow \mathbb{Z}_{p-1} \\ g^x &\longmapsto \bar{x} \end{aligned}$$

Remark 1.4.5 There are some methods to solve the discrete logarithm problem over an arbitrary groups as baby step–giant step method (for example we will describe it in chapter 3 over the group of an elliptic curve) and Pollard's ρ method. For details see [5], [18].

Chapter 2

Introduction to elliptic curves

In this chapter, we begin with some concepts in algebraic geometry, then we present our topic elliptic curves.

Throughout this chapter, Let K be a field and \overline{K} an algebraic closure of K .

2.1 Weierstrass equation

Definition 2.1.1 *A Weierstrass equation is an equation of the form*

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

where $a_1, a_2, a_3, a_4, a_6 \in K$.

Also we define the quantities

$$\begin{aligned} d_2 &= a_1^2 + 4a_2 \\ d_4 &= 2a_4 + a_1a_3 \\ d_6 &= a_3^2 + 4a_6 \\ d_8 &= a_1a_6 + a_2a_6 - a_1a_3a_4 + a_2a_3 - a_4^2 \\ \Delta &= -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6. \end{aligned}$$

The quantity Δ is called the **discriminant** of the Weierstrass equation and it is the discriminant of the cubic polynomial $x^3 + a_2x^2 + a_4x + a_6$.

- If $\text{char}(K) \neq 2$, then the Weierstrass equation can be written as follows

$$y_1^2 = x^3 + b_2x^2 + b_4x + b_6, \quad (2.2)$$

where

$$y_1 = y + \frac{a_1}{2}x + \frac{a_3}{2},$$

and

$$b_2 = \frac{a_2}{4} + a_1^2, \quad b_4 = \frac{a_2a_3}{2} + a_4, \quad b_6 = \frac{a_3^2}{4} + a_6.$$

- If $\text{char}(K) \neq 3$, then we can also write the equation

$$y_1^2 = x^3 + b_2x^2 + b_4x + b_6,$$

as follows

$$y_1^2 = x_1^3 + Ax_1^2 + Bx_1, \quad (2.3)$$

where $x_1 = (x + \frac{b_2}{3})$ and some constants A and B .

- The discriminant of the Weierstrass equation (2.3) is $\Delta = -16(4A^3 + 27B^2)$.
- The equation (2.1) is called the **generalized Weierstrass equation** and the equation (2.3) is called the **standard Weierstrass equation**.

Remark 2.1.1 There are other forms of equations that can be transformed to Weierstrass equation. For example:

Let be the equation defined over K as follows

$$cy^2 = dx^3 + ax + b$$

with $c, d \neq 0$. Multiply both sides by c^3d^2 to obtain

$$(c^2dy)^2 = (cdx)^3 + (ac^2d)(cdx) + (bc^3d^2).$$

The change of variables

$$y_1 = c^2 dy, \quad x_1 = c dx$$

yields an equation in Weierstrass form.

2.2 Affine plane curves

In this section we introduce basic definitions and notations related to affine curves .

Definition 2.2.1 *The set K^n is called the n -affine space over K and denoted by $\mathbb{A}^n(K)$ or simply \mathbb{A}^n and we write*

$$\mathbb{A}^n(K) = \{(x_1, \dots, x_n) \mid x_1, \dots, x_n \in K\}.$$

- *If $n = 2$, then the affine space is called affine plane.*
- *If $n = 1$, then the affine space is called affine line.*

Definition 2.2.2 *An affine plane algebraic curve C over K is the set of roots in \overline{K} of a non-constant polynomial $f(x, y) \in \overline{K}[x, y]$.*

The set

$$C(K) = \{(x, y) \in \mathbb{A}^2(K) : f(x, y) = 0\}.$$

is called the set of K -rational points of C .

- *When we write C/K we mean that a curve C defined over K .*
- *The **degree** (or the order) of a plane curve C is the degree of the polynomial associated with C .*
- *A plane curve of degree 1, 2, 3, 4, 5, 6 is called a line, quadric, cubic, quartic, quintic, sextic respectively.*

Example 2.2.1 *$C : x^2 + y^2 = 1$ is an affine plane curves over \mathbb{R} . The set of \mathbb{R} -rational points of C is a circle of center $(0, 0)$ and radius 1.*

Throughout this memory, by the word plane curve we always mean plane algebraic curve.

Definition 2.2.3 Let $C : f(x, y) = 0$, be a curve and $P = (x_0, y_0)$ a point on C . Then P is **singular** on C if $\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$. Otherwise The point P is called **nonsingular**.

- A singular curve is a curve with at least one singular point.
- If the curve C has no singular point, then it is called a **nonsingular** (or **smooth**) curve.

Example 2.2.2 Let $C_1 : y^2 = x^3 + x$ and $C_2 : y^2 = x^3 + x^2$ are two curves over \mathbb{R} .

The curve C_1 is nonsingular curve but the curve C_2 is singular at the point $P = (0, 0)$.

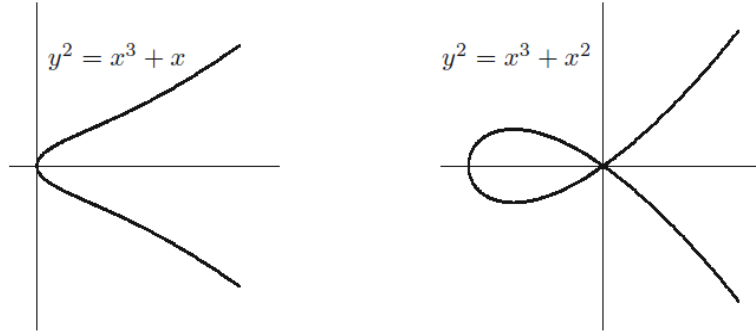


Figure 2.1 A nonsingular and singular curves.

Remark 2.2.1 the curve being nonsingular or smooth means that there is a unique tangent line at each point on the curve.

Proposition 2.2.1 The curve given by a Weierstrass equation is nonsingular if and only if $\Delta \neq 0$.

Lemma 2.2.1 The intersection (resp. the union) of two curves over K is also a curve over K .

The next result gives the precise number of intersection points of two plane curves C and C' .

Theorem 2.2.1 (*Bezout's theorem*) *Let C and C' be plane curves of degree m and n respectively then the number of points of intersection of C and C' is mn .*

For the proof of the theorem we refer to any textbook in algebraic geometry.

2.3 Projective plane curves

Generally, Bezout's theorem is not true in the actual affine setting, because two parallel lines do not intersect at all. So we have to add extra points (which are called points at infinity) for each parallel class of lines to make Bezout's theorem work. The resulting object is called the projective plane space.

Definition 2.3.1 *The projective plane space over K denoted by $\mathbb{P}^2(K)$ is the set of equivalence classes of $K^3 \setminus \{(0, 0, 0)\}$ under the equivalence relation*

$$(x, y, z) \sim (x', y', z') \iff \exists \lambda \in K^* : (x, y, z) = \lambda(x', y', z').$$

- The set of equivalence class of (x, y, z) is devoted by $(x : y : z)$ and write

$$(x : y : z) = \{\lambda(x', y', z') \mid (x', y', z') \in K^3 \setminus \{(0, 0, 0)\}, \lambda \in K^*\}.$$

Therefore

$$\mathbb{P}^2(K) = \{(x : y : z) \mid (x, y, z) \in K^3\}.$$

- The triple (x, y, z) is called homogeneous coordinates for the corresponding point in $\mathbb{P}^2(K)$, (the homogeneous coordinates are not unique for example $(1, 1, 1)$, $(2, 2, 2)$, (π, π, π) are all homogeneous coordinates to the same point $P \in \mathbb{P}^2(\mathbb{R})$).
- Notice that if $(x', y', z') \in (x : y : z)$ then $(x : y : z) = (x' : y' : z')$; that is, any element of an equivalence class can serve as its representative.

- If $(x : y : z)$ is a point with $z = 0$, then $(x : y : z) = (\frac{x}{z} : \frac{y}{z} : 1)$. These are the “finite” points in $\mathbb{P}^2(K)$. However, if $z = 0$ then dividing by z should be thought of as giving ∞ in either the x or y coordinate, and therefore the points $(x : y : 0)$ are called the “**points at infinity**” in $\mathbb{P}^2(K)$. (The point at infinity on an elliptic curve will soon be identified with one of these points at infinity in $\mathbb{P}^2(K)$).
- The point at infinity (or infinity point) is generally denoted by ∞ , \mathcal{O} or I .
- The set of all points at infinity is called the **line at infinity**.

Proposition 2.3.1 *The map*

$$\begin{aligned} \Psi : \mathbb{A}^2(K) &\longrightarrow \mathbb{P}^2(K) \\ (x, y) &\longmapsto (x : y : 1) \end{aligned}$$

is one-to-one and the complement of the image of Ψ is the line at infinity.

- the projective plane space is the set

$$\mathbb{P}^2(K) = \mathbb{A}^2(K) \cup \{\text{the set of points at infinity}\}.$$

Definition 2.3.2 *A polynomial $F \in K[X, Y, Z]$ is called **homogeneous** of degree d if*

$$F(\lambda x, \lambda y, \lambda z) = \lambda^d F(x, y, z) \quad \text{for all } \lambda \in K.$$

- If F is homogeneous of some degree, and $(x, y, z) \sim (x', y', z')$, then

$$F(x, y, z) = 0 \quad \text{if and only if} \quad F(x', y', z') = 0.$$

Therefore, a zero of F in $\mathbb{P}^2(K)$ does not depend on the choice of representative for the equivalence class, so the set of zeros of F in $\mathbb{P}^2(K)$ is well defined.

