FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

ASSIGNMENT OF MASTER’S THESIS

Title:	Summation polynomials and the discrete logarithm problem on elliptic curve
Student:	Bc. Matyáš Hollmann
Supervisor:	Ing. Ivo Petr, Ph.D.
Study Programme:	Informatics
Study Branch:	Computer Security
Department:	Department of Information Security
Validity:	Until the end of winter semester 2020/21

Instructions

Discrete logarithm problem (DLP) is a fundamental problem arising in modern cryptography. While there exist subexponential algorithms that solve DLP in multiplicative groups of finite fields, no such algorithms are known for groups of points of elliptic curves (ECDLP). Attempts to develop index calculus methods for elliptic curves include so called summation polynomials that give algebraic relations whose solution may give a solution of ECDLP.

The goal of the thesis is to get acquainted with cryptography of elliptic curves, give thorough description of the state of the art of the summation polynomial algorithm, implement it in suitable language and test its performance. Student will focus on available methods of effective generation and solution (Groebner basis and other methods) of algebraic relations appearing in the algorithm.

References

[1] I. Semaev, New algorithm for the discrete logarithm problem on elliptic curves, Cryptology ePrint Archive, Report 2015/310
[2] S. D. Galbraith and S. W. Gebregiyorgis, Summation polynomial algorithms for elliptic curves in characteristic two, Cryptology ePrint Archive, Report 2014/806

prof. Ing. Róbert Lórencz, CSc.
Head of Department

doc. RNDr. Ing. Marcel Jiřina, Ph.D.
Dean

Prague February 22, 2019

FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Master's thesis

Summation polynomials and the discrete logarithm problem on elliptic curve

Bc. Matyáš Hollmann

Department of Information Security
Supervisor: Ing. Ivo Petr, Ph.D.

April 29, 2019

Acknowledgements

THANKS (remove entirely in case you do not with to thank anyone)

Declaration

I hereby declare that the presented thesis is my own work and that I have cited all sources of information in accordance with the Guideline for adhering to ethical principles when elaborating an academic final thesis.

I acknowledge that my thesis is subject to the rights and obligations stipulated by the Act No. 121/2000 Coll., the Copyright Act, as amended. In accordance with Article 46(6) of the Act, I hereby grant a nonexclusive authorization (license) to utilize this thesis, including any and all computer programs incorporated therein or attached thereto and all corresponding documentation (hereinafter collectively referred to as the "Work"), to any and all persons that wish to utilize the Work. Such persons are entitled to use the Work in any way (including for-profit purposes) that does not detract from its value. This authorization is not limited in terms of time, location and quantity. However, all persons that makes use of the above license shall be obliged to grant a license at least in the same scope as defined above with respect to each and every work that is created (wholly or in part) based on the Work, by modifying the Work, by combining the Work with another work, by including the Work in a collection of works or by adapting the Work (including translation), and at the same time make available the source code of such work at least in a way and scope that are comparable to the way and scope in which the source code of the Work is made available.

In Prague on April 29, 2019 . . . .

Czech Technical University in Prague
Faculty of Information Technology

0.0.1 Citation of this thesis

Hollmann, Matyáš. *Summation polynomials and the discrete logarithm problem on elliptic curve.* Master's thesis. Czech Technical University in Prague, Faculty of Information Technology, 2019.

Abstrakt

V několika větách shrňte obsah a přínos této práce v českém jazyce.

Klíčová slova Replace with comma-separated list of keywords in Czech.

Abstract

Summarize the contents and contribution of your work in a few sentences in English language.

Keywords Replace with comma-separated list of keywords in English.

Contents

List of Figures

List of Tables

Introduction

Chapter 1

Mathematical Background

In this chapter, we define terms that we use in the rest of this thesis. The first section is a revision of the terms standard in general algebra, the second part focuses on polynomials, and the last section introduces the reader to the topic of Gröbner bases. In the next chapter, we revise elliptic curve theory, introduce the reader to the concept of summation polynomials and state the discrete logarithm problem. This chapter is based mostly on the book by David A. Cox [1], MI-MKY lecture notes [2] and my bachelor thesis [3]. Other sources are cited individually at specific locations.

1.1 Introduction to General Algebra

General algebra, also called universal algebra in the past, is the theory of algebraic structures. An algebraic structure is a set of objects with a collection of mathematical operations on this set. An algebraic structure is defined by a set of axioms, requirements on the set and operations on it, and other properties of said algebraic structure are logically deduced based on the axioms. When we encounter a particular problem, we may try to classify it as a specific algebraic structure (by verifying its axioms) and use all of its deduced properties without the need to reprove them. We start this section with a definition of a simple algebraic structure called group.

Definition 1.1.1. A **group** G is an ordered pair $(M, \circ)$, where M is a non-empty set and binary operation $\circ : M \times M \to M$ (sometimes called the group law of G) that satisfies three requirements known as group axioms:

- $\forall x, y, z \in M : x \circ (y \circ z) = (x \circ y) \circ z,$ (associativity)
- $\exists e \in M,\ \forall x \in M : e \circ x = x \circ e = x,$ (identity element)
- $\forall x \in M,\ \exists x^{-1} \in M : x \circ x^{-1} = x^{-1} \circ x = e.$ (inverse element)

Remark. M is closed under the operation $\circ$.

Notational Remark. When we talk about an element g of a group G ($g \in G$), we mean that g is an element of the underlying set M ($g \in M$).

Groups that satisfy commutativity law:

- $\forall x, y \in M : x \circ y = y \circ x$,

are called **Abelian groups** (in honour of a famous Norwegian mathematician Niels Henrik Abel).

Definition 1.1.2. If the set M has a finite number of elements, $G = (M, \circ)$ is called a **finite group**. **Order** of the finite group G is the number of elements of the underlying set M, and we denote it by $\#G$. If the set M is infinite, the order of G is infinite as well.

A simple example of an infinite Abelian group is $(\mathbb{Z}, +)$, the set of all integers equipped with standard addition. An example of a finite Abelian group is $\mathbb{Z}_n^+ = (\{0, 1, \dots, n-1\}, +_n),\ n \in \mathbb{N}$, where $+_n$ is addition modulo n and $\mathbb{N}$ is the set of all natural numbers (positive integers). Order of this group is n.

Remark. In every group, there exists just one unique identity element. Also, for every element $q \in G$ there exists just one inverse element, denoted by q^{-1} in the multiplicative notation and $-q$ in the additive notation. The inverse of a product of two group elements is a product of the respective inverses in the reversed order (order does matter in non-commutative groups, although in this thesis we are only concerned about Abelian groups).

An identity element in the additive notation is called a **zero** and denoted by 0, in the multiplicative notation an **unit** and denoted by 1.

In an additive group G, we define **multiplication** by an integer (repeated application of the group law) as follows:

$$\forall p \in G,\ \forall k \in \mathbb{Z} : kp := \begin{cases} \underbrace{p + p + \cdots + p}_{k\text{-times}} & k > 0, \\ 0 \text{ (identity element)} & k = 0, \\ \underbrace{(-p) + (-p) + \cdots + (-p)}_{k\text{-times}} & k < 0. \end{cases}$$

In a multiplicative group G, we define **exponentiation** (repeated application of the group law) in a similar manner:

$$\forall p \in G,\ \forall k \in \mathbb{Z} : p^k := \begin{cases} \underbrace{p \cdot p \cdot\ \cdots\ \cdot p}_{k\text{-times}} & k > 0, \\ 1 \text{ (identity element)} & k = 0, \\ \underbrace{p^{-1} \cdot p^{-1} \cdot\ \cdots\ \cdot p^{-1}}_{k\text{-times}} & k < 0. \end{cases}$$

Definition 1.1.3. Order of an element $a \in G$ is the smallest positive integer $k \in \mathbb{N}$ such that: $a^k = 1$ (similarly $ka = 0$ in the additive notation). We denote the order of an element a by $\#a = k$, and if there isn't such k, we say the order of a is infinite (this case may only happen if G itself is of infinite order). Elements of finite order are sometimes called **torsion** elements.

Remark. Order of an identity element in any group G is always 1, and due to the uniqueness of the identity element, it's also the only element in G of this order.

Definition 1.1.4. A group $(H, \circ)$ is a **subgroup** of a group $(G, \circ)$ if and only if $H \subseteq G$. The group law $\circ$ is the same, therefore an identity element $e \in G$ has to be an identity in any subgroup H of G as well. H is called a **trivial subgroup** of G if $H = \{e\}$ or $H = G$.

Definition 1.1.5. Lagrange's Theorem: Let G be a finite group and H a subgroup of G, then the order of the subgroup H divides the order of the group G: $\exists n \in \mathbb{N} : \#G = \#H \cdot n$.

Definition 1.1.6. Group G is called a **cyclic group** if and only if there exists an element $g \in G$ such that:

- $G = \langle g \rangle := \{g^n \mid n \in \mathbb{Z}\},$ (in the multiplicative notation)

or

- $G = \langle g \rangle := \{ng \mid n \in \mathbb{Z}\}.$ (in the additive notation)

Element g is then called a **generator** of the group G.

Remark. Ordered pair $(\langle a \rangle, \circ)$ form a subgroup of $(G, \circ)$ for any $a \in G$. The order of the group generated by the element a is the same as the order of the element a.

$$\forall a \in G : \#\langle a \rangle = \#a.$$

Definition 1.1.7. A **ring** $R = (M, +, \cdot)$ is a set equipped with two binary operations $+ : M \times M \to M$ and $\cdot : M \times M \to M$ satisfying following requirements:

- $(M, +)$ is an Abelian group,
- $\forall x, y, z \in M : x \cdot (y \cdot z) = (x \cdot y) \cdot z,$ (associativity)
- $\exists e \in M,\ \forall x \in M : e \cdot x = x \cdot e = x,$ (identity element w.r.t. oper. $\cdot$)
- $\forall x, y, z \in M : x \cdot (y + z) = x \cdot y + x \cdot z,$ (left distributive law)
- $\forall x, y, z \in M : (y + z) \cdot x = y \cdot x + z \cdot x.$ (right distributive law)

Notational Remark. When we talk about an element r of a ring R ($r \in R$), we mean that r is an element of the underlying set M ($r \in M$).

Definition 1.1.8. Let $R = (M, +, \cdot)$ be a ring and $(M \setminus \{0\}, \cdot)$ be an Abelian group, then $\mathbb{F} = (M, +, \cdot)$ is a **field**. Abelian group $(M, +)$ is called the additive group of the field $\mathbb{F}$ and denoted by $\mathbb{F}^+$, the identity element of this group is denoted by 0. Abelian group $(M \setminus \{0\}, \cdot)$ is called the multiplicative group of the field $\mathbb{F}$ and denoted by $\mathbb{F}^\times$, the identity element of this group is denoted by 1.