Example 2.3.1 *Let $F(x, y, z) = x^2 + 2y - 3z$. Then $F(1, 1, 1) = 0$, so we might be tempted to say that F vanishes at $(1 : 1 : 1)$. But $F(2, 2, 2) = 2$ and $(1 : 1 : 1) = (2 : 2 : 2)$. To avoid this problem, we need to work with homogeneous polynomials.*

- A polynomial $f(x, y) \in K[x, y]$ of total degree d can be homogenised by defining

$$F(x, y, z) = z^d f\left(\frac{x}{z}, \frac{y}{z}\right) \in K[x, y, z].$$

- A homogeneous polynomial $F(X, Y, Z) \in K[x, y, z]$ can be dehomogenised by defining

$$f(x, y) = F(x, y, 1) \in K[x, y].$$

Example 2.3.2 If $f(x, y) = y^2 - x^3 - Ax - B$, with $d = \deg f(x, y) = 3$, then we obtain the homogeneous polynomial $F(x, y, z) = y^2z - x^3 - Axz^2 - Bz^3$.

Definition 2.3.3 A plane projective algebraic curve over K is the set of roots in \overline{K} of a non-constant homogeneous polynomial $F(x, y, z) \in K[x, y, z]$.

We define

$$C(K) = \{(x : y : z) \in \mathbb{P}^2(K) : F(x, y, z) = 0\}$$

the set of K -rational points of C . A point at infinity of this curve is a point $P = (x : y : z) \in C$ with $z = 0$.

- We can now see that two parallel lines meet at a point at infinity.

Let

$$y = mx + b_1, \quad y = mx + b_2$$

be two nonvertical parallel lines with $b_1 \neq b_2$. They have the homogeneous forms

$$y = mx + b_1z, \quad y = mx + b_2z.$$

When we solve the simultaneous equations to find their intersection, we obtain

$$z = 0 \quad \text{and} \quad y = mx.$$

Since we cannot have all of x, y, z being 0, we must have $x \neq 0$. Therefore, we can rescale by dividing by x and find that the intersection of the two lines is

$$(x : mx : 0) = (1 : m : 0).$$

Similarly, if $x = c_1$ and $x = c_2$ are two vertical lines, they intersect in the point $(0 : 1 : 0)$. This is one of the points at infinity in $\mathbb{P}^2(K)$.

- Now let's look at the curve E given by the Weierstrass equation

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

Its homogeneous form is

$$y^2z = x^3 + Axz^2 + Bz^3.$$

The points (x, y) on the affine curve correspond to the points $(x : y : 1)$ in the projective version.

To see what points on lie at infinity, set $z = 0$ and obtain $0 = x^3$.

Therefore $x = 0$, and y can be any nonzero number (recall that $(0 : 0 : 0)$ is not allowed).

Rescale by y to find that $(0 : y : 0) = (0 : 1 : 0)$ is the only point at infinity on E . As we saw above, $(0 : 1 : 0)$ lies on every vertical line, so every vertical line intersects E at this point at infinity.

In this memory we almost always work in affine (nonprojective) coordinates and treat the point at infinity as a special case when needed.

2.4 Elliptic curves

In this section we present the main of our study, elliptic curves, which are cubic plane curves.

Definition 2.4.1 *An elliptic curve E over K is a nonsingular plane curve given by a Weierstrass equation*

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

with a point at infinity \mathcal{O} .

The set of K -rational points of E is given as the following

$$E(K) = \{(x, y) \in K^2 \mid y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{\mathcal{O}\}.$$

- *If $\text{char}(K) \neq 2, 3$ we can define the elliptic curve by the equation (2.3) with the condition $4A^3 + 27B^2 \neq 0$. So*

$$E(K) = \{(x, y) \in K^2 \mid y^2 - x^3 - Ax^2 - Bx = 0, 4A^3 + 27B^2 \neq 0\} \cup \{\mathcal{O}\}.$$

- *The condition $4A^3 + 27B^2 \neq 0$, ensures that the elliptic curve E is nonsingular by proposition 2.1.1.*

Remark 2.4.1

- *Elliptic curves are not ellipses. The terminology stems historically from the fact that in the 1700s, the problem of finding arclength on an ellipse led, via “elliptic integrals,” into the realm of these cubic equations.*
- *Note that the term rational does not refer to the rational field \mathbb{Q} . Elliptic curves over \mathbb{Q} are often referred to as rational elliptic curves.*

Example 2.4.1 *The Figure 2.1 shows the graphs of set of points of elliptic curves over the real numbers.*

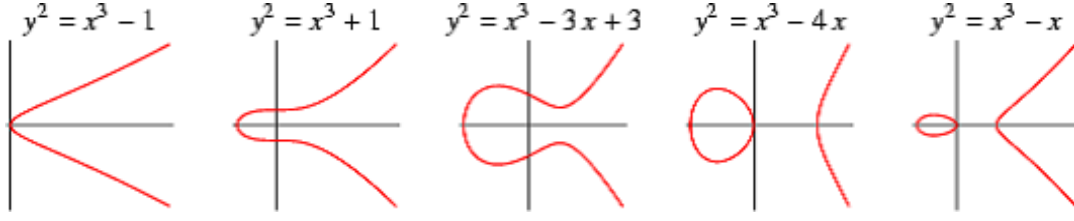


Figure 2.2

We see that these graphs are symmetric graphs around the x -axis.

Proposition 2.4.1 *Let E be an elliptic curve over K . The point at infinity is nonsingular point of E .*

Proof. Let E be given by the Weierstrass equation

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

We look at the curve in $\mathbb{P}^2(K)$ with homogeneous equation

$$F(x, y, z) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3 = 0$$

and at the point $\mathcal{O} = (0 : 1 : 0)$. Since

$$\frac{\partial F}{\partial z}(\mathcal{O}) = 1 \neq 0,$$

we see that \mathcal{O} is a nonsingular point of E . ■

2.4.1 j -invariant and Isomorphisms

Definition 2.4.2 *Let E be an elliptic curve given by the Weierstrass equation*

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

with the quantities

$$\begin{aligned}
 d_2 &= a_1^2 + 4a_2 \\
 d_4 &= 2a_4 + a_1a_3 \\
 d_6 &= a_3^2 + 4a_6 \\
 d_8 &= a_1a_6 + a_2a_6 - a_1a_3a_4 + a_2a_3 - a_4^2 \\
 c_4 &= d_2^2 - 24d_4 \\
 \Delta &= -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6 \\
 j(E) &= c_4^3/\Delta.
 \end{aligned}$$

The quantity $j(E)$ is called the j -**invariant** of E .

- If the elliptic curve is defined by the equation (2.3), the j -invariant of E is

$$j(E) = -1728 \frac{(4A)^3}{\Delta}.$$

- There are two special values of j that arise quite often:

1. $j = 0$: In this case, the elliptic curve E has the form $y^2 = x^3 + B$.
2. $j = 1728$: In this case, the elliptic curve E has the form $y^2 = x^3 + Ax$.

Definition 2.4.3 Two elliptic curves defined by Weierstrass equations

$$\begin{aligned}
 E &: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \\
 E' &: y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6
 \end{aligned}$$

are isomorphic over K , denoted $E/K \cong E'/K$, if there exist constants $r, s, t \in K$ and $u \in K^*$, such that the change of variables

$$(x, y) \longmapsto (u^2x + r, u^3y + su^2x + t) \tag{I}$$

transforms equation E to equation E' . This change of variables is referred to as an *admissible change of variables*.

- If $E = E'$, such a transformation is called an *automorphism* of E .

- the change of variables (I) transforms equation E to equation E' , then the change of variables

$$(x, y) \mapsto (u^{-1}(x - r), u^{-3}(y + sx - t + rs)) \quad (II)$$

transforms equation E' to equation E and it is also an admissible change of variables.

Example 2.4.2 Let E/K be an elliptic curve given by the Weierstrass equation (2.1). If $\text{char}(K) \neq 2$, then the admissible change of variables

$$(x, y) \mapsto \left(x, y + \frac{a_1}{2}x + \frac{a_3}{2}\right),$$

transforms E/K to the curve given by the equation (2.2).

Curves isomorphism is an equivalence relation. The following theorem establishes the fact that, over the algebraic closure K , the j -invariant characterizes the equivalence classes in this relation.

Theorem 2.4.1 Two elliptic curves that are isomorphic over K have the same j -invariant. Conversely, two curves with the same j -invariant are isomorphic over \overline{K} .

2.4.2 Group law

The amazing feature of elliptic curves is that we can define a group structure over the points of elliptic curves. In this section we give the addition law⁽¹⁾ of this group.

We use the following application of Bézout's theorem:

Theorem 2.4.2 A line intersects an elliptic curve in exactly three points.

Proof. For the proof see [24]. ■

⁽¹⁾Note that the choice of naming the operation “addition” is completely arbitrary; we could have also called it multiplication.

Definition 2.4.4 Let E be an elliptic curve over K and $P, Q \in E$ be two (not necessary distinct) points. The line through P and Q intersects the elliptic curve in a third point R' . We consider the L' line through R' and \mathcal{O} , this line intersects the curve in a third point R . We define

$$P + Q = R.$$

- If $P = Q$, one has to take the tangent line at E in P .
- If the line throughout P and Q is a vertical line, then we define $P + Q = \mathcal{O}$.

Theorem 2.4.3 Let E be an elliptic curve over K . The set of points of E is an additive abelian group under the addition defined above, with the point at infinity \mathcal{O} as identity element. So the addition law has the following properties:

- (a) $P + Q \in E$ for all $P, Q \in E$. (Closure)
- (b) $P + \mathcal{O} = \mathcal{O} + P = P$ for all $P \in E$. (Identity)
- (c) $P + (-P) = \mathcal{O}$ for all $P \in E$. (Inverse)
- (d) $P + Q = Q + P$ for all $P, Q \in E$. (Commutative)
- (e) $(P + Q) + R = P + (Q + R)$ for all $P, Q, R \in E$. (Associative)

Proof.

- (a) The closure property holds by definition and Theorem 2.4.2.
- (b) The identity property of \mathcal{O} holds by definition. Taking $Q = \mathcal{O}$, we see that the lines L and L' coincide. The former intersects E at P, \mathcal{O}, R and the latter at $R, \mathcal{O}, P + \mathcal{O}$, so $P + \mathcal{O} = P$.
- (c) For inverse, Let P' be the third point of intersection of the line through P and \mathcal{O} with the curve. Then $P + P' = \mathcal{O}$, therefore $P' = -P$.
- (d) The commutativity is obvious from the fact that the line through P and Q is the same as the line through Q and P .

- (e) The proof of associativity needs some results from algebraic geometry that we have not mentioned; for this, we will not discuss the proof here. (For details see [18], [24]).

■

The following theorem gives formulae to compute the addition of two points on the elliptic curve.

Theorem 2.4.4 (*Elliptic curves algorithm*). *Let E be an elliptic curve given by the standard Weierstrass equation.*

$$E : Y^2 = X^3 + AX + B$$

and let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be points on E .

- (a) $-P = (x_1, -y_1)$.
- (b) If $x_1 = x_2$ and $y_1 = -y_2$, then $P + Q = \mathcal{O}$.
- (c) Otherwise, define λ by

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\ \frac{3x_1^2 + A}{2y_1} & \text{if } P = Q \end{cases}$$

and let

$$x_3 = \begin{cases} \lambda^2 - x_1 - x_2 & \text{if } P \neq Q \\ \lambda^2 - 2x_1 & \text{if } P = Q \end{cases},$$

$$y_3 = \lambda(x_1 - x_3) - y_1.$$

Then $P + Q = (x_3, y_3)$.

Proof. Let $E : Y^2 = X^3 + AX + B$.

- (a) The line L through $P = (x_1, y_1) \in E(K)$ and \mathcal{O} is $L : x = x_1$.

We compute the intersection point $P' = (x'_1, y'_1)$ of L and E .

Substitute $x = x_1$ in the equation of E , we get $y^2 = x_1^3 + Ax_1 + B$.

Since $P = (x_1, y_1) \in E(K)$, then $y_1^2 = x_1^3 + Ax_1 + B$.

Therefore, $y^2 = y_1^2$. Then, $y = y_1$ or $y = -y_1$.

Then, $y'_1 = -y_1$.

The third intersection point of L with E is therefore $P' = (x_1, -y_1)$.

With Theorem 1.2.2, this point P' is equal to $-P$.

(b) follows from (a).

(c) Let $P = (x_1, y_1)$, $Q = (x_2, y_2)$ are two points on an elliptic curve E . The third intersection point of the line L with E is a point $R = (x_3, y_3)$ (by assumption $R \neq \mathcal{O}$). We now compute this intersection point:

1. Assume first that $x_1 \neq x_2$ and $y_1 \neq y_2$.

Let the line connecting P to Q be

$$L : y = \lambda x + \nu.$$

Its slope is

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

then the equation of L is

$$y = \lambda(x - x_1) + y_1.$$

To find the intersection with E , substitute to get

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

This can be rearranged to the form

$$0 = x^3 - \lambda^2 x^2 + \dots.$$

We already know that x_1 and x_2 are solutions, so we can find the third solution x_3 by comparing the two sides of

$$\begin{aligned} x^3 - \lambda^2 x^2 + \dots &= (x - x_1)(x - x_2)(x - x_3) \\ &= x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3. \end{aligned}$$

Therefore,

$$x_1 + x_2 + x_3 = \lambda^2.$$

Then,

$$x_3 = \lambda^2 - x_1 - x_2.$$

By substituting x_3 into the equation of L . This gives

$$y'_3 = \lambda(x_3 - x_1) + y_1.$$

Hence, $R = (x_3, y'_3)$.

Therefore, $P + Q = -R$, where

$$x_3 = \lambda^2 - x_1 - x_2 \text{ and } y_3 = \lambda(x_1 - x_3) - y_1.$$

2. If $P = Q = (x_1, y_1)$, then $P + P = 2P$ represents doubling of point. The line L through P is a tangente line.

If $P = Q = (x_1, y_1)$ and $y_1 = 0$, then the line is vertical and we set $P + Q = \mathcal{O}$. Otherwise, we have:

Implicit differentiation allows us to find the slope λ of L

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

The equation of L is

$$y = \lambda(x - x_1) + y_1,$$

as before, we obtain the cubic equation

$$0 = x^3 - \lambda^2 x^2 + \dots$$

This time, we know only one root, namely x_1 , but it is a double root since L is tangent to E at P . Therefore, proceeding as before, we obtain

$$x_3 = \lambda^2 - 2x_1 \quad \text{and} \quad y_3 = \lambda(x_1 - x_3) - y_1.$$

■

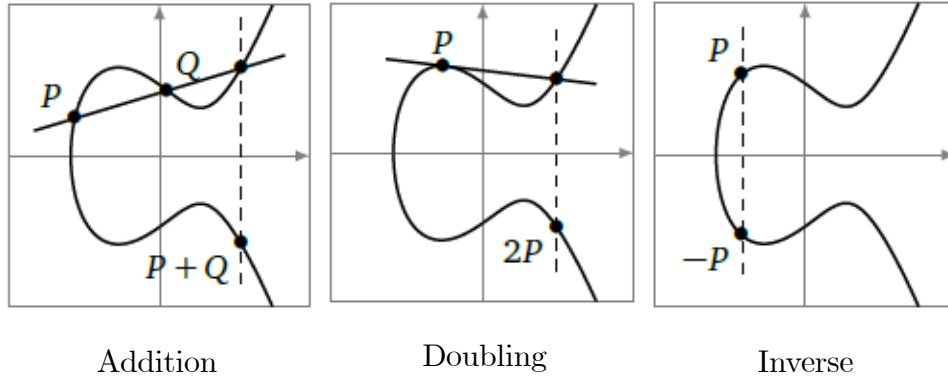


Figure 2.3 Geometric illustration of addition, doubling and inverse of elliptic curve points.

Example 2.4.3 Let the elliptic curve defined over \mathbb{Q} as follows

$$E : y^2 = x^3 + 17.$$

Let $P_1 = (-2, 3)$, $P_2 = (2, 5)$, $P_3 = (4, 9)$, $P_4 = (2, 5)$ are points on E .

Using the addition formulae, one easily can verify that

$$P_2 + P_3 = P_1, \quad P_3 = P_1 - P_4, \quad 2P_1 = (8, -23).$$

Remark 2.4.2 *If we define the elliptic curve by the generalized Weierstrass equation*

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

the addition formulae will be changing as the following:

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q, \\ \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{if } P = Q, \end{cases}$$

and

$$x_3 = \begin{cases} \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 & \text{if } P \neq Q, \\ \lambda^2 + a_1\lambda - a_2 - 2x_1 & \text{if } P = Q, \end{cases}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 - (a_1x_3 + a_3).$$

Also the inverse of P will be changing as $-P = (x_1, -y_1 - a_1x_1 - a_3)$.

- *When the characteristic of the field is 2, if we use the standard Weierstrass equation the curve will be singular, for this we define the elliptic curve by the generalized Weierstrass equation.*

Theorem 2.4.5 *Let E be an elliptic curve over K . The set of K -rational points $E(K)$ is a subgroup of $(E, +)$.*

Proof. Let E be an elliptic curve over K .

- (a) Let P and $Q \in E(K)$. Since P and Q have coordinates in K , then the equation of the line connecting them has coefficients in K . The third point of intersection has coordinates given by a rational combination of the coordinates of coefficients of the line and of E , so will be in K . (See the formulae in the theorem 2.4.4). Therefore $P + Q \in E(K)$.
- (b) $\mathcal{O} \in E(K)$. This holds by definition.

(c) If $P \in E(K)$, then $-P \in E(K)$. This is clear.

■

Definition 2.4.5 Let n be a positive integer and let P be a point on $E(K)$. The point

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

is called *point multiplication* or *scalar multiplication*.

- The order of P is the smallest positive integer n such that $nP = \mathcal{O}$.

Example 2.4.4 We consider the elliptic curve $E : Y^2 = X^2 + 1$, over \mathbb{Q} .

This curve has a \mathbb{Q} -rational point $P = (2, -3)$. We compute

$$2P = (0, -1), \quad 3P = (-1, 0), \quad 4P = (0, 1), \quad 5P = (2, 3), \quad 6P = \mathcal{O}.$$

We thus see that $5P = -P$. The point P is a point of order 6.

Remark 2.4.3 Point multiplication is analog to exponentiation in multiplicative groups. In order to do it efficiently, we can directly adopt the square-and-multiply algorithm. The only difference is that squaring becomes doubling and multiplication becomes addition of P (for example see [15]).

2.4.3 Torsion points

The torsion points have an important role in the study of elliptic curves and they are points of a finite order.

Definition 2.4.6 Let n be a positive integer. A n -torsion point is a point $P \in E(\overline{K})$ satisfying $nP = \mathcal{O}$. The set of n -torsion points denoted by $E[n]$, and write

$$E[n] = \{P \in E(\overline{K}) \mid nP = \mathcal{O}\}.$$

- The set $E[n]$ is a subgroup of $E(\overline{K})$.

- If the field K is finite, all the points of $E(K)$ are torsion points.
- If the field K has characteristic p , the curve E is called **supersingular** if $E[p] = \{\mathcal{O}\}$, otherwise the curve E is called **ordinary**.

Example 2.4.5 Let K be a field such that $\text{char}(K) \neq 2$. Let

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3), \text{ where } e_1, e_2, e_3 \in \overline{K}.$$

A point P satisfies $2P = \mathcal{O}$ if and only if the tangent line at P is vertical. Hence $y = 0$,
so

$$E[2] = \{\mathcal{O}, (e_1, 0), (e_2, 0), (e_3, 0)\}.$$

Remark 2.4.4 Note that saying that P is an n -torsion point does not necessarily mean that P has order n , it means rather that P has order dividing n .