Definition 1.1.9. Let $\mathbb{F}$ be a field, 0 be the identity element of $\mathbb{F}^+$ and 1 be the identity element of $\mathbb{F}^\times$, if there exists such $n \in \mathbb{N}$:

$$\underbrace{1 + 1 + \cdots + 1}_{n\text{-times}} = 0,$$

we define the smallest $n \in \mathbb{N}$ satisfying this condition to be the **characteristic** of the field $\mathbb{F}$. If there isn't such n, we define the characteristic of the field $\mathbb{F}$ to be 0. We denote the characteristic of the field $\mathbb{F}$ by char($\mathbb{F}$).

The characteristic of a field is either 0 or a prime number. An example of a field of characteristic 0 are real numbers with standard addition and multiplication $(\mathbb{R}, +, \cdot)$.

An example of a field of prime characteristic p is a set of non-negative integers less than p equipped with addition modulo p and multiplication modulo p $(\{0, 1, \ldots, p-1\}, +_p, \cdot_p)$, we call this field the **Galois Field** of order p (order of a field is defined as the order of its additive group) and denote it by $GF(p)$.

Remark. All finite fields (fields with finite number of elements) are of prime characteristic.

Definition 1.1.10. Let $\mathbb{F}$, $\mathbb{T}$ be fields (equipped with the same binary operations), if $\mathbb{F} \subseteq \mathbb{T}$ we call $\mathbb{T}$ a **field extension** of the field $\mathbb{F}$. The field extension $\mathbb{T}$ of $\mathbb{F}$ can be viewed as $\mathbb{F}$-vector space, we treat elements of $\mathbb{F}$ as scalars and elements of $\mathbb{T}$ as vectors. If it is a finite-dimensional vector space, we call the dimension of this vector space the **degree of the extension** and denote it by $[\mathbb{T} : \mathbb{F}]$. From now on, we will denote the n-dimensional vector space over a field $\mathbb{F}$ by $\mathbb{F}^n$, $n \in \mathbb{N}$.

Remark. The finiteness of a vector space over a field is related only to the dimension of said vector space, it doesn't have to do anything with the finiteness of the base field. For example, we can view complex numbers $\mathbb{C}$ (an infinite field) as a 2-dimensional vector space over the real numbers $\mathbb{R}$ with a basis $(1,\ i)$, where i is the imaginary unit satisfying the equation: $i^2 = -1$.

1.2 Multivariate Polynomials

In this section, we discuss monomials and polynomials of multiple variables. In the first part, we revise some standard notation regarding polynomials. And in the second part, we introduce the reader to the concept of a monomial ordering, which is an essential building block for Gröbner bases that are the main topic of the next section. This section is based on [1].

Definition 1.2.1. A **monomial** m in $x_1, x_2, \ldots, x_n$ is a product of the form:

$$m(x_1, x_2, \ldots, x_n) := \prod_{k=1}^{n} x_k^{\alpha_k},\ \forall k \in \{1, \ldots, n\} : \alpha_k \in \mathbb{Z}_{\geq 0},$$

where $x_1, x_2, \ldots, x_n$ are **formal variables** and $\alpha_1, \alpha_2, \ldots, \alpha_n$ are **exponents**.

Notational Remark. We can simplify the notation. Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ be an n-tuple of non-negative integers and $X = (x_1, x_2, \ldots, x_n)$ an n-tuple of formal variables, then we set:

$$X^\alpha := \prod_{k=1}^{n} x_k^{\alpha_k},\ \alpha_k \in \mathbb{Z}_{\geq 0}, k \in \{1, \ldots, n\}.$$

Definition 1.2.2. The **total degree** of a monomial $X^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ is the sum of all its exponents and is denoted by $|\alpha|$.

$$|\alpha| := \sum_{k=1}^{n} \alpha_k.$$

Definition 1.2.3. A **polynomial** f over a field $\mathbb{F}$ in variables $X = (x_1, x_2, \ldots, x_n)$ is a finite linear combination (with coefficients in $\mathbb{F}$) of monomials.

$$f(X) := \sum_{\alpha} a_\alpha X^\alpha, \quad a_\alpha \in \mathbb{F},$$

where the sum is over a finite number of n-tuples $\alpha = (\alpha_1, \ldots, \alpha_n)$, a_α is the **coefficient** of a monomial X^α. If $a_\alpha \neq 0$, then we call $a_\alpha X^\alpha$ a **term** of the polynomial f. The **total degree** of the polynomial $f \neq 0$ is the maximum of $|\alpha|$ over the terms of f. The total degree of a zero polynomial is undefined. We denote the total degree of a polynomial f by $\deg(f)$.

Remark. The set of all polynomials in X over a field $\mathbb{F}$ is denoted by $\mathbb{F}[X]$, and it has the ring structure (with standard polynomial addition and multiplication). We call it a **polynomial ring** over a field $\mathbb{F}$.

Notational Remark. When dealing with polynomials in a small number of formal variables we will usually use variables x, y, z.

For example:

$$f(x, y, z) = 2x^2y^5 - 17x^5z^4.$$

f is a polynomial in $\mathbb{Z}[x, y, z]$ of a total degree, $\deg(f) = 9$.

Remark. Every polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ can be viewed as a function $f(x_1, \ldots, x_n) : \mathbb{F}^n \to \mathbb{F}$.

Definition 1.2.4. Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial, we say f has a **root** $r = (r_1, \ldots, r_n),\ r_1, \ldots, r_n \in \mathbb{F}$ if $f(r) = 0$. We may also view r as a vector in $\mathbb{F}^n$. We say that a field $\mathbb{F}$ is **algebraically closed** if every non-constant polynomial in $\mathbb{F}[x_1, \ldots, x_n]$ has a root in $\mathbb{F}^n$. For example, $\mathbb{C}$ is an algebraically closed field. On the other hand, $\mathbb{R}$ is not an algebraically closed field, because there exist polynomials with coefficients in $\mathbb{R}$ that have only complex roots, e.g. $f(x) = x^2 + 16$.

Definition 1.2.5. A polynomial $f \in \mathbb{F}[X]$ is called **symmetric** if and only if:

$$f(x_{i_1}, \ldots, x_{i_n}) = f(x_1, \ldots, x_n)$$

for every possible permutation $x_{i_1}, \ldots, x_{i_n}$ of the variables $x_1, \ldots, x_n$.

For example, polynomials $x^2 + y^2 + z^2$ and xyz in variables x, y, z are clearly symmetric.

Definition 1.2.6. A polynomial $f \in \mathbb{F}[X]$ is **homogeneous of total degree** $m \in \mathbb{Z}_{\geq 0}$ provided that every term of f has total degree m.

Remark. A polynomial $f \in \mathbb{F}[X]$ is symmetric if and only if all of its homogeneous components are symmetric.

Definition 1.2.7. Let $\mathbb{F}$ be a field, and let $f_1, \ldots, f_s,\ s \in \mathbb{N}$, be polynomials in $\mathbb{F}[x_1, \ldots, x_n]$. Then the set of their common zeroes:

$$\mathcal{V}(f_1, \ldots, f_s) := \{a \in \mathbb{F}^n \mid \forall k \in \{1, \ldots, s\} : f_k(a) = 0\},$$

is called the **affine variety** in $\mathbb{F}^n$ defined by polynomials $f_1, \ldots, f_s$.

Thus, an affine variety $\mathcal{V}(f_1, \ldots, f_s) \subseteq \mathbb{F}^n$ is the set of all solutions of the system of multivariate polynomial equations $f_1(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, x_n) = 0$ restricted to $\mathbb{F}^n$, in the case $\mathbb{F}^n$ is not an algebraically closed field, there might be some solutions that lie in an extension $\mathbb{F}^n$, but not in $\mathbb{F}^n$ itself.

For example consider the variety $\mathcal{V}(xz,\ yz)$ in $\mathbb{R}$, we can easily check that the set of all solutions to the polynomial system:

$$\begin{aligned} xz &= 0, \\ yz &= 0, \end{aligned}$$

is the union of the (x, y)-plane and the z-axis. For graphical illustration see figure 1.1.

Definition 1.2.8. Let R be a commutative ring, then any non-empty subset $I \subseteq R$ is called a (two-sided) **ideal** of R if it satisfies following requirements:

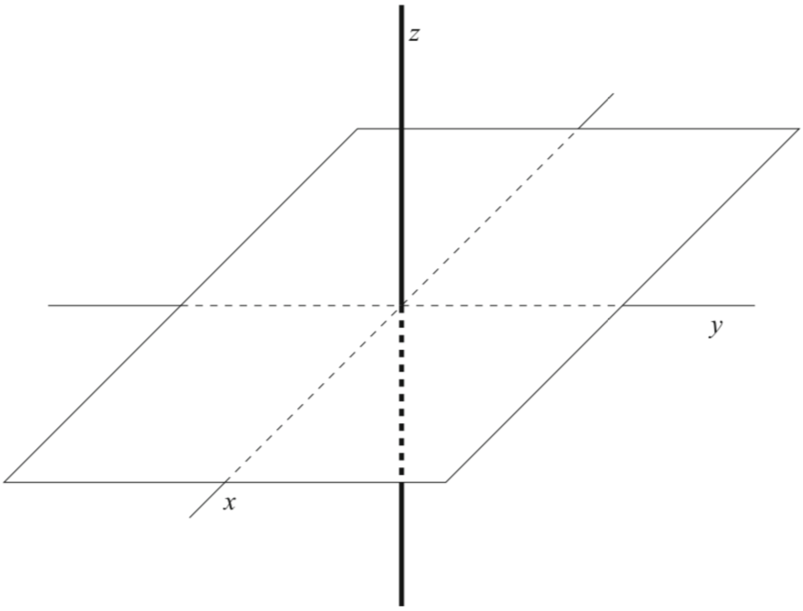

Figure 1.1: Affine variety defined by (xz, yz). Image source: ([1], page 9).

- $I \neq \emptyset$, $\qquad$ (I is a non-empty set)
- $\forall f, g \in I : (f + g) \in I$, $\qquad$ (I is closed under addition)
- $\forall f \in I,\ \forall h \in R : hf \in I.$ $\qquad$ (I is closed under multiplication by R)

In this thesis we are mostly concerned about ideals generated by a finite number of polynomials over some field.

Definition 1.2.9. Let $X = (x_1, \ldots, x_n)$ be an ordered n-tuple of formal variables and let $f_1, \ldots, f_s \in \mathbb{F}[X]$ be an s-tuple of polynomials. Then we set

$$\langle f_1, \ldots, f_x \rangle := \{\sum_{i=1}^{n} h_i f_i \mid h_1, \ldots, h_s \in \mathbb{F}[X]\}$$

to be the **ideal generated by** polynomials $f_1, \ldots, f_s$.