Theorem 2.4.6 Let E be an elliptic curve over K and let n be a positive integer.

If the characteristic of K does not divide n , or is 0, then

$$E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n.$$

If the characteristic of K is $p > 0$ and $p \mid n$, write $n = p^r n'$ with $p \nmid n'$. Then

$$E[n] \cong \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \text{ or } \mathbb{Z}_n \oplus \mathbb{Z}_{n'}.$$

Proof. For the proof see [2]. ■

Example 2.4.6 In the Example 1.3.5 we have $E[2] \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

2.4.4 Elliptic curves over finite fields

An elliptic curve over a finite field has a finite abelian group structure. Applications of such group to cryptography, will be discussed in the later chapter.

Definition 2.4.7 *Let \mathbb{F}_q be a finite field of characteristic p . We define an elliptic curve over \mathbb{F}_q to be an equation of the form*

$$E : y^2 + a_1xy + a_3y \equiv x^3 + a_2x^2 + a_4x + a_6 \pmod{p}$$

with the point at infinity \mathcal{O} , and then we look at the points on E with coordinates in \mathbb{F}_q , which we denote by $E(\mathbb{F}_q)$.

- *The elliptic curve addition algorithm (Theorem 2.4.4) applied to points P and Q in E/\mathbb{F}_q yields a point in E/\mathbb{F}_p . But divisions should be interpreted as multiplications by multiplicative inverses.*
- *Though the formulae above are obtained from a geometrical construction, however these formulae are evaluated using modular arithmetics (congruences) over a finite field, thus loosing their geometric interpretations.*
- *The addition law on E/\mathbb{F}_q satisfies all of the properties listed in Theorem 2.4.3. In other words, this addition law makes E into a **finite abelian group** with \mathcal{O} as an identity element.*

Now let's discuss an example of elliptic curve over a finite field.

Example 2.4.7 *Let E be an elliptic curve over \mathbb{F}_5 given by the equation $y^2 = x^3 + 2x + 1$.*

- *To count points on E , we make a list of the possible values of x , then of $x^3 + 2x + 1 \pmod{5}$, then of the square roots y of $x^3 + 2x + 1 \pmod{5}$. This yields the points on E .*

x	$x^3 + 2x + 1$	y	$points$
0	0	1, 4	$(0, 1), (0, 4)$
1	4	1, 2	$(1, 2), (1, 3)$
2	3	—	—
3	4	2, 3	$(3, 2), (3, 3)$
4	3	—	—
\mathcal{O}	\mathcal{O}	\mathcal{O}	\mathcal{O}

Table 2.1

Therefore, $E(\mathbb{F}_5) = \{\mathcal{O}, (0, 1), (0, 4), (1, 2), (1, 3), (3, 2), (3, 3)\}$.

The addition law is described in the table below .

$+$	\mathcal{O}	$(0, 1)$	$(0, 4)$	$(1, 2)$	$(1, 3)$	$(3, 2)$	$(3, 3)$
\mathcal{O}	\mathcal{O}	$(0, 1)$	$(0, 4)$	$(1, 2)$	$(1, 3)$	$(3, 2)$	$(3, 3)$
$(0, 1)$	$(0, 1)$	$(1, 3)$	\mathcal{O}	$(0, 4)$	$(3, 3)$	$(1, 2)$	$(3, 2)$
$(0, 4)$	$(0, 4)$	\mathcal{O}	$(1, 2)$	$(3, 2)$	$(0, 1)$	$(3, 3)$	$(1, 3)$
$(1, 2)$	$(1, 2)$	$(0, 4)$	$(3, 2)$	$(3, 3)$	\mathcal{O}	$(1, 3)$	$(0, 1)$
$(1, 3)$	$(1, 3)$	$(3, 3)$	$(0, 1)$	\mathcal{O}	$(3, 2)$	$(0, 4)$	$(1, 2)$
$(3, 2)$	$(3, 2)$	$(1, 2)$	$(3, 3)$	$(1, 3)$	$(0, 4)$	$(0, 1)$	\mathcal{O}
$(3, 3)$	$(3, 3)$	$(3, 2)$	$(1, 3)$	$(0, 1)$	$(1, 2)$	\mathcal{O}	$(0, 4)$

Table 2.2 Addition Cayley table of elliptic curve group over \mathbb{F}_5 .

- Let's compute $(1, 2) + (3, 3)$ on $E(\mathbb{F}_5)$.

The slope is

$$\lambda = (3 - 2)(3 - 1)^{-1} \equiv 3 \pmod{5}.$$

Therefore,

$$x_3 = \lambda^2 - x_1 - x_2 \equiv 3^2 - 1 - 3 \equiv 0 \pmod{5}.$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \equiv 3^2(1 - 0) - 2 \equiv 1 \pmod{5}.$$

This means that

$$(1, 2) + (3, 3) = (0, 1).$$

- Let's compute $(0, 1) + (0, 1) = 2(0, 1)$ on $E(\mathbb{F}_5)$.

The slope is

$$\lambda = (3 \cdot 0 + 1)(2 \cdot 1)^{-1} \equiv 1 \pmod{5}.$$

Therefore,

$$x_3 = \lambda^2 - x_1 - x_2 \equiv 1^2 - 0 - 1 \equiv 1 \pmod{5}.$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \equiv 1^2(0 - 1) - 1 \equiv 3 \pmod{5}.$$

This means that

$$2(0, 1) = (1, 3).$$

The Figure 2.2 shows the discrete and finite points of elliptic curve $E : y^2 = x^3 + 2x + 1$ which are defined over \mathbb{F}_5 .

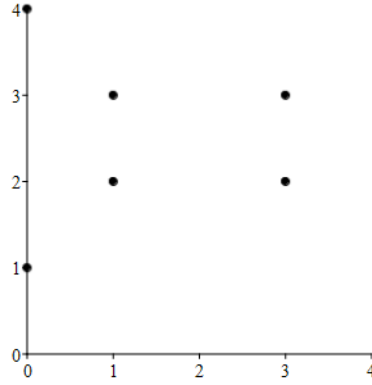


Figure 2.3 Elliptic Curve $E : y^2 = x^3 + 2x + 1$ over \mathbb{F}_5 .

Remark 2.4.5 If $P = (x, y) \in E(\mathbb{F}_p)$, then $-P = (x, p - y)$.

The next theorem shows us that the group of points $E(\mathbb{F}_q)$ is always either a cyclic group or the direct product of two cyclic groups.

Theorem 2.4.7 *Let E be an elliptic curve over the finite field \mathbb{F}_q . Then*

$$E(\mathbb{F}_q) \cong \mathbb{Z}_n \quad \text{or} \quad \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

for some integer $n \geq 1$, or for some integers $n_1, n_2 \geq 1$ with $n_1 | n_2$.

Proof. For the proof see [2], [18]. ■

Example 2.4.8 *Let E be an elliptic curve.*

- *If $E : y^2 = x^3 + 2$ over \mathbb{F}_7 , then*

$$E(\mathbb{F}_7) = \{\mathcal{O}, (0, 3), (0, 4), (3, 1), (3, 6), (5, 1), (5, 6), (6, 1), (6, 6)\}.$$

All of these points P satisfy $3P = \mathcal{O}$.

$$E(\mathbb{F}_7) \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3.$$

- *If $E : y^2 + xy = x^3 + 1$ over \mathbb{F}_2 , then $E(\mathbb{F}_2) = \{\mathcal{O}, (0, 1), (1, 0), (1, 1)\}$.*

$(0, 1); (1, 0)$ have order 4 and $(1, 1)$ has order 2.

$$E(\mathbb{F}_2) \cong \mathbb{Z}_4.$$

Frobenius map

Definition 2.4.8 *The q^{th} -power Frobenius map, on an elliptic curve, E , defined over \mathbb{F}_q , is defined by*

$$\phi : \begin{cases} E(\overline{\mathbb{F}}_q) & \longrightarrow & E(\overline{\mathbb{F}}_q) \\ (x, y) & \longrightarrow & (x^q, y^q) \\ \mathcal{O} & \longrightarrow & \mathcal{O} \end{cases}$$

the map ϕ is a group endomorphism of E over \mathbb{F}_q , referred to as the **Frobenius endomorphism**.

To set up discrete logarithm cryptosystems (see chapter 3) it is important to know the order of the group.

Hass's theorem

Hass's theorem gives bounds for the group of points on an elliptic curve over a finite field.

Theorem 2.4.8 (Hasse) *Let E be an elliptic curve over a finite field \mathbb{F}_q , then the order of $E(\mathbb{F}_q)$ satisfies*

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

Hass's theorem is also known as Hasse's bound. For more details about the proof see [18].

Definition 2.4.9 *The quantity*

$$t = q + 1 - \#E(\mathbb{F}_q),$$

is called the trace of Frobenius for $E(\mathbb{F}_q)$.

Example 2.4.9 *Let E be an elliptic curve over \mathbb{F}_q given by the equation $E : y^2 = x^3 + 4x + 6$. The table below lists the results for the first few primes, together with the value of t and the value $2\sqrt{q}$.*

q	$\#E(\mathbb{F}_q)$	t_q	$2\sqrt{q}$
3	4	0	3.46
5	8	-2	4.47
7	11	-3	5.29
11	16	-4	6.63
13	14	0	7.21
17	15	3	8.25

Table 2.3

2.4.5 Determining the group order

The problem of determining the order of the group of rational points on an elliptic curve over a finite field is of critical importance in applications such as primality proving and cryptography. In this subsection we will give two results for actually determining the order of the group over a finite field.

Subfield Curves

Sometimes we have an elliptic curve E defined over a small finite field \mathbb{F}_q and we want to know the order of $E(\mathbb{F}_q)$ for some n . We can determine the order of $E(\mathbb{F}_{q^n})$ when $n = 1$ by listing the points or by some other elementary procedure. The amazing fact is that this allows us to determine the order for all n .

Theorem 2.4.9 *Let $\#E(\mathbb{F}_q) = q + 1 - t$. Where $t \in \mathbb{N}$ is the trace of Frobenius. Write $X^2 - tX + q = (X - \alpha)(X - \beta)$. Then*

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

for all $n \geq 1$.

The polynomial $X^2 - tX + q$ is often called the **characteristic polynomial of Frobenius**.

Example 2.4.10 In Example 2.4.8, we showed that the elliptic curve E given by $y^2 + xy = x^3 + 1$ over \mathbb{F}_2 satisfies $\#E(\mathbb{F}_2) = 4$. Therefore, $t = 2 + 1 - 4 = -1$, and we obtain the polynomial

$$X^2 + X + 2 = \left(X - \frac{-1 - \sqrt{-7}}{2}\right) \left(X - \frac{-1 + \sqrt{-7}}{2}\right).$$

By the theorem we obtain

$$\#E(\mathbb{F}_4) = 4 + 1 - \left(\frac{-1 - \sqrt{-7}}{2}\right)^2 - \left(\frac{-1 + \sqrt{-7}}{2}\right)^2.$$

Legender symbol

To make a list of points on $y^2 = x^3 + Ax + B$ over a finite field, we tried each possible value of x , then found the square roots y of $x^3 + Ax + B$, if they existed. This procedure is the basis for a simple point counting algorithm. Recall the **Legendre symbol** $\left(\frac{x}{p}\right)$ for an odd prime p , which is defined as follows:

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

This can be generalized to any finite field \mathbb{F}_q with q odd by defining, for $x \in \mathbb{F}_q$,

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

Theorem 2.4.10 *Let E be an elliptic curve defined by $y^2 = x^3 + Ax + B$ over \mathbb{F}_q .*

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

Example 2.4.11 *Let E be the curve $y^2 = x^3 + 3x - 1$ over \mathbb{F}_7 , where*

$$E(\mathbb{F}_7) = \{\mathcal{O}, (3, 0), (6, 3), (6, 4)\}.$$

The only nonzero square mod 7 is 2. Therefore,

$$\begin{aligned} \#E(\mathbb{F}_7) &= 7 + 1 + \sum_{x=0}^6 \left(\frac{x^3 + 3x - 1}{\mathbb{F}_7} \right) \\ &= 8 + \left(\frac{6}{7}\right) + \left(\frac{3}{7}\right) + \left(\frac{6}{7}\right) + \left(\frac{0}{7}\right) + \left(\frac{5}{7}\right) + \left(\frac{6}{7}\right) + \left(\frac{2}{7}\right) \\ &= 8 - 1 - 1 - 1 - 1 - 1 + 1 = 4. \end{aligned}$$

Remark 2.4.6 *We can use Maple program to do some computations on elliptic curves. (For details see [17]).*

Chapter 3

Cryptosystems based on elliptic curves

In this chapter we begin with an introduction to private and public key cryptography, then proceed to present elliptic curve cryptosystems.

3.1 Private and Public key cryptosystems

The fundamental goal of cryptography has historically been to achieve privacy, i.e., to enable two people, Alice and Bob, to send each other messages over an insecure channel (e.g. a telephone line or computer network) in such a way that only the intended recipient can read the message which means that an eavesdropper, Eve, can not read their messages.

Alice wants to send a message, often called the **plaintext**, to Bob. In order to keep the eavesdropper Eve from reading the message, she **encrypts** it to obtain the **ciphertext**. When Bob receives the ciphertext, he **decrypts** it and reads the message. In order to encrypt the message, Alice uses an **encryption key**. Bob uses a **decryption key** to decrypt the ciphertext. Clearly, the decryption key must be kept secret from Eve.

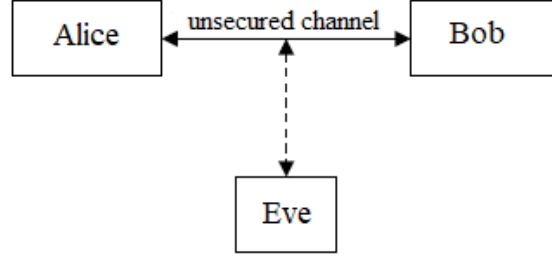


Figure 3.1 Basic communications model.

These ideas are described formally using the following mathematical notation.

Definition 3.1.1 *A Cryptosystem is a five tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ satisfying the following conditions;*

- (i) \mathcal{P} is a finite set of possible plaintexts.
- (ii) \mathcal{E} is a finite set of possible ciphertexts.
- (iii) \mathcal{K} , the key space, is a finite set of possible keys.
- (iv) For each $\mathcal{P}, \mathcal{E}, \mathcal{K}$, there is an encryption rule $e_k \in \mathcal{E}$ and a corresponding decryption rule $d_k \in \mathcal{D}$. Each

$$e_k : \mathcal{P} \longrightarrow \mathcal{C} \quad \text{and} \quad d_k : \mathcal{C} \longrightarrow \mathcal{P}$$

are functions such that $d_k(e_k(x)) = x$ for every plaintext $x \in \mathcal{P}$.

Remark 3.1.1 *The property (iv) says that if a plaintext x is encrypted using e_k and the resulting ciphertext is subsequently decrypted using d_k , then the original plaintext x results.*

There are two basic types of cryptosystems:

- (i) A **private key** or **symmetric** cryptosystem is constructed in a way so that either d_k and e_k are the same or can be easily derived from each other. The key which is used in encryption is the same as the key which is used in the decryption. The most common private key cryptosystem is probably Data Encryption Standard (DES).

- (ii) A **public key** or an **asymmetric** cryptosystem is constructed so that for each $k \in K$, it is infeasible to determine d_k given e_k . The keys which used in encryption and decryption are different.

The main public key cryptosystems and their features are given as the following:

- **RSA cryptosystem:** Based on the fact that it is difficult to factor large integers.
- **Discrete Logarithm cryptosystems:** Based on the difficulty in finding discrete logarithm in large finite field.
- **Elliptic curves cryptosystems:** A generalization of the discrete logarithm cryptosystems are elliptic curve public-key cryptosystems (which we will describe in the next section).
- **Knapsack cryptosystem** (Merkle–Hellman system): Based on difficulty in solving general knapsack problem.

Public key cryptography depends on the notion of trapdoor function.

Definition 3.1.2 A **one way function** $f : \mathcal{M} \longrightarrow \mathcal{C}$ is an invertible function such that for each $m \in \mathcal{M}$ it is "easy" to compute $f(m)$, while for most $c \in \mathcal{C}$ it is "hard" to compute $f^{-1}(c)$.

- A one way function $f : \mathcal{M} \longrightarrow \mathcal{C}$ is said to be a **trapdoor one –way function** if there is some extra information with which f can be efficiently inverted. This extra information is called the **trapdoor**.

Example 3.1.1 If g is a primitive element of a finite field \mathbb{F}_p , then the function

$f : \{0, 1, \dots, p-2\} \longrightarrow \{0, 1, \dots, p-1\}, x \longmapsto g^x$ is easy to compute by fast exponentiation, but an efficient inversion function is not known because it is difficult to compute discrete logarithms. Therefore, f can be used as a one way function.

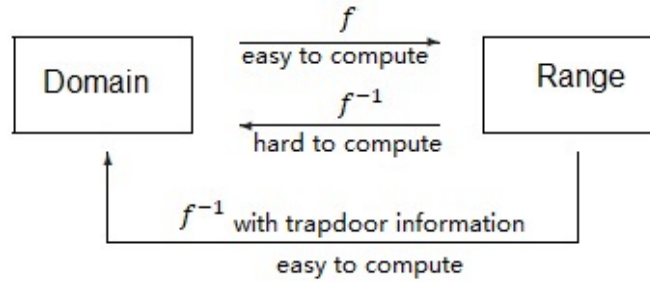


Figure 3.2 Illustration of a one-way trapdoor function.

The popular public key cryptosystem is RSA which is based on the hardness of factoring large integers.

3.1.1 RSA cryptosystem

RSA cryptosystem was invented in 1977 and named for its inventors **R**ivest, **S**hamir, and **A**dleman. (For details see [5]).

The sender Alice wishes to transmit a message M securely over a public channel to the receiver Bob. This can be accomplished by the following steps.

Key generation:

Bob creates his public and private keys by the following process:

1. *generates two large primes p and q .*
2. *computes $n = pq$ and $\varphi(n) = (p - 1)(q - 1)$, where φ denotes Euler's phi function.*
3. *chooses a random integer $e, 1 < e < \varphi(n)$, so that $\gcd(e, \varphi(n)) = 1$.*
4. *computes $d \equiv e^{-1} \pmod{\varphi(n)}$ using the Euclidean extended algorithm (see [5]).*
5. *publishes (n, e) and keeps d, p, q secret.*

Encryption:

Alice wants to send a message to Bob. First, she encodes the message M as an integer m such that $0 < m < n$. Then she

1. *looks up Bob's public key (n, e) .*
2. *computes $c \equiv m^e \pmod{n}$.*
3. *sends c to Bob.*

Decryption:

Bob recovers the message m via

$$c^d \equiv m^{ed} \equiv m^{1+j\varphi(n)} \equiv m \pmod{n};$$

where j is an integer such that $ed = 1 + j\varphi(n)$.

Formally, RSA cryptosystem is given as the following :

Given positive integer n and primes p, q such that $n = pq$. The RSA cryptosystem is the five-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$, and

$$\mathcal{K} = \{(n, p, q, e, d) | e, d \in \mathbb{Z}_{\varphi(n)}; ed \equiv 1 \pmod{\varphi(n)}\}.$$

For each $K = (n, p, q, e, d) \in \mathcal{K}$ and $m, c \in \mathbb{Z}_n$, we define

$$e_K(m) = m^e \pmod{n}, \quad d_K(c) = c^d \pmod{n}.$$

Where e_K, d_K are respectively the encryption and decryption functions.