Remark. Every ideal I of $\mathbb{F}[X]$ is finitely generated, which means:

$$\exists s \in \mathbb{N},\ \exists f_1, \ldots, f_s \in \mathbb{F}[X] : I = \langle f_1, \ldots, f_s \rangle,$$

and we say that the polynomials $f_1, \ldots, f_s$ form a **basis** of I. Note that a given ideal I may have many different bases. If we have two different bases $B_1 = (f_1, \ldots, f_s),\ s \in \mathbb{N}$, and $B_2 = (g_1, \ldots, g_t),\ t \in \mathbb{N}$, of the same ideal I in

$\mathbb{F}[X]$, such that $I = \langle B_1 \rangle = \langle B_2 \rangle$, then the affine varieties in $\mathbb{F}^n$, defined by the bases B_1 and B_2, are the same.

$$\mathcal{V}(B_1) = \mathcal{V}(B_2).$$

Definition 1.2.10. Let $\mathcal{V} \subseteq \mathbb{F}^n$ be an affine variety and let $X = (x_1, \ldots, x_n)$ be an ordered n-tuple of formal variables. Then we set

$$\mathbf{I}(\mathcal{V}) := \{f \in \mathbb{F}[X] \mid \forall a \in \mathcal{V} : f(a) = 0\}.$$

to be the **ideal of affine variety** $\mathcal{V}$.

Remark. The natural question to ask is whether $\mathbf{I}(\mathcal{V}(f_1, \ldots, f_s)) = \langle f_1, \ldots, f_s \rangle$. The answer, unfortunately, is not always yes, but the following set inclusion holds:

$$\langle f_1, \ldots, f_s \rangle \subseteq \mathbf{I}(\mathcal{V}(f_1, \ldots, f_s)).$$

Definition 1.2.11. Let $f, g \in \mathbb{F}[x]$ be two non-constant polynomials of degrees $l, m \in \mathbb{Z}_{>0}$, $\deg(f) = l$, $\deg(g) = m$. Then f, g have a common factor in $\mathbb{F}[x]$ if and only if there are polynomials $A, B \in \mathbb{F}[x]$, such that:

1. $A \neq 0,\ B \neq 0,$
2. $\deg(A) \leq m - 1$, $\deg(B) \leq l - 1$,
3. $Af + Bg = 0$.

To decide whether polynomials f, g have a common factor, we can rewrite $Af + Bg = 0$ as a system of linear equations and find a non-zero solution.

$$\begin{aligned} A &= u_0 x^{m-1} + \cdots + u_{m-1}, \\ B &= v_0 x^{l-1} + \cdots + v_{l-1}, \\ f &= c_0 x^l + \cdots + c_l, \quad c_0 \neq 0, \\ g &= d_0 x^m + \cdots + d_m, \quad d_0 \neq 0. \end{aligned}$$

If we compare the coefficients of powers of x, then we get a system of linear equations with variables $u_i,\ i \in \{0, 1, \ldots, m-1\}$ and $v_j,\ j \in \{0, 1, \ldots, l-1\}$ and coefficients $c_i, d_j \in \mathbb{F}$. The coefficient matrix of this system is called the **Sylvester matrix** of f and g with respect to x, denoted by $\mathrm{Syl}_x(f, g)$.

$\mathrm{Syl}_x(f,g)$ is the following $(l+m)\times(l+m)$ matrix:

$$\mathrm{Syl}_x(f,g) := \begin{array}{c}\begin{pmatrix} c_0 & & & & d_0 & & & \\ c_1 & c_0 & & & d_1 & d_0 & & \\ c_2 & c_1 & \ddots & & d_2 & d_1 & \ddots & \\ \vdots & & \ddots & c_0 & \vdots & & \ddots & d_0 \\ & \vdots & & c_1 & & \vdots & & d_1 \\ c_l & & & & d_m & & & \\ & c_l & & \vdots & & d_m & & \vdots \\ & & \ddots & & & & \ddots & \\ & & & c_l & & & & d_m \end{pmatrix} \\ \underbrace{\hphantom{c_0\quad c_0\quad \ddots\quad c_0}}_{m\text{ columns}}\quad\underbrace{\hphantom{d_0\quad d_0\quad \ddots\quad d_0}}_{l\text{ columns}}\end{array},$$

where the empty spaces are filled by zeros.

The determinant (we expect our reader is familiar with this term, if not, you can find its definition in any decent linear algebra textbook) of the Sylvester matrix is called the **resultant** of polynomials f and g with respect to x, and is denoted by $\mathrm{Res}_x(f,g)$. Furthermore, f,g have a common factor in $\mathbb{F}[x]$ if and only if $\mathrm{Res}_x(f,g)=0$, which is equivalent to the above-presented system of linear equations having a non-zero solution. An example of the resultant of two quadratic polynomials is shown on page 40.

If f,g have a common factor $h\in\mathbb{F}[x]$, $\deg(h)\geq 1$, then there exist $f_1,g_1\in\mathbb{F}[x]$, such that:

$$f = hf_1, \quad g = hg_1.$$

Moreover, if $\mathbb{F}$ is an algebraically closed field, polynomials f,g have a common root $r\in\mathbb{F}$. Since $\mathbb{F}$ is algebraically closed field, a (non-constant) common factor h has a root $r\in\mathbb{F}$: $h(r)=0$. Therefore, r is a common root of polynomials f,g:

$$(hf_1)(r) = h(r)f_1(r) = 0f_1(r) = 0 \Leftrightarrow f(r) = 0,$$
$$(hg_1)(r) = h(r)g_1(r) = 0g_1(r) = 0 \Leftrightarrow g(r) = 0.$$

1.2.1 Monomial Ordering

The notion of ordering of terms in a polynomial is a key ingredient in many algorithms, e.g. the long division of polynomials. When dealing with polynomials in only one variable, we usually write the terms of the polynomial in the decreasing order by their monomial degree.

For example, $f(x) = 2x^4 - 10x^3 + x^2 + x - 12$. The degree ordering on the one-variable monomials is straightforward:

$$\cdots > x^{m+1} > x^m > x^{m-1} \cdots > x^2 > x > 1$$

We would like to establish an ordering on the terms in polynomials in $\mathbb{F}[X]$, where $X = (x_1, \dots, x_n)$. First, we note that we can reconstruct the monomial $X^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ from the n-tuple of exponents $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$. Based on this observation, we define an ordering $>$ on the space $\mathbb{Z}^n_{\geq 0}$ which also gives us an ordering on the monomials $\in \mathbb{F}[X]$. If for some $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ and some ordering $>$ holds: $\alpha > \beta$ we also say that $X^\alpha > X^\beta$. In this thesis, we only consider **total orderings**, which means that for every pair of monomials X^α and X^β, exactly one of the three statements holds:

- $X^\alpha > X^\beta$, (when $\alpha > \beta$)
- $X^\alpha = X^\beta$, (when $\alpha = \beta$)
- $X^\alpha < X^\beta$, (when $\alpha < \beta$)

and $>$ is transitive:

$$\forall \alpha, \beta, \gamma \in \mathbb{Z}^n_{\geq 0} : (X^\alpha > X^\beta \wedge X^\beta > X^\gamma) \implies X^\alpha > X^\gamma.$$

We also require that multiplication of two polynomials does not change the relative order of terms. Therefore, the following property for $>$ must hold:

$$\forall \alpha, \beta, \gamma \in \mathbb{Z}^n_{\geq 0} : X^\alpha > X^\beta \implies X^\alpha X^\gamma > X^\beta X^\gamma.$$

Which in terms of the exponent vectors means:

$$\forall \alpha, \beta, \gamma \in \mathbb{Z}^n_{\geq 0} : \alpha > \beta \implies \alpha + \gamma > \beta + \gamma.$$

To summarize all the requirements, we make the following definition.

Definition 1.2.12. A **monomial ordering** $>$ on $\mathbb{F}[X]$, where $X = (x_1, \dots, x_n)$ is a relation $>$ on $\mathbb{Z}^n_{\geq 0}$ satisfying:

- $>$ is a total order on $\mathbb{Z}^n_{\geq 0}$,
- $\forall \alpha, \beta, \gamma \in \mathbb{Z}^n_{\geq 0} : \alpha > \beta \implies \alpha + \gamma > \beta + \gamma$,
- $\forall A \subseteq \mathbb{Z}^n_{\geq 0},\ A \neq \emptyset : \exists \alpha \in A,\ \forall \beta \in A \setminus \{\alpha\} : \beta > \alpha$.

The last requirement tells us, that in every non-empty subset of $\mathbb{Z}^n_{\geq 0}$ there exists a minimum element under the relation $>$.

Definition 1.2.13. Let $\alpha = (\alpha_1, \ldots, \alpha_n),\ \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. **Lexicographic Order** (**lex**), denoted by $>_{lex}$, is a generalisation of the way words are ordered in a dictionary. We say $\alpha >_{lex} \beta$ if the leftmost non-zero entry of the vector difference $\alpha - \beta \in \mathbb{Z}^n$ is positive. We write: $X^\alpha >_{lex} X^\beta$ if $\alpha >_{lex} \beta$.

For example:

- $(10, 4, 3) >_{lex} (10, 3, 4)$, since $\alpha - \beta = (0, 1, -1)$.
- $(7, 5, 3, 1) >_{lex} (7, 5, 2, 4)$, since $\alpha - \beta = (0, 0, 1, -3)$.
- The variables $x_1, \ldots, x_n$ are ordered in the usual way by the lexicographic order:

$$(1, 0, \ldots, 0) >_{lex} (0, 1, 0, \ldots, 0) >_{lex} \cdots >_{lex} (0, \ldots, 0, 1),$$

so $x_1 >_{lex} x_2 >_{lex} \cdots >_{lex} x_n$.

In the rest of this thesis, we assume $x >_{lex} y >_{lex} z$, unless stated otherwise.

Definition 1.2.14. Let $\alpha = (\alpha_1, \ldots, \alpha_n),\ \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. **Graded Lexicographic Order** (**grlex**), denoted by $>_{grlex}$, at first orders the terms by the total degree, then break ties using the standard lexicographic order defined above.

$$\alpha >_{grlex} \beta : (|\alpha| > |\beta|) \vee (|\alpha| = |\beta| \wedge \alpha >_{lex} \beta),$$

where $|\alpha| = \sum_{i=1}^n \alpha_i$ and $|\beta| = \sum_{i=1}^n \beta_i$.