Example 3.1.2 *We represent the letters of the alphabet by elements in \mathbb{Z}_{26} as $A = 1, B = 2, \dots, Z = 26$. Let $n = pq = 3 \cdot 11 = 33$ and choose $e = 3$. Then $\varphi(n) = 20$ and $3d \equiv 1 \pmod{20}$ has the solution $d = 7$.*

- To encipher⁽¹⁾ the word ALGEBRA we represent it in the numerical form, namely 1, 12, 7, 5, 2, 18, 1.

By computing $1^3 \equiv 1 \pmod{33}$, $12^3 \equiv 12 \pmod{33}$, etc., we find the ciphertext 1, 12, 13, 268, 24, 1, which is the word ALMZIXA.

- To decipher the ciphertext, say, QZLLI or 17, 26, 12, 12, 9, we calculate $17^7 \equiv 8 \pmod{33}$ etc. and find the message "HELLO".

Remark 3.1.2 The trapdoor—one way RSA function is given as follows :

$$f(m) = m^e \pmod{m} \quad \text{for } m \in \mathbb{Z}_n \text{ and } e, n \in \mathbb{N}^*. \quad \text{It is}$$

- easy to evaluate $m \mapsto m^e \pmod{n}$.
- difficult to invert $c \mapsto c^{\frac{1}{e}} \pmod{n}$, for integers c with $1 < c < n$ and $\gcd(c, n) = 1$.
- possible to invert $f(m)$ with the "trapdoor" d .

Remark 3.1.3 Practical RSA parameters are much, much larger. So the primes p and q are much larger, for this there are primality tests to find p and q for example Fermat and Miller–Rabin Primality tests (see [5]).

3.2 Elliptic curve cryptosystems

In this section, we will discuss some cryptosystems based on elliptic curves especially on the discrete logarithm problem for elliptic curves. For this we first need to define the DLP on the elliptic curves.

3.2.1 The Elliptic Curves Discrete Logarithm Problem

Similar to the discrete logarithm problem for elements from finite fields \mathbb{F}_p , as described in section 1.4, we can define the discrete logarithm problem for elements of $E(\mathbb{F}_p)$ for an elliptic curve E .

⁽¹⁾The words encipher and decipher are sometimes used instead of encrypt and decrypt.

Definition 3.2.1 Let E be an elliptic curve over the finite field \mathbb{F}_p and let P a point which generates a cyclic subgroup of $E(\mathbb{F}_p)$. 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 for \mathbb{F}_p , we denote this integer n by

$$n = \log_P(Q)$$

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

In other words, we need to find out how many times P must be added to itself in order to get Q .

Example 3.2.1 Let $E : y^2 \equiv x^3 + 2x + 2 \pmod{17}$, and let $P = (5, 1)$ and $Q = (16, 4)$ are two points on E . We want to find the integer n such that $Q = nP$.

We compute point multiplication as the following:

P	$2P$	$3P$	\dots	$12P$	$13P$
$(5, 1)$	$(6, 3)$	$(10, 6)$	\dots	$(0, 11)$	$(16, 4)$

Therefore, $\log_P(Q) = 13$.

Remark 3.2.1

- If n_0 is a solution of an ECDLP, $Q = nP$, then $n + is$ is also solution where $i \in \mathbb{Z}$ and s is the order of P . Hence $\log_P(Q) \in \mathbb{Z}_s$.
- The elliptic discrete logarithm satisfies

$$\log_P(Q_1 + Q_2) = \log_P(Q_1) + \log_P(Q_2), \quad \text{for all } Q_1, Q_2 \in E(\mathbb{F}_p).$$

- \log_P is a group morphism from $E(\mathbb{F}_p)$ to \mathbb{Z}_s .
- Note that the symbol “+” was chosen arbitrarily to denote the group operation. If we had chosen a multiplicative notation instead, the ECDLP would have had the form $Q = P^n$, which would have been more consistent with the conventional DLP in \mathbb{F}_p^* .

Group	\mathbb{F}_p^*	$E(\mathbb{F}_p)$
Discrete Logarithm Problem	Given $g \in \mathbb{F}_p^*$ and $g^n = h \pmod{p}$, find n .	Given $P \in E(\mathbb{F}_p)$ and $Q = nP$, find n .

Table 3.1 Correspondence between DLP and ECDLP.

The following algorithm allows us to solve the *ECDLP* in some cases.

Baby step–Giant step algorithm

This method work for arbitrary group G . developed by D. Shanks [18, p146], requires approximately \sqrt{N} steps and around \sqrt{N} storage. Therefore it only works well for moderatesized N . Since our main focus is elliptic curves, we choose $G = E(\mathbb{F}_p)$ with $\#E(\mathbb{F}_p) = N$.

Suppose that there exists an integer k such that $Q = kP$ with $P, Q \in E(\mathbb{F}_p)$. 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 $j = 0, 1, \dots, m-1$ until one matches an element from the stored list.
4. If $iP = Q - jmP$, we have $Q = kP$ with $k \equiv i + jm \pmod{N}$.

Why does this work?

Since $m > \sqrt{N}$, we may assume the answer k satisfies $0 \leq k < m^2$. Write $k = k_0 + mk_1$ with $k_0 \equiv k \pmod{m}$ 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

$$Q - k_1mP = kP - k_1mP = k_0P,$$

so there is a match.

Remark 3.2.2

- 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 $Q - (j-1)mP$.
- 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.

Example 3.2.2 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 $k = 23$.

Remark 3.2.3 There are other methods to solve ECDLP that we have not mentioned here. For details see [18].

The hardness of the elliptic curve discrete logarithm problem is essential for the security of all elliptic curve cryptographic schemes (cryptosystems).

3.2.2 Elliptic Curve Diffie–Hellman key exchange

By analogy to the conventional Diffie–Hellman key exchange that is proposed by Whitfield Diffie and Martin Hellman in 1976 (see [5], [26]), we can now realize a key exchange using elliptic curves. This is referred to as elliptic curve Diffie–Hellman key exchange, or ECDH.

Alice and Bob want to send a message to each other. The process is given as the following:

1. Alice and Bob agree to use a particular elliptic curve $E(\mathbb{F}_p)$ and a particular point $P \in E(\mathbb{F}_p)$. Alice chooses a secret integer n_A , and Bob chooses a secret integer n_B . They compute the associated multiples

$$\overbrace{Q_A = n_A P}^{\text{Alice computes this}} \quad \text{and} \quad \overbrace{Q_B = n_B P}^{\text{Alice computes this}}.$$

2. They exchange the values of Q_A and Q_B .
3. Alice then uses her secret multiplier to compute $n_A Q_B$, and Bob similarly computes $n_B Q_A$.

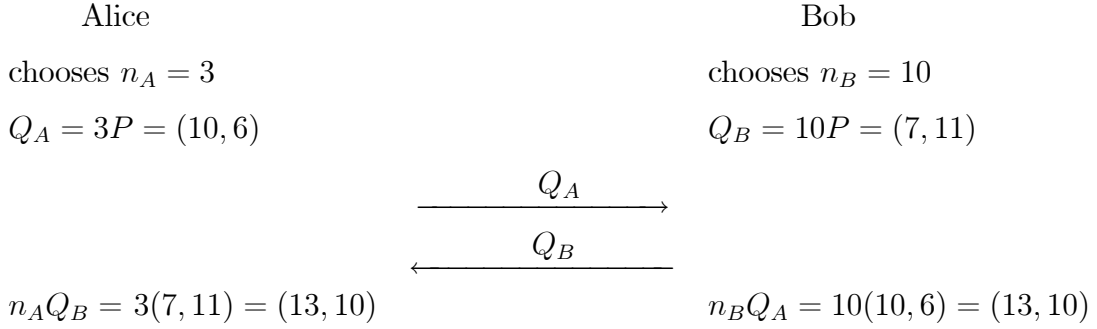
They now have the shared secret value

$$K_{A,B} = n_A Q_B = n_A(n_B P) = n_B(n_A P) = n_B Q_A.$$

Therefore they use the x -coordinate of the point $K_{A,B}$ as a key to communicate privately via a symmetric cipher.

Example 3.2.3 *Alice and Bob decide to use Elliptic Curve Diffie–Hellman with the following:*

The elliptic curve is $y^2 \equiv x^3 + 2x + 2 \pmod{17}$, which forms a cyclic group of order $\#E(\mathbb{F}_{17}) = 19$. The base point is $P = (5, 1)$. The process is as follows:



Remark 3.2.4

- Since Bob and Alice will use the x -coordinate as their shared secret key, then they can only exchange the x -coordinates of Q_A and Q_B respectively, then they compute the y -coordinates from the equation of the elliptic curve and they will obtain either the actual point or its negative. Eventually, they will obtain $\pm K_{A,B}$ but, since the x -coordinates of $K_{A,B}$ and $-K_{A,B}$ are the same, no confusion results.
- Note that the eavesdropper Eve knows Q_A and Q_B , so if she can solve the ECDLP of $Q_A = n_A P$ or $Q_B = n_B P$, then she can find the shared key $K_{A,B}$.
- Suppose that Eve can solve $Q_A = n_A P$, then she finds n_A and computes

$$n_A Q_B = K_{A,B} = n_B Q_A.$$

The precise problem that Eve needs to solve is given in the following definition.

Definition 3.2.2 Let $E(\mathbb{F}_p)$ be an elliptic curve over a finite field and let $P \in E(\mathbb{F}_p)$. The Elliptic Curve Diffie–Hellman Problem (ECDHP) is the problem of computing the value of $n_1 n_2 P$ from the known values of $n_1 P$ and $n_2 P$.

3.2.3 Elliptic ElGamal public key cryptosystem

Elliptic ElGamal cryptosystem is directly based on ECDLP described above, and it is analog of ElGamal cryptosystem which was proposed by Taher ElGamal in 1985 (see [26]).

Alice wants to send a message to Bob. The process is given as follows:

Key generation:

Bob establishes his public and private keys as follows:

1. *He chooses an elliptic curve E over a finite field \mathbb{F}_q such that the discrete logaeithm 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).*
2. *He chooses a secret integer n_B and computes $Q_B = n_BP$.*
 - *The elliptic curve E , the finite field \mathbb{F}_q , and the points P and Q_B are Bob's public key, they are made public.*
 - *Bob's private key is the integer n_B .*

Encryption:

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

1. *Expresses her message as a point $M \in E(\mathbb{F}_q)$.*
2. *Chooses a secret random ephemral integer k_e and computes $C_1 = k_eP$.*
3. *Computes $C_2 = M + k_eQ_B$.*
4. *Finally, the two points (C_1, C_2) are sent to Bob.*

Decryprion:

Bob decrypts by calculating

$$M = C_2 - n_BC_1.$$

This decryption works because

$$C_2 - sC_1 = (M + k_eQ_B) - n_B(k_eP) = M + k_e(n_BP) - n_Bk_e(P) = M.$$

Formally, the elliptic curve ElGamal cryptosystem is given as the following:

the elliptic curve ElGamal cryptosystem is the five-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where

$$\mathcal{P} = E(\mathbb{F}_q), \mathcal{C} = E(\mathbb{F}_q) \times E(\mathbb{F}_q), \mathcal{K} = \{(q, E, P, n, Q, d) \mid Q = dP\}.$$

For each $K = (q, E, n, Q, d) \in \mathcal{K}$ and $k_e = [1, n - 1]$,

$$e_K(M) = (k_e, P, M + k_e Q).$$

For $(C_1, C_2) \in E(\mathbb{F}_q) \times E(\mathbb{F}_q)$,

$$d_k(C_1, C_2) = C_2 - dC_1.$$

Where e_K, d_K are respectively the encryption and decryption functions.

Remark 3.2.5 *If Eve can solve the ECDLP $Q_B = n_B P$ or $C_1 = k_e P$, then she can know n_B, k_e , then she will discover the messages between Alice and Bob*

Example 3.2.4 *Let $E : y^2 = x^3 + x + 4$ be an elliptic curve over \mathbb{F}_{23} , $E(\mathbb{F}_{23})$ is a cyclic group of order $\#E(\mathbb{F}_{23}) = 29$. We put a correspondence between the points of $E(\mathbb{F}_{23})$ and the english alphabet letters excluding space, punctuation marks, etc. as in the following table:*

\square	A	B	C	D	E	F	G	H
\mathcal{O}	(0, 2)	(0, 21)	(1, 11)	(1, 12)	(4, 7)	(4, 16)	(7, 3)	(7, 20)
I	J	K	L	M	N	O	P	Q
(8, 8)	(8, 15)	(9, 11)	(9, 12)	(10, 5)	(10, 18)	(11, 9)	(11, 14)	(13, 11)
R	S	T	U	V	W	X	Y	Z
(13, 12)	(14, 5)	(14, 18)	(15, 6)	(15, 17)	(17, 9)	(17, 14)	(18, 9)	(18, 14)
,	.							
(22, 5)	(22, 18)							

Table 3.2 Correspondence table for the elliptic curve $E : y^2 = x^3 + x + 1 \pmod{23}$.

Alice wants to send the message $M = \text{"HELLO"}$ to Bob. So Bob chooses a point $P = (0, 2)$, a random number $n_B = 5$ as his private key and he computes his public key $Q_B = n_BP = (7, 20)$.

Encryption: to encrypt the word "HELLO", Alice converts the letters H, E, L, L, O into points on the elliptic curve using the correspondence in the above table as the following $H \leftrightarrow (7, 20), E \leftrightarrow (4, 7), L \leftrightarrow (9, 12), O \leftrightarrow (11, 9)$, and chooses a random ephemeral key k_e then he computes C_1 and C_2 as follows:

1. Alice selects a random number $k_e = 9$ for encrypting the character 'H'. Then the point $(7, 20)$ is encrypted as

$C_1 = k_e P = 9(0, 2) = (4, 7)$ which corresponds to the character 'E' in the conversion table.

$C_2 = m + k_e Q_B = (7, 20) + 9(7, 20) = (1, 11)$ which corresponds to 'C' in the conversion table. So, the character 'H' in the plain text is encrypted to two characters $\{E, C\}$ in the cipher text.

2. Let $k_e = 7$. Then the point $(7, 20)$ is encrypte as

$C_1 = 7(0, 2) = (15, 6)$ which corresponds to 'U' in the table.

$C_2 = (4, 7) + 7(7, 20) = (18, 14)$, which corresponds to 'Z' in the table.

So, 'E' is encrypted as $\{U, Z\}$.

3. Let $k_e = 6$. then the point $(9, 12)$ is encrypted as

$C_1 = 6(0, 2) = (9, 11)$ which corresponds to 'K' in the table.

$C_2 = (9, 12) + 6(7, 20) = (7, 3)$, which corresponds to 'G' in the table.

So, 'L' is encrypted as $\{K, G\}$.

4. Let $k_e = 2$. Then the point $(9, 12)$ is encrypted as

$C_1 = 2(0, 2) = (13, 12)$ which corresponds to 'R' in the table.

$C_2 = (9, 12) + 2(7, 20) = (1, 12)$, which corresponds to 'D' in the table.

So, 'L' is encrypted as $\{R, D\}$.

5. Let $k_e = 8$. Then the point $(7, 20)$ is encrypted as

$C_1 = 8(0, 2) = (14, 5)$ which corresponds to 'S' in the table.

$C_2 = (11, 9) + 8(7, 20) = (18, 9)$, which corresponds to 'Y' in the table.

So, 'O' is encrypted as $\{S, Y\}$.

Alice communicates $\{E, C; U, Z; K, G; T, D; S, Y\}$ as the ciphertext to Bob in public channel.

Decryption: Bob after receiving the cipher text $\{E, C; U, Z; K, G; T, D; S, Y\}$ converts the cipher characters into the points

$$(1, 30), (2, 13); (15, 6), (18, 14); (9, 11), (7, 3); (13, 12), (1, 12); (14, 5), (18, 9).$$

He decrypts the message taking two points at a time as the points C_1 and C_2 and computing $C_2 - n_A C_1 \in E(\mathbb{F}_{23})$.

For $(C_1, C_2) = ((13, 12), (18, 14))$, we have $C_2 - n_A C_1 = (18, 14) - 5(13, 12) = (7, 20) \leftrightarrow H$.

By the similar way, He continues to obtain the plaintext "HELLO".

Remark 3.2.6 In the above example we choose a small numbers just to explain the idea but in the general case the numbers n_A, k_e and the order of $E(\mathbb{F}_q)$ are much larger.

Remark 3.2.7

- It is important for Alice to use a different random k_e each time she sends a message to Bob because if Alice uses the same k_e for both M and M' . Eve recognizes this because then $C_1 = C'_1$. She then computes $C_2 - C'_2 = (M + k_e Q_A) - (M' + k_e Q_A) = M - M'$. Then $M' = C'_2 - C_2 - M$.
- Suppose that Eve has discovered the message M , then she can find out M' , so she calculates $M' = C'_2 - C_2 - M$. Therefore, knowledge of one plaintext M' allows Eve to deduce another plaintexts M' in this case.

3.2.4 The Elliptic Curve Digital Signature Algorithm

A **digital signature** is an electronic analogue of a hand-written signature. This means that a digital signature allows the receiver of a message to convince any third party that the message in fact originated from the sender.

The Elliptic Curve Digital Signature Algorithm (ECDSA) was standardized in the US by the American National Standards Institute (ANSI) in 1998.

Before introducing the elliptic curves digital signatures we first need to define the notion of a **hash function**.

Definition 3.2.3 *Let \mathcal{M} and \mathcal{M}' be two sets, the hash function is a function $h : \mathcal{M} \longrightarrow \mathcal{M}'$, satisfies the following properties:*

1. *Given $x \in \mathcal{M}$, the value $h(x)$ can be calculated very quickly.*
2. *Given $y \in \mathcal{M}'$, it is computationally infeasible to find x with $h(x) = y$.*
3. *It is computationally infeasible to find distinct elements x_1 and x_2 with $h(x_1) = h(x_2)$.*

Remark 3.2.8

- *There are several popular hash functions available, for example MD5 (due to Rivest, it produces a 128-bit output), we will not discuss these here. (For details, see [5], [11] and [26]).*
- *The importance of the use of the hash functions in the digital signatures is that they do not allow to forge the signature.*

The steps in the ECDSA standard are conceptionally closely related to the Digital Signature Algorithm (DSA) cryptosystem (see [26]). However, its discrete logarithm problem is constructed in the group of an elliptic curve. The former is often preferred in practice, and we will only introduce this one in what follows.

Suppose that Alice needs to send a message x to Bob. Alice wants to sign her message. The process of ECDSA is composed of three main steps: key generation, signature generation and signature verification.

Key Generation:

1. Choose an elliptic curve E over a finite field \mathbb{F}_q , a point P which generates a cyclic group of prime order ℓ .
2. For Alice to sign a message m he needs to choose a random integer d as her private key. Then compute her public key $Q = dP$.

Signature Generation:

To sign the message m , Alice does the following steps:

1. Choose an integer as random ephemeral key k_e with $0 < k_e < \ell$.
2. Compute $R = k_e P = (x_R, y_R)$.
3. Let $r = x_R$.
4. Compute $s \equiv (h(m) + d \cdot r)k_e^{-1} \bmod \ell$. ($h(m)$ is the hash value of x).