- $(10, 2, 6) >_{grlex} (10, 3, 4)$, since $|\alpha| = 18 > |\beta| = 17$.
- $(7, 5, 3, 1) >_{grlex} (7, 5, 2, 4)$, since $|\alpha| = 16 = |\beta|$ and $\alpha >_{lex} \beta$.
- The variables $x_1, \ldots, x_n$ are ordered in the same way as by $>_{lex}$ order:

$$(1, 0, \ldots, 0) >_{grlex} (0, 1, 0, \ldots, 0) >_{grlex} \cdots >_{grlex} (0, \ldots, 0, 1),$$

Definition 1.2.15. Let $\alpha = (\alpha_1, \ldots, \alpha_n),\ \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. **Graded Reverse Lexicographic Order** (**grevlex**), denoted by $>_{grevlex}$, is somehow less intuitive order, but it is usually the most efficient for computations. We say $\alpha >_{grevlex} \beta$ if $|\alpha| > |\beta|$ or if $|\alpha| = |\beta|$ and the rightmost non-zero entry of vector difference $\alpha - \beta \in \mathbb{Z}^n$ is negative.

- $(4, 7, 1) >_{grevlex} (4, 2, 5)$, since $|\alpha| = 12 > |\beta| = 11$.
- $(7, 5, 1, 3) >_{grevlex} (1, 5, 3, 7)$, since $|\alpha| = 16 = |\beta|$,
  and $\alpha - \beta = (6, 0, -2, -4),\ -4 < 0$.

- The variables $x_1, \dots, x_n$ are ordered in the same way as by $>_{lex}$ order:

$$(1, 0, \dots, 0) >_{grevlex} (0, 1, 0, \dots, 0) >_{grevlex} \cdots >_{grevlex} (0, \dots, 0, 1),$$

Now we show, how would the polynomial $f(x, y, z) = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in \mathbb{Z}[x, y, z]$ be written, if we reorder its terms by a monomial order in decreasing order:

- With respect to the lex order:

$$f(x, y, z) = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2.$$

- With respect to the grlex order:

$$f(x, y, z) = 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2.$$

- With respect to the grevlex order:

$$f(x, y, z) = 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2.$$

  The first two terms have the same total degree of 4 and $xy^2z >_{grevlex} x^2z^2$ because $(1, 2, 1) - (2, 0, 2) = (-1, 2, -1)$ and $-1 < 0$.

Definition 1.2.16. Let $f = \sum_\alpha a_\alpha X^\alpha$ be a non-zero polynomial in $\mathbb{F}[X]$, and let $>$ be a monomial order.

- The **multidegree** of f is:

$$\text{multideg}(f) := \max(\alpha \in \mathbb{Z}^n_{\geq 0} \mid a_\alpha \neq 0),$$

  the maximum is taken with respect to $>$.

  Let $g \in \mathbb{F}[X],\ g \neq 0$, then $\text{multideg}(fg) = \text{multideg}(f) + \text{multideg}(g)$. If $(f + g) \neq 0$, then $\text{multideg}(f + g) \leq \max(\text{multideg}(f),\ \text{multideg}(g))$, more precisely if the multidegrees of f and g are not equal, then the equality occurs: $\text{multideg}(f + g) = \max(\text{multideg}(f),\ \text{multideg}(g))$.

- The **leading coefficient** of f is:

$$\text{LC}(f) := a_{\text{multideg}(f)} \in \mathbb{F}.$$

- The **leading monomial** of f is:

$$\text{LM}(f) := X^{\text{multideg}(f)} \in \mathbb{F}[X],$$

  with coefficient 1.

- The **leading term** of f is:

$$\mathrm{LT}(f) := (\mathrm{LC}(f) \cdot \mathrm{LM}(f)) \in \mathbb{F}[X].$$

To illustrate that, let $f(x,y,z) = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in \mathbb{Z}[x,y,z]$ as before and lets use $>_{grevlex}$ order.

$$\begin{aligned} f(x,y,z) &= 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2, \text{ (in grevlex order)} \\ \mathrm{multideg}(f) &= (1,2,1), \\ \mathrm{LC}(f) &= 4, \\ \mathrm{LM}(f) &= xy^2z, \\ \mathrm{LT}(f) &= 4xy^2z. \end{aligned}$$

Now we can formulate the idea of a general division algorithm in $\mathbb{F}[X]$.

Remark. Let $p, q \in \mathbb{F}[X]$ be two monomials, we say the monomial p is **divisible** by the monomial q if and only if there exists a monomial $h \in \mathbb{F}[X]$, such that: $p = qh$. We denote it by $q \mid p$ which we read as **q divides p**.

Definition 1.2.17. Let $>$ be a monomial order on $\mathbb{Z}^n_{\geq 0}$, let $F = (f_1, \ldots, f_s)$ be an ordered s-tuple of polynomials in $\mathbb{F}[X]$, where $X = (x_1, \ldots, x_n)$. Then every $f \in \mathbb{F}[X]$ can be written as:

$$f = q_1 f_1 + \cdots + q_s f_s + r,$$

where $q_i, r \in \mathbb{F}[X]$, and either $r = 0$ (is a zero polynomial) or r is a linear combination, with coefficients in $\mathbb{F}$, of monomials $\in \mathbb{F}[X]$, none of those monomials is divisible by any of $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$. We call polynomial r a **remainder** of f on division by F. Furthermore, if $q_i f_i \neq 0$, then

$$\mathrm{multideg}(f) \geq \mathrm{multideg}(q_i f_i).$$

We won't describe the division algorithm itself in this thesis. If you are not familiar with this algorithm, please refer to [1] on pages 61-68, where the algorithm is discussed in great detail.

Unfortunately, the remainder is not uniquely characterised and depends on the order of the divisors in the set F, and also on the monomial order itself.

Furthermore, we would like to use this idea to answer the ideal membership problem. Let $f, f_1, \ldots, f_s \in \mathbb{F}[X]$ and let $I = \langle f_1, \ldots, f_s \rangle$ be an ideal. We would like to determine whether $f \in I$ is true. We can clearly state, that if the remainder r obtained after division of f by $F = (f_1, \ldots, f_s)$ is 0, then f has to be an element of the ideal I. So $r = 0$ is a sufficient condition for the ideal membership. However, it isn't a necessary condition for f being in the ideal. To remedy this situation, we try to describe a "good" basis of the ideal I, such that the remainder r on division by the polynomials of this basis is uniquely determined, and that the condition $r = 0$ is equivalent to the membership in the ideal. Exactly those good properties have Gröbner bases, which we describe in the following section.

1.3 Gröbner Bases

Gröbner bases may be used to solve many problems about polynomial ideals in an algorithmic or computational fashion. It is one of the most used methods for solving systems of multivariate polynomial equations, i.e. calculating the affine variety defined by those polynomial equations. This section is based on [1].

Definition 1.3.1. An ideal $I \subseteq \mathbb{F}[X]$ is called a **monomial ideal** if there exists a (possibly infinite) subset $A \subseteq \mathbb{Z}^n_{\geq 0}$, such that I consists of all polynomials which are finite sums: $\sum_{\alpha \in A} h_\alpha X^\alpha$, where $h_\alpha \in \mathbb{F}[X]$. We can then write I in the form: $I = \langle X^\alpha \mid \alpha \in A \rangle$. Monomial $X^\beta, \beta \in \mathbb{Z}^n_{\geq 0}$, lies in the ideal I if and only if there exist $\alpha \in A$, such that $X^\alpha \mid X^\beta$ (X^β is divisible by some X^α).

Remark. **(Dickson's Lemma).** Any monomial ideal $I = \langle X^\alpha \mid \alpha \in A \rangle \subseteq \mathbb{F}[X]$ can be written in the form $I = \langle X^{\alpha(1)}, \dots, X^{\alpha(s)} \rangle,\ s \in \mathbb{N}$, where $\alpha(1), \dots, \alpha(s) \in A$. In particular, I has a finite basis $(X^{\alpha(1)}, \dots, X^{\alpha(s)})$.

Definition 1.3.2. A monomial ideal $I \subseteq \mathbb{F}[X]$ has a finite basis $(X^{\alpha(1)}, \dots, X^{\alpha(s)})$ with the property that $X^{\alpha(i)}$ does not divide $X^{\alpha(j)}$ for any $i \neq j$. Furthermore, this basis is unique and is called the **minimal basis** of I.

Definition 1.3.3. Let $I \subseteq \mathbb{F}[X],\ I \neq 0$, be an ideal and fix a monomial order on $\mathbb{F}[X]$. Then:

- We denote by $\mathrm{LT}(I)$ the **set of leading terms** of non-zero elements of I.
$$\mathrm{LT}(I) = \{cX^\alpha \mid \exists f \in I \setminus \{0\} : \mathrm{LT}(f) = cX^\alpha\}.$$
- We denote by $\langle \mathrm{LT}(I) \rangle$ the **ideal of leading terms** of I. $\langle \mathrm{LT}(I) \rangle$ is a monomial ideal, therefore there exist a finite set $g_1, \dots, g_t \in I,\ t \in \mathbb{N}$, such that:
$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_t) \rangle.$$

Definition 1.3.4. Fix a monomial order on $\mathbb{F}[X]$, therefore every polynomial $f \in \mathbb{F}[X]$ has a unique leading term. A finite subset $G = \{g_1, \dots, g_t\}$ of an ideal $I \subseteq \mathbb{F}[X],\ I \neq \{0\}$ is said to be a **Gröbner basis** (or **standard basis**) if:

$$\langle \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle.$$

Additionally, we define the Gröbner basis of the zero ideal $\{0\}$ to be the empty set $\emptyset$ using the convention that $\langle \emptyset \rangle = \{0\}$.

Remark. Every ideal $I \subseteq \mathbb{F}[X]$ has a Gröbner basis. Furthermore, any Gröbner basis for an ideal I is a basis of I. Gröbner bases for ideals in polynomial rings were introduced by B. Buchberger in his PhD thesis (1965) [4] and named by him in honour of his thesis's advisor W. Gröbner. Buchberger also developed fundamental algorithms to find and work with Gröbner bases. In many computer algebra systems, there is usually used an alternative spelling ”Groebner bases”.

Now we will mention few important properties of Gröbner bases.

Remark. Let $I \subseteq \mathbb{F}[X]$ be an ideal and let $G = \{g_1, \dots, g_t\}$ be a Gröbner basis of I. Then for any $f\mathbb{F}[X]$, there is a unique polynomial r with those two properties:

- No term of r is divisible by any of $\mathrm{LT}(g_1), \dots$,$\mathrm{LT}(g_t)$.
- $\exists g \in I :\ f = g + r$. In particular, r is the remainder on division of f by set G no matter, how are the elements of G listed, when using the division algorithm.

Polynomial r is called the **normal form** of f.

Polynomial $f \in I$ if and only if the remainder r on division f by G is zero, $r = 0$.

Definition 1.3.5. Let $f \in \mathbb{F}[X]$ be a polynomial and let $F = (f_1, \dots, f_s) \subseteq \mathbb{F}[X]$ be an ordered s-tuple of polynomials. We will denote the remainder on the division of f by F by $\overline{f}^F$. If F is a Gröbner basis for $\langle f_1, \dots, f_s \rangle$, then we can regard F as a set without any particular order, because the remainder on the division by a Gröbner basis is unique.

Definition 1.3.6. Let $f, g \in \mathbb{F}[x_1, \dots, x_n]$ be non-zero polynomials. Let $\alpha = \mathrm{multideg}(f)$ and $\beta = \mathrm{multideg}(g)$, then $\gamma = (\gamma_1, \dots, \gamma_n)$, where $\gamma_i = \max(\alpha_i, \beta_i)$ for each $i \in \{1, \dots, n\}$. We call X^γ the **least common multiple** of $\mathrm{LM}(f)$ and $\mathrm{LM}(g)$, denoted by $X^\gamma = \mathrm{lcm}(\mathrm{LM}(f), (\mathrm{LM}(g))$.

The **S-polynomial** of f and g is the combination:

$$\mathrm{S}(f, g) := \frac{X^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{X^\gamma}{\mathrm{LT}(g)} \cdot g.$$

For example, let $f = x^3y^2 - x^2y^3 + x$ and $g = 3x^4y + y^2$ in $\mathbb{R}[x,y]$ with grlex order. Then $\gamma = (4,2)$ and

$$\begin{aligned} \mathrm{S}(f,g) &= \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g \\ &= x \cdot f - \frac{1}{3}y^3 \cdot g \\ &= -x^3y^3 + x^2 - \frac{1}{3}y^3. \end{aligned}$$

An S-polynomial is "designed" to produce cancellation of the leading terms.

Definition 1.3.7. (Buchberger's Criterion): Let I be a polynomial ideal. Then a basis $G = \{g_1, \ldots, g_t\}$ of I is a Gröbner basis of I if and only if for all pairs $i \neq j$, the remainder on division by $\mathrm{S}(g_i, g_j)$ by G (listed in some order) is zero.

Based on this criterion, there is the Buchberger's algorithm (described on page 91 in [1]), that computes the Gröbner basis.

Definition 1.3.8. A **reduced Gröbner basis** for a polynomial ideal I is a Gröbner basis G for I such that:

- $\forall p \in G : \mathrm{LC}(p) = 1.$
- $\forall p \in G$: no monomial p lies in $\langle \mathrm{LT}(G \setminus \{p\}) \rangle$.

Any polynomial ideal $I \neq \{\emptyset\}$ for a given monomial order has a unique reduced Gröbner basis.

Now we describe, how to use Gröbner bases for finding all the solutions of a system of multivariate polynomial equations.

Definition 1.3.9. Given ideal $I = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$, the l-th **elimination ideal** I_l is the ideal of $\mathbb{F}[x_{l+1}, \ldots, x_n]$ defined by:

$$I_l := I \cap \mathbb{F}[x_{l+1}, \ldots, x_n].$$

Note that different orderings of the variables lead to different elimination ideals.

Definition 1.3.10. (The Elimination Theorem). Let $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be an ideal and let G be a Gröbner basis of I with respect to lex order where $x_1 > x_2 > \cdots > x_n$. Then, for every $0 \leq l \leq n$, the set:

$$G_l := G \cap \mathbb{F}[x_{l+1}, \ldots, x_n]$$

is a Gröbner basis of the l-th elimination ideal I_l.

To find all the points in the affine variety $\mathcal{V}(I)$, we build up the solutions one coordinate at a time. At first, we find the affine variety $\mathcal{V}(I_{n-1})$, which is equivalent to finding the roots of a univariate polynomial in $\mathbb{F}[x_n]$. We call any solution $(a_n) \in \mathcal{V}(I_{n-1})$ a **partial solution** of the original system of equations. Next step is to extend a partial solution (a_n) to a partial solution $(a_{n-1}, a_n) \in \mathcal{V}(I_{n-2})$. To do that, we substitute (a_n) into all the polynomial equations in I_{n-2}. Thereafter, we obtain a univariate polynomial equation in $\mathbb{F}[x_{n-1}]$, which we can conveniently solve. Note that not every partial solution in $\mathcal{V}(I_{n-1})$ extends to a partial solution in $\mathcal{V}(I_{n-2})$. We repeat this process until we find $\mathcal{V}(I_0) = \mathcal{V}(I)$, a set of all **complete solutions** to the original system of equations.

Chapter 2

Elliptic Curves and the Discrete Logarithm Problem

In this chapter, we revise the theory of elliptic curves and state the elliptic curve discrete logarithm problem (ECDLP). In the last section, we also introduce the reader to the concept of summation polynomials, which are the primary building block in many specialised algorithms (exploiting the particular group structure) solving the ECDLP. Examples of such algorithms are discussed in detail in chapter 3.

2.1 Elliptic Curves

This section focuses on elliptic curves over finite fields and groups of points on them. At first, we define what is a general elliptic curve. Afterwards, we show how to define an Abelian group on the set of points of an elliptic curve. This section is based mostly on [2].

Definition 2.1.1. An **elliptic curve** over a (prime order) finite field $GF(p)$, $p > 3,\ p$ prime, defined by the short Weierstrass equation, is a set:

$$E(GF(p)) := \{(x, y) \mid x, y \in \mathbb{F},\ y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\},$$

where $A, B \in GF(p)$ are **coefficients of the elliptic curve**. Coefficients A, B have to satisfy the following condition: $4A^3+27B^2 \neq 0$, which guarantees the right-hand side polynomial $f(x) = x^3 + Ax + B$ has 3 distinct roots. Elliptic curves are **non-singular** curves, i.e. they don't have any cusps nor self-intersections.
Point $\mathcal{O}$ is called the **point at infinity** (in the projective plane).

Definition 2.1.2. Let $E(GF(p))$ be an elliptic curve, and let $P, Q \in E(GF(p))$, $P = (x_1, y_1),\ Q = (x_2, y_2)$ be two points on the elliptic curve E. We define the binary operation $\oplus : E(GF(p)) \times E(GF(p)) \to E(GF(p))$, called **addition on the elliptic curve** $E(GF(p))$, as follows:

- Point at infinity $\mathcal{O}$ is an identity element of the operation $\oplus$, therefore if $P = \mathcal{O},\ P \oplus Q = Q$, or if $Q = \mathcal{O},\ P \oplus Q = P$.

- Else if $x_1 = x_2$ and $P \neq Q$, $P \oplus Q = \mathcal{O}$. Point at infinity $\mathcal{O}$ is the identity element of the operation $\oplus$. Therefore, point Q is the **additive inverse** of the point P, denoted by $\ominus P$. We now state the explicit formula for the point $\ominus P$, we know its x-coordinate is x_1, and we use the E equation and substitute X with x_1:

$$Y^2 = (x_1^3 + Ax_1 + B),$$

  which is a quadratic equation in the variable Y. We already know one of its roots y_1, the other root has to be $-y_1$. Therefore:

$$\ominus P = (x_1, -y_1).$$

- Else if $x_1 \neq x_2$, let λ be the slope of the line defined by the points P, Q.

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

  Else if $P = Q$ (**point doubling**), let λ be the slope of the tangent line to the elliptic curve equation at the point P.

$$\lambda = \frac{\frac{\mathrm{d}E}{\mathrm{d}X}}{\frac{\mathrm{d}E}{\mathrm{d}Y}}(x_1, y_1) = \frac{3x_1^2 + A}{2y_1},$$

  where $\frac{\mathrm{d}E}{\mathrm{d}X}, \frac{\mathrm{d}E}{\mathrm{d}Y}$ are the derivatives of the elliptic curve equation with respect to X, Y.

  The result of the operation $\oplus$ is:

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= \lambda(x_1 - x_3) - y_1, \\ P \oplus Q &= (x_3, y_3). \end{aligned}$$

Definition 2.1.3. A set of points on the elliptic curve defined by the short Weierstrass equation and the binary operation $\oplus$ form an Abelian group, $(E(GF(p)), \oplus)$ is a group, and we denote it by $E(p)$. If we want to explicitly mention the coefficients A, B we use $E_{A,B}(p)$.

Notational Remark. Let $P \in E(p)$ be a point on an elliptic curve E over $GF(p)$. To shorten the notation of the repeated application of the group law, we use the notation introduced in chapter 1. To remind our readers;

multiplication of a point on the elliptic curve E by an integer t has the following meaning:

$$\forall P \in E(p),\ \forall t \in \mathbb{Z} : tP := \begin{cases} \underbrace{P \oplus P \oplus \cdots \oplus P}_{t\text{-times}} & t > 0, \\ \mathcal{O} \text{ (identity element)} & t = 0, \\ \underbrace{(\ominus P) \oplus (\ominus P) \oplus \cdots \oplus (\ominus P)}_{t\text{-times}} & t < 0. \end{cases}$$

2.1.1 Complexity of the Arithmetic Operations on an Elliptic Curve

The complexity of arithmetic operations on E is based on the complexity of operations in the underlying finite field $GF(p)$. The exact number of arithmetic operations depends on the used algorithm, its implementation, and on the architecture of the CPU, where the particular code is executed. Table 2.1 provides a brief summary of the relationship between the operations on elliptic curve E and the number of arithmetic operations in the underlying finite field $GF(p)$. Addition in $GF(p)$ is denoted by $+_p$, multiplication in $GF(p)$ is denoted by $\cdot_p$, and the last column is the number of multiplicative inverses in $GF(p)^\times$.

	$\# +_p$	$\# \cdot_p$	# mult. inverses
$\ominus P$	1	0	0
$P \oplus Q, P \neq Q$	6	3	1
$P \oplus Q, P = Q$	5	5	1
$tP,\ t \in \mathbb{Z}_{\geq 0},\ k = \lceil \log_2(t) \rceil$	$(5k + 0.5k)$[1]	$5k$	0

Table 2.1: Complexity of arithmetic operations on the elliptic curve E over a finite field $GF(p)$.