Therefore the signed message is $((m, (r, s)))$.

Signature Verification:

Bob verifies that the signature is valid by the following process:

1. Compute auxiliary value $w \equiv s^{-1} \bmod \ell$.
2. Compute auxiliary value $u_1 \equiv w \cdot h(m) \bmod \ell$.
3. Compute auxiliary value $u_2 \equiv w \cdot r \bmod \ell$.
4. Compute $V = u_1 P + u_2 Q = (x_V, y_V)$.
5. The verification of the signature (r, s) follows from:

$$x_V \begin{cases} \equiv r \bmod \ell & \implies \text{valid signature.} \\ \not\equiv r \bmod \ell & \implies \text{invalid signature.} \end{cases}$$

The verifier accepts a signature (r, s) only if the x_V has the same value as the signature parameter $r \bmod \ell$. Otherwise, the signature should be considered invalid.

Proof. We show that a signature (r, s) satisfies the verification condition $r \equiv x_V \bmod \ell$. We'll start with the signature parameters:

$$s \equiv (h(m) + d \cdot r)k_e^{-1} \bmod \ell$$

which is equivalent to

$$k_e \equiv s^{-1}h(m) + s^{-1} \cdot d \cdot r \bmod \ell.$$

The right-hand side can be expressed in terms of the auxiliary values u_1 and u_2 :

$$k_e \equiv u_1 + d \cdot u_2 \bmod \ell.$$

Since the point P generates a cyclic group of order ℓ , we can multiply both sides of the equation with P :

$$k_e P = (u_1 + d \cdot u_2)P.$$

Since the group operation is associative, we can write

$$k_e P = u_1 P + d \cdot u_2 P$$

and

$$k_e P = u_1 P + u_2 Q.$$

What we showed so far is that the expression $u_1 P + u_2 Q$ is equal to $k_e P$ if the correct signature and key (and message) have been used. But this is exactly the condition that we check in the verification process by comparing the x -coordinates of $V = u_1 P + u_2 Q$ and $R = k_e P$. ■

Remark 3.2.9

- *It is essential for the security of ECDSA that signers use distinct values for k_e for every signature, since repeated values allow an adversary to efficiently compute the long-term private key from one or two signature values.*
- *If Alice wants to keep her message m secret, she encrypts it (for example by RSA cryptosystem) and sign the ciphertext instead of m .*

Example 3.2.5 *We will base our example on the elliptic curve $y^2 = x^3 + x + 6$, defined over \mathbb{F}_{11} . The parameters of the ECDSA are $p = 11, \ell = 13, P = (2, 7), d = 7$ and $Q = (7, 2)$. Suppose we have a message m with $h(m) = 4$, and Alice wants to sign the message m using the random value $k_e = 3$. She will compute*

$$\begin{aligned} R &= (x_R, y_R) = 3(2, 7) = (8, 3) \\ r &= x_R \bmod 13 = 8, \text{ and} \\ s &= 3^{-1}(4 + 7 \times 8) \bmod 13 = 7. \end{aligned}$$

Therefore $(8, 7)$ is the signature.

Bob verifies the signature by performing the following computations.

$$\begin{aligned} w &= 7^{-1} \bmod 13 = 2 \\ u_1 &= 2 \times 4 \bmod 13 = 8 \\ u_2 &= 2 \times 8 \bmod 13 = 3 \\ (u, v) &= 8A + 3B = (8, 3), \text{ and} \\ u &= 8 \bmod 13 = r. \end{aligned}$$

Hence, the signature is verified.

Remark 3.2.10 *The hash function that used in ECDSA is called SHA–1. For details see [11], [5].*

There are other types of cryptosystems based on elliptic curves that we have not mentioned. For details see [11], [18].

3.2.5 Comparing ECC with RSA public key cryptosystem

RSA is the best known and the most widely asymmetric cryptosystem. For this we compare it with ECC.

- The elliptic curve discrete logarithm problem is harder than the integer factorisation. Thus the breaking of ECC is harder than RSA cryptosystem.
- The ECC achieves the same level of security as RSA with smaller key lengths. For example, to achieve 128 bits of security level, RSA algorithm needs a key length of 3072 bits, while ECC needs a key length of 256 bits as shown in Table 3.3.

Security Level (bit)	ECC key length (bit)	RSA key length (bit)
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

Table 3.3 Comparable Key lengths.

- In many cases, ECC has performance advantages (fewer computations) and bandwidth advantages (shorter signatures and keys) over RSA cryptosystem. However, RSA operations which involve short public keys are still much faster than ECC operations (e.g. see the first row in Tables 3.4–3.5).
- The tables 3.4–3.5 shows a comparative analysis of RSA and ECC is presented on the total (encryption and decryption) time for the data (plaintext) of lengths 64 bits and 256 bits respectively. (The results are from [9]).

Scurity level (bit)	Total Time	
	ECC	RSA
80	8.0784	5.6738
112	16.9188	20.5743
128	22.4466	46.6454
144	28.7093	77.9027

Table 3.4 64 bits – Total time (in seconds).

Scurity level (bit)	Total Time	
	ECC	RSA
80	30.8091	19.8772
112	66.0339	102.6153
128	85.8446	210.1697
144	109.6556	311.6368

Table 3.5 256 bits – Total time (in seconds).

Conclusion

The objective of this memory was the study of elliptic curves and their uses in cryptography.

We have presented the elliptic curves cryptosystems which are an extension to the cryptosystems that based on the difficulty of the discrete logarithm problem. Also we have compared them with RSA asymmetric cryptosystem, the principal attraction of elliptic curve cryptosystem compared to RSA is that it offers equal security for a smaller keylengths which results in a faster encryption and decryption process. This advantage led to use elliptic curves cryptosystems in many applications especially the devices that have a small memory space such as mobile phones and smart cards.

Bibliography

- [1] **A.K. Bhandari, D.S. Nagaraj, B. Ramakrishnan, T.N. Venkataramana.** Elliptic Curves, Modular Forms and Cryptography. Hindustan Book Agency, India, 2003.
- [2] **A. Enge.** Elliptic Curves and their applications to cryptography: An Introduction, (2nd ed.). Kluwer Academic Publishers, 2001.
- [3] **A. Jurišić, A. Menezes.** Elliptic Curves and Cryptography. Dr. Dobb's Journal, 26-36, 1997.
- [4] **A. Menezes.** Elliptic curve public key cryptosystems. Springer & Business Media, New York, 1993.
- [5] **C. Paar, J. Pelzl.** Understanding Cryptography. Springer, Verlag Berlin Heidelberg, 2010.
- [6] **D. Hankerson, A. Menezes, S. Vanstone.** Guide to Elliptic Curve Cryptography. Springer-Verlag, New York, 2004.
- [7] **D. Cox, J. Little, D. O'Shea.** Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, (3ed ed). Springer Science & Business Media, LLC, New York, 2007.
- [8] **D.M. Burton.** Elementary Number Theory, (7th ed.). McGraw-Hill Companies, Inc., New York, 2011.
- [9] **D. Mahto, D.K. Yadav.** RSA and ECC: A Comparative Analysis. International Journal of Applied Engineering Research, 12(19), 9053-9061, 2017.

- [10] **D. Mihoubi.** Introduction à la Cryptographie, Master Courses. M'sila University, 2018 – 2019.
- [11] **D.R. Stinson.** Cryptography: Theory and Practice, (3ed ed.).Chapman & Hall/CRC, New York, 2006.
- [12] **D.S. Kumar, CH. Suneetha, A. Chandrasekhar.** Encryption of data using elliptic curve over finite fiels. International Journal of Distributed and Parallel Systems (IJDPS), 3(1), 301-308, 2012.
- [13] **F. Heß, A. Stein, S. Stein, M. Lochter.** The Magic of Elliptic Curves and Public-Key Cryptography. Jahresbericht der Deutschen Mathematiker-Vereinigung, 114(2), 59-88, 2012.
- [14] **I. Blake, G. Seroussi, N. Smart.** Elliptic Curves in Cryptography. Cambridge University Press, 1999.
- [15] **J. Hoffstein, J. Pipher, J.H. Silverman.** An Introduction to Mathematical Cryptography. Springer, New York, 2008.
- [16] **J.H. Silverman.** The Arithmetic of Elliptic Curves, (2nd ed.). Springer-Verlag, New York, 2009.
- [17] **J.L.G. Pardo.** Introduction to Cryptography with Maple. Springer-Verlag, Berlin, 2013.
- [18] **L.C. Washington.** Elliptic Curves: Number Theory and Cryptography, (2nd ed.). Chapman & Hall/CRC, New York, 2008.
- [19] **N. Koblitz.** A Course in Number Theory and Cryptography, (2nd ed.). Springer-Verlag, New York, 1994.
- [20] **N.L. Biggs.** Codes: An Introduction to Information Communication and Cryptography. Springer-Verlag, London, 2008.
- [21] **R.A. Mollin.** An introduction to cryptography, (2nd ed.). Chapman & Hall/CRC, New York, 2007.

- [22] **R. Lidl, G. Pilz.** Applied Abstract Algebra, (2nd ed.). Springer-Verlag, New York, 1998.
- [23] **S. Ling, C. Xing.** Coding Theory: A First Course. Cambridge University Press, 2004.
- [24] **S. Schmitt, H.G. Zimmer.** Elliptic Curves: A Computational Approach. Walter de Gruyter GmbH & Co. KG, Germany, 2003.
- [25] **W.J. Gilbert, W.K. Nicholson.** Modern Algebra With Applications, (2nd ed.). John Wiley & Sons, Inc., Hoboken, New Jersey, Canada, 2004.
- [26] **W. Stallings.** Cryptography and network security: Principles and Practices, (5th ed.). New York, Pearson Education, Inc., 2011.