We denote the number of bits of p by $n = \lceil \log_2(p) \rceil$, then addition in $GF(p)^+$ is asymptotically $O(n)$, multiplication in $GF(p)^\times$, using Montgomery method [5], is $O(n^2)$ and calculation of a multiplicative inverse in $GF(p)^\times$, using a careful implementation of the extended Euclidean algorithm (EEA) [5], is $O(n^2)$. An alternative to the EEA, for calculating a multiplicative inverse in $GF(p)^\times$, is based on (Lagrange's) theorem 1.1.5.

$$\begin{aligned} \forall a \in GF(p)^\times,\ \exists n \in \mathbb{N} : \#a \cdot n = \#GF(p)^\times = p - 1, \\ \forall a \in GF(p)^\times,\ \forall n \in \mathbb{N} : a^{\#a \cdot n} = 1 \implies a^{\#a \cdot n - 1} = a^{-1}, \\ \forall a \in GF(p)^\times : a^{-1} = a^{p-2}. \end{aligned}$$

[1] Using signed binary expansion of t for the double-and-add algorithm, see [2] page 105.

To calculate a^{p-2}, we can use the standard algorithm, called square-and-multiply, for details see [2], which has the same complexity $O(n^2)$ as the EEA.

2.2 Discrete Logarithm Problem

Let $y = b^x$, given $y \in \mathbb{R}_{>0}$ and the base $b \in \mathbb{R}_{>0}$, we are asked to find the exponent $x \in \mathbb{R}$. We can rewrite this problem from the exponential form to the logarithmic form, i.e. $x = \log_b(y)$. To find the x we can easily evaluate it on a calculator (using change of logarithm basis rule). Even if we didn't know the inverse function (logarithm), the exponential function is a strictly increasing function. Therefore, we could have just guessed a random initial solution x_0, evaluate b^{x_0}, compare it with y. And based on the result of this comparison, we would have immediately known, whether the true solution x is greater, equal, or less than x_0. Therefore, we can solve this problem effortlessly over the real numbers.

If we were asked to solve the same problem in a finite group instead, the situation would be significantly more complicated.

Definition 2.2.1. Let $G = (M, \cdot)$ be an Abelian group and let $h = g^x$, given $h \in M$ and the base $g \in M$, $\langle g \rangle = G$, we are asked to find the exponent $x \in \{0, 1, \dots, \#G - 1\}$. We call x the **discrete logarithm** of h with respect to the base g, and denote it by $x = \log_g(h)$. Problem of finding the solution x is therefore called the **discrete logarithm problem** (DLP). We require g to be a generator of G, in order to guarantee the existence of the solution to the DLP.

To illustrate the difficulty of solving the DLP. Lets consider the multiplicative group G of the finite field $GF(19)$. $G = (\{1, 2, \dots, 18\}, \cdot_{19})$ and its generator $g = 3,\ g \in G$. Group structure is shown on the figure 2.1. We might be asked to find such k, that $3^k \equiv 4 \pmod{19}$. Unfortunately, the function $g^k \pmod{19}$, $k \in \mathbb{N}$, isn't monotonic, therefore we can't use the idea of trying a randomly selected k_0 and comparing $3^{k_0} \pmod{19}$ with 4, but we can use the fact that the group G is finite and its order is $\#G = 18 \implies 3^{18} \equiv 1 \pmod{19}$. We can just try all possible values of $k \in \{0, 1, \dots, 17\}$ and find the answer.

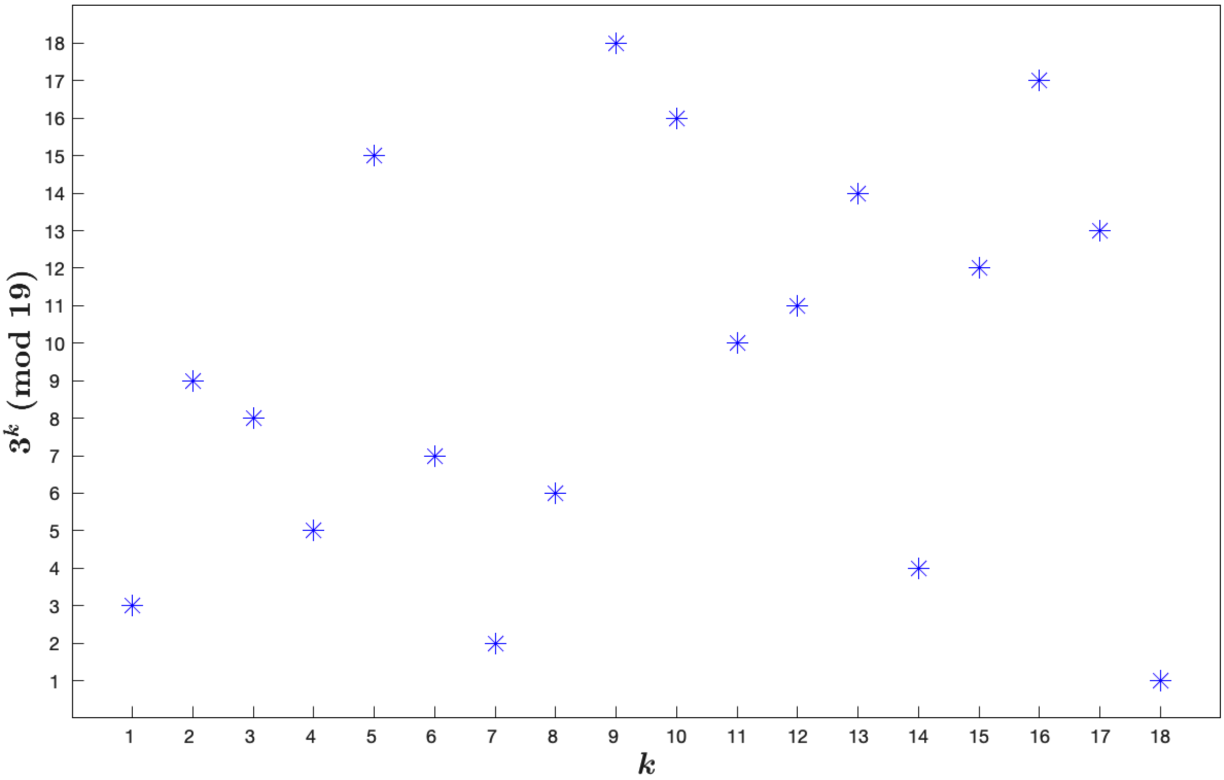

Figure 2.1: Powers of the generator $g = 3$ in $GF(19)^\times$. Image was created by the author himself.

This method is called the **brute-force attack**.

$$\begin{aligned} 3^0 &\equiv 1 \pmod{19} \not\equiv 4 \pmod{19}, \\ 3^1 &\equiv 3 \pmod{19} \not\equiv 4 \pmod{19}, \\ 3^2 &\equiv 9 \pmod{19} \not\equiv 4 \pmod{19}, \\ 3^3 &\equiv 8 \pmod{19} \not\equiv 4 \pmod{19}, \\ &\vdots \quad \vdots \\ 3^{13} &\equiv 14 \pmod{19} \not\equiv 4 \pmod{19}, \\ 3^{14} &\equiv 4 \pmod{19}. \end{aligned}$$

The solution of this DLP is therefore $k = 14$ and we can see that the brute-force approach is very lengthy even for DLP in groups of small order. Complexity of solving the DLP in a group G using the brute-force attack is $O(\#G)$ of group operations.

Remark. Standard properties of the logarithm may be used in the discrete logarithm case as well. Let G be a finite Abelian group and let g be a generator of G.

- $\forall p, q \in G : \log_g(pq) \equiv log_g(p) + log_g(q) \pmod{\#G}$,
- $\forall p, q \in G : \log_g(p(q)^{-1}) \equiv log_g(p) - log_g(q) \pmod{\#G}$,
- $\forall k \in \mathbb{Z},\ p \in G : \log_g(p^k) \equiv k \cdot log_g(p) \pmod{\#G}$,
- $h \in G,\ \langle h \rangle = G,\ \forall p \in G : log_g(p) \equiv log_h(p) \cdot log_g(h) \pmod{\#G}$.

Last property is the well-known change-of-base formula and tells us that if we are able to effectively solve the DLP with respect to some base we can use it to effectively solve the DLP with respect to any other base.

Discrete logarithm problem can be stated in any group, the difficulty of solving it greatly depends on the group structure and the group operation. To solve the DLP we can develop a generic algorithm that works in any group and doesn't explore the group structure, or we can develop a specific algorithm for a chosen type of a group. For example, in an additive group $(\{0, 1, \ldots, p-1\}, +_p)$, p prime, we can solve the DLP in $O(\log^2(p))$ time using the extended Euclidean algorithm. Shoup proved that a generic algorithm to solve the DLP in a generic group of prime order p would have to do $O(\sqrt{p})$ group operations [6]. The best general algorithm to match this lower bound is Pollard's ρ (rho) algorithm, described in the subsection **??**.

The main focus of this thesis is to solve the DLP stated on an elliptic curve using a specific algorithm.

Definition 2.2.2. Let E be an elliptic curve over a prime field $GF(p)$, let P be a generator of E and let Q be a second point on E. **Elliptic curve discrete logarithm problem** (ECDLP) is to find an integer $k \in \{1, 2, \ldots, \#E\}$ such that $Q = kP$.

2.3 Generic Algorithms for Solving ECDLP

In this section we will describe three most known generic algorithms for solving the DLP, we will use the elliptic curve notation. The first algorithm is based on collision finding, time complexity is lower than for a naive brute-force algorithm, but we the memory requirements are significant. This section was based mostly on [2].

2.3.1 Baby-step Giant-step Algorithm (BsGs)

Definition 2.3.1. (Baby-step Giant-step): Let E be an elliptic curve group over $GF(p)$, equipped with operation $\oplus$, $P \in E$ its generator and $xP = Q \in G,\ x \in \{0, 1, \dots, \#E - 1\}$, we will denote the order of E by $N = \#E$. We know, based on Hasse's theorem (**??**), for large p, N is approximately p. Following algorithm solves the ECDLP in $O(\sqrt{N})$ group operations $\oplus$.

- Let $n = \left\lceil \sqrt{N} \right\rceil$, we will pre-compute a list of length n of multiples of P.
- $0P = \mathcal{O}, P, 2P, \dots, (n-1)P,$ (baby-step phase) next generate multiples of Q and try to find it in the list generated in the baby-step phase.
- $Q \oplus (0 \cdot n \ominus P) = Q, Q \oplus (1 \cdot n \ominus P), Q \oplus (2 \cdot n \ominus P), \dots, Q \oplus ((n-1) \cdot n \ominus P),$ This is called the giant-step phase.
- If there is a collision for some iP and $Q \oplus (j \cdot n \ominus P)$, we can solve the ECDLP and find x:

$$\begin{aligned} iP = Q \oplus (j \cdot n \ominus P) \implies & i \equiv x + (-jn) \pmod N \\ & x \equiv i + jn \pmod N. \end{aligned}$$

The algorithm is deterministic and is guaranteed to find the solution, because it basically tries all the possible values of x. Every number in $\{0, 1, \dots, N-1\}$ can be expressed as $i + jn,\ n = \left\lceil \sqrt{N} \right\rceil, i, j \in \{0, 1, \dots, n-1\}$. For the efficient implementation it's crucial to be able to effectively find a collision in the pre-computed list, therefore it's advisable to use a hash table, to achieve the constant time lookup. If that is satisfied the algorithm time complexity is $O(\sqrt{N})$ of group operations and space complexity is $O(\sqrt{N})$.

For example, let $E = E(1, 1, 29)$ be an elliptic curve group over $GF(29)$ and its elliptic curve equation is $y^2 = x^3 + x + 1$. Let $P = (24, 25)$ be a generator of E, let $Q \in E$, we want to find an integer x such that: $Q = xP$. Order of E is 36, so we will set $n = 6$ and pre-calculate the baby-step list:

i	0	1	2	3	4	5
iP	$\mathcal{O}$	$(24, 25)$	$(6, 7)$	$(0, 28)$	$(10, 24)$	**(28,12)**

This step depends only on the group E and its generator P, we can pre-calculate it only once and reuse it for different points Q. Let solve the ECDLP in this group for $Q = (18, 15)$. We will now iterate over multiples of Q and look for a collision in the pre-calculated list.

j	0	1	2	3	4	5
$Q \oplus (6j \ominus P)$	$(18, 15)$	$(11, 3)$	$(12, 1)$	$(8, 17)$	$(\mathbf{28}, \mathbf{12})$	$(24, 4)$

We have found a collision for $j = 4$ and $i = 5$ (in the pre-computed list):

$$5P = Q \oplus (24 \ominus P) \implies 4 \equiv x - 24 \pmod{36} \implies x \equiv 29 \pmod{36}.$$

We can now verify that $29P = (18, 15) = Q$.

2.3.2 Pollard ρ-Algorithm

The main drawback of the BsGs algorithm is its space complexity, we need to store $\sqrt{\#E}$ elliptic curve points. To remedy this problem, in 1978 John Pollard published a different algorithm, which is called after him the Pollard ρ(rho)-algorithm, with the same time complexity as BsGs but with very little memory requirements. A similar algorithm can be used for factoring composite integers. This subsection is based on [2].

Definition 2.3.2. (Pollard ρ algorithm): Let S be a finite set of N elements, let $f : S \to S$ be a function. Choose $x_0 \in S$ a starting point of the sequence defined by: $x_i = (\underbrace{f \circ f \circ \cdots \circ f}_{i\text{-times}})(x_0)$, then there exists $L \in \mathbb{N}$ such that:

$$x_{2i} = x_i, \quad 1 \leq i < L.$$

Set S is finite, therefore for some $k \in \mathbb{N}_{<N}$ the sequence $x_0, x_1, \ldots, x_k$ has to a point that repeats twice in this sequence, we denote the first such point by x_T, it's clear that after that point the sequence is in a cycle of length M, where $T + M$ is the index of the second occurrence of the point x_T in the sequence. To prove the existence of i such that: $x_{2i} = x_i$ we can start with the fact that: $\forall k \in \{0, 1, \ldots, M-1\} : x_{T+k} = x_{T+k+M}$, which implies:

$$\exists i \geq T,\ i < T + M : 2i \equiv i \pmod{M} \implies i \mid M.$$

The argument is simple, in every sequence of M consecutive integers there has to be exactly one that is divisible by M, therefore we can see that the L in the definition 2.3.2 is in fact $L = T + M \leq N$. On average (with different choices of x_0 and function f) it takes $O(\sqrt{N})$ steps to obtain a collision with a probability over 50% (based on the birthday paradox), for a thorough analysis see [7].

For a graphical illustration see figure 2.2, the first point in the sequence that repeats itself twice is x_3, therefore we set $T = 3$, and the length of the cycle is $M = 6$, because $x_T = x_3 = x_{3+6}$. The only integer in the set $\{3, 4, 5, 6, 7, 8\}$ that is divisible by $M = 6$ is 6, therefore $i = 6$ and we can easily verify that $x_6 = x_{2*6} = x_{12}$. The graph 2.2 has a strong resemblance to the Greek letter ρ, hence the name of the algorithm.

Definition 2.3.3. The Pollard ρ algorithm might be used to solve the ECDLP. Let E be an elliptic curve group with points' coordinates $\in GF(p)$, let P be its

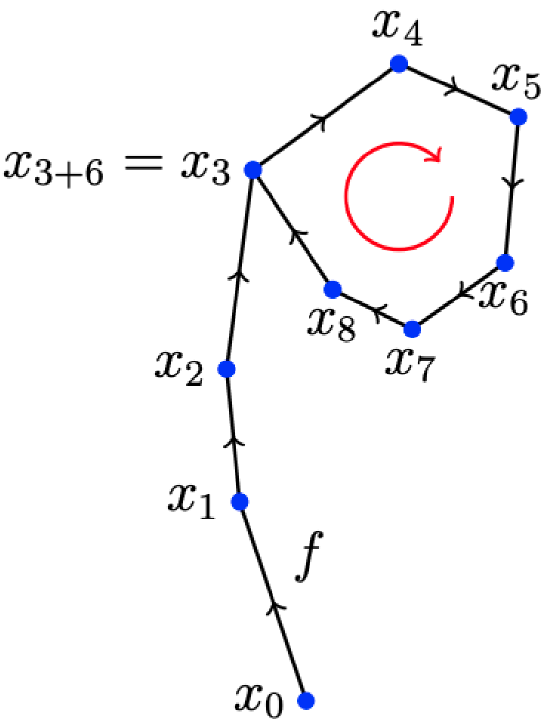

Figure 2.2: Graphical illustration of the idea behind the Pollard ρ algorithm. $T = 3$, length of the cycle $M = 6$. Image source: ([2], page 70).

generator and let $Q \in E$ be some other point. We want to find $x = \log_P(Q)$. Let denote the order of E by $N := \#E$. We divide E into three disjunctive sets S_1, S_2, S_3, so that $\mathcal{O} \notin S_2$ and for $i \in \mathbb{Z}_{\geq 0}$ define $f : E \to E$:

$$T_{i+1} = f(T_i) := \begin{cases} P \oplus T_i, & T_i \in S_1, \\ 2T_i, & T_i \in S_2, \\ Q \oplus T_i, & T_i \in S_3. \end{cases}$$

We can start with $T_0 = \mathcal{O}$, so after k steps we get:

$$T_k = (\underbrace{f \circ f \circ \cdots \circ f}_{k\text{-times}}(\mathcal{O}) = \alpha_k P \oplus \beta_k Q.$$

We need to keep track of $\alpha_k,\ \beta_k$, so we set $\alpha_0 = \beta_0 = 0$ and define it recursively for $k \in \mathbb{Z}_{\geq 0}$:

$$\alpha_{k+1} := \begin{cases} \alpha_k + 1 \pmod N, & T_k \in S_1, \\ 2\alpha_k \pmod N, & T_k \in S_2, \\ \alpha_k, & T_k \in S_3. \end{cases}$$

$$\beta_{k+1} := \begin{cases} \beta_k, \quad T_k \in S_1, \\ 2\beta_k \pmod N, \quad T_k \in S_2, \\ \beta_k + 1 \pmod N, \quad T_k \in S_3. \end{cases}$$

We also create a second sequence of points on elliptic curve E: $R_0 = \mathcal{O}, \forall k \in \mathbb{N} : R_k := T_{2k} = \gamma_k P \oplus \delta_k Q$, we also need to keep track of $\gamma_k,\ \delta_k$. After some number of steps (i) we will encounter a collision: $R_i = T_{2i} = T_i$, then we have a relation:

$$\gamma_i P \oplus \delta_i Q = \alpha_i P \oplus \beta_i Q.$$

Let $d = \gcd(\beta_i - \delta_i, N)$, if $d = 1$ we can easily find the solution x to the ECDLP:

$$x \equiv (\gamma_i - \alpha_i) \cdot (\beta_i - \delta_i)^{-1} \pmod N.$$

If $d \neq 1$ and is small it might be worthy to to find a solution y mod$(\frac{N}{d})$ in the same fashion:

$$y \equiv (\gamma_i - \alpha_i) \cdot (\beta_i - \delta_i)^{-1} \left(\text{mod } \frac{N}{d}\right),$$

then we can find x in the set:

$$\left\{ y + k \cdot \frac{N}{d} \;\middle|\; k \in \{0, 1, \ldots, d-1\} \right\}.$$

For N prime d will be small, if N is not small and d is not small we can restart the algorithm with a different partitioning S_1, S_2, S_3 or a different starting point T_0. Another option is to use the Pohlig-Hellman algorithm and solve multiple ECDLPs in prime subgroups and then find the final solution x using the Chinese remainder theorem (CRT).

For example, let $E = E(11, 18, 29)$ be an elliptic curve group over $GF(29)$ and its elliptic curve equation is $y^2 = x^3 + 11x + 11$. Let $P = (1, 1)$ be a generator of E, let $Q \in E$, we want to find an integer x such that: $Q = xP$. Order of E is 29 (prime). We divide elliptic curve points into sets S_1, S_2, S_3 based on their x-coordinates:

$$\forall R = (R_x, R_y) \in E : \begin{cases} R \in S_1, & \text{if } 0 \leq R_x < \lfloor \frac{p}{3} \rfloor, \\ R \in S_2, & \text{if } \lfloor \frac{p}{3} \rfloor \leq R_x < 2\lfloor \frac{p}{3} \rfloor, \\ R \in S_3, & \text{if } 2\lfloor \frac{p}{3} \rfloor \leq R_x, \end{cases}$$

where $p = 29$. Set S_1 contains the identity element $\mathcal{O}$. Cardinalities of the sets are following $|S_1| = 9,\ |S_2| = 12,\ |S_3| = 8$.
Lets solve the ECDLP for $Q = (13, 26)$. In the table 2.2 are shown the intermediate results of the algorithm.
After 10 iterations we have found a collision:

$$4P + 9Q = 12P \implies x \equiv 8 \cdot 9^{-1} \pmod{29} \equiv 17 \pmod{29}.$$

We can now verify that $17P = (13, 26) = Q$.

i	α_i	β_i	T_i	γ_i	δ_i	R_i
0	0	0	$\mathcal{O}$	0	0	$\mathcal{O}$
1	1	0	$(1,1)$	2	0	$(18,25)$
2	2	0	$(18,25)$	3	1	$(3,22$
3	2	1	$(5,13)$	8	2	$(11,7)$
4	3	1	$(3,22)$	3	8	$(8,3)$
5	4	1	$(12,14)$	4	9	$(13,3)$
6	8	2	$(11,7)$	8	19	$(13,3)$
7	16	4	$(14,4)$	16	10	$(13,3)$
8	3	8	$(8,3)$	3	21	$(13,3)$
9	4	8	$(26,25)$	6	14	$(13,3)$
10	4	9	$(\mathbf{13},\mathbf{3})$	12	0	$(\mathbf{13},\mathbf{3})$

Table 2.2: Intermediate values of the Pollard ρ algorithm.

2.3.3 Pohlig-Hellman Algorithm

As we have mentioned in the previous subsection, Pollard *rho* algorithm works the best in a prime order group. In a case when order of a group G is a composite number N with small factors, we can solve multiple ECDLPs in subgroups of prime order and then using the CRT find the final solution. This algorithm was presented in 1978 by Stephen Pohlig and Martin Hellman in their article [8].

Definition 2.3.4. (**Chinese Remainder Theorem** (CRT)): Let $m_i \in \mathbb{N}$, $i \in \{1,\dots,k\}$, be mutually relatively prime integers, and $N = \prod_{i=1}^{k} m_i$, $x_i \in \mathbb{Z}$, $i \in \{1,\dots,k\}$. The following system of congruences:

$$\begin{aligned} x &\equiv x_1 \pmod{m_1}, \\ x &\equiv x_2 \pmod{m_2}, \\ \vdots\ &\ \ \vdots \\ x &\equiv x_k \pmod{m_k}, \end{aligned}$$

has a solution c:

$$c = \sum_{i=1}^{k} x_i N_i M_i,$$

where $N_i = \frac{N}{m_i}$ and $M_i \equiv (N_i)^{-1} \pmod{m_i}$ and any other solution c' is congruent to c modulo N.

Definition 2.3.5. (**Pohlig-Hellmann algorithm**): Let E be an elliptic curve group of composite order N and let the factorization of N be:

$$N = \prod_{i=1}^{k} p_i^{e_i},\ \forall i \in \{1,2,\dots,k\} : e_i \in \mathbb{Z}_{\geq 0},\ p_i \text{ is prime}.$$

Let P be a generator of E and let $Q \in E$, we want to find an integer x such that: $xP = Q$. We can split this ECDLP into multiple ECDLPs in a prime power subgroups.

- For each $i \in \{1, 2, \dots, k\}$ let:

  $$P_i := \frac{N}{p_i^{e_i}} P, \quad Q_i := \frac{N}{p_i^{e_i}} Q.$$

  Each P_i is a generator of an elliptic curve subgroup of prime power order $\#P_i = p_i^{e_i}$. In this subgroup we will solve the ECDLP, find an integer x_i such that: $x_i P_i = Q_i$.

- For each $i \in \{1, 2, \dots, k\}$ we will solve the ECDLP in a prime power subgroup. We may rewrite the unknown integer $x_i := y_{i,0} + y_{i,1}p_i + y_{i,2}p_i^2 + \cdots + y_{i,e-1}p_i^{e_i-1}$. We can now repeatedly solve the ECDLP in a prime subgroup to obtain one unknown digit of x_i by shifting the rest of them out. To find the first digit $y_{i,0}$ we will multiply both sides of the equation by $p_i^{e_i-1}$:

  $$\begin{aligned} p_i^{e_i-1} Q_i &= p_i^{e_i-1} \cdot x_i P_i \\ &= p_i^{e_i-1} \cdot (y_{i,0} + y_{i,1}p_i + y_{i,2}p_i^2 + \cdots + y_{i,e-1}p_i^{e_i-1}) P_i \\ &= p_i^{e_i-1} y_{i,0} P_i \oplus p_i^{e_i} \cdot \underbrace{(y_{i,1} + y_{i,2}p_i + \cdots + y_{i,e-1}p_i^{e_i-2}) P_i}_{\in \langle P_i \rangle} \\ &= y_{i,0} p_i^{e_i-1} P_i, \quad (\text{because } \forall T \in \langle P_i \rangle : p_i^{e_i} T = \mathcal{O}) \end{aligned}$$

  We may now solve the ECDLP in a prime subgroup of order p_i generated by $p_i^{e_i-1}P_i$ and obtain first digit $y_{i,0}$. Now we can move to the next digit $y_{i,1}$:

  $$\begin{aligned} p_i^{e_i-2} Q_i &= p_i^{e_i-2} \cdot x_i P_i \\ &= p_i^{e_i-2} \cdot (y_{i,0} + y_{i,1}p_i + y_{i,2}p_i^2 + \cdots + y_{i,e-1}p_i^{e_i-1}) P_i \\ &= (p_i^{e_i-2} y_{i,0} + p_i^{e_i-1} y_{i,1}) P_i \oplus p_i^{e_i} \cdot \underbrace{y_{i,2} + \cdots + y_{i,e-1}p_i^{e_i-3}) P_i}_{\in \langle P_i \rangle} \\ &= y_{i,0} p_i^{e_i-2} P_i \oplus y_{i,1} p_i^{e_i-1} P_i \implies \\ p_i^{e_i-2}(Q_i \ominus y_{i,0}P_i) &= y_{i,1} p_i^{e_i-1} P_i. \end{aligned}$$

  To find the next digit $y_{i,1}$ we just need to solve the ECDLP in a prime subgroup of order p_i. We continue in the same fashion until all digits of x_i are found.

- Finally we solve the following system of congruences

$$\begin{aligned} x &\equiv x_1 \pmod{p_1^{e_1}}, \\ x &\equiv x_2 \pmod{p_2^{e_2}}, \\ \vdots\ & \ \vdots \\ x &\equiv x_k \pmod{p_k^{e_k}}, \end{aligned}$$

using the CRT to obtain the final solution x.

In the individual phase when we are solving the ECDLP in a prime order subgroup we can use any algorithm, usually BsGs or Pollard ρ are used. The time complexity of Pohlig-Hellman algorithm is therefore (for more information see [2]):

$$O\Big(\sum_{i=1}^{k}\Big[e_i(S(p_i)+\log(p_i))\Big]\Big),$$

where $S(p_i)$ is the time complexity of the algorithm used to solve the ECDLP in the prime subgroup of order p_i. For elliptic curve groups of order with small factors is Pohlig-Hellman significantly faster than the BsGs or Pollard ρ (we often need to run it more than once with different starting points if the order is composite). For example, let $E = E(1, 2, 75941)$ be an elliptic curve group over $GF(75941)$ and its elliptic curve equation is $y^2 = x^3 + x + 2$. Let $P = (64579, 62139)$ be a generator of E, let $Q \in E$ be a point on elliptic curve E, we want to find an integer x such that: $Q = xP$. Order of E is $76428 = 2^2 \cdot 3^2 \cdot 11 \cdot 193$. We will solve this problem using Pohling-Hellman algorithm. Let $Q = (1447, 50835)$. For $i = 1, 2$ we need to solve the ECDLP in a subgroup of prime square order. In the subgroup of order 2^2 generated by $P_1 = (1, 75939)$, we can rewrite the unknown x_1 as $x_1 = y_{1,0} + 2y_{1,1}$, to find the first digit $y_{1,0}$ we will use the relation:

i	p_i	e_i	P_i	Q_i	x_i
1	2	2	$19107P = (1, 75939)$	$19107Q = (1, 2)$	3
2	3	2	$8492P = (55693, 45178)$	$8492Q = (17273, 40444)$	2
3	11	1	$6948P = (39499, 25804)$	$6948Q = (29264, 5197)$	9
4	193	1	$396P = (58124, 73147)$	$396Q = (34502, 8697)$	189

Table 2.3: Intermediate values of Pohlig-Hellman algorithm stating individual ECDLPs in prime power subgroups.

$$\begin{aligned} 2Q_1 &= y_{1,0} \cdot 2P_1 \\ (75940, 0) &= y_{1,0}(75940, 0) \implies y_{1,0} = 1. \end{aligned}$$

To find the second digit $y_{1,1}$ we will use the relation:

$$\begin{aligned}
Q_1 \ominus y_{1,0} \cdot P_1 &= y_{1,1} \cdot 2P_1 \\
(1,2) \oplus (1,2) &= y_{1,1}(75940, 0) \\
(75940, 0) &= y_{1,1}(75940, 0) \implies y_{1,1} = 1.
\end{aligned}$$

Therefore, $x_1 = y_{1,0} + y_{1,0} \cdot 2 = 1 + 2 = 3$. In reality we could have just tried all four possible values for x_1. We will repeat the whole process in the subgroup generated by $P_2 = (55693, 45178)$ of order 3^2. We rewrite the unknown integer x_2 as $x_2 = y_{2,0} + 3y_{2,1}$, to find the first digit $y_{2,0}$ we will use the relation:

$$\begin{aligned}
3Q_2 &= y_{2,0} \cdot 3P_2 \\
(35655, 11621) &= y_{2,0}(35655, 64320) \implies y_{2,0} = 2.
\end{aligned}$$

To find the second digit $y_{2,1}$ we will use the relation:

$$\begin{aligned}
Q_2 \ominus y_{2,0} \cdot P_2 &= y_{2,1} \cdot 3P_2 \\
Q_2 \ominus 2P_2 &= y_{2,1} \cdot (35655, 64320) \\
\mathcal{O} &= y_{2,1} \cdot (35655, 64320) \implies y_{2,1} = 0.
\end{aligned}$$

Therefore, $x_2 = 2 + 0 \cdot 3 = 2$. In this case there are nine possible values for x_2, so in reality we could have easily tried them all. Now we can put the system of congruences together and solve it to find the final solution x.

$$\begin{aligned}
x &\equiv 3 \pmod{4}, \\
x &\equiv 2 \pmod{9}, \\
x &\equiv 9 \pmod{11}, \\
x &\equiv 189 \pmod{193},
\end{aligned}$$

Using the CRT we compute x (the intermediate values are in the table 2.4):

i	x_i	m_i	N_i	M_i
1	3	4	19107	3
2	2	9	8492	2
3	9	11	6948	8
4	189	193	396	58

Table 2.4: Intermediate values of the CRT phase of the Pohlig-Hellman algorithm.

$$x \equiv 3 \cdot 19107 \cdot 3 + 2 \cdot 8492 \cdot 2 + 9 \cdot 6948 \cdot 8 + 189 \cdot 396 \cdot 58 \pmod{76428} \equiv 2891 \pmod{76428}.$$

We can now verify that $2891P = (1447, 50835) = Q$.

2.4 Index Calculus for ECDLP

The Index Calculus is originally a **subexponential** algorithm to solve the DLP in the multiplicative group of a finite field.

Definition 2.4.1. Let $0 \leq a \leq 1,\ a \in \mathbb{R}$ and $c \in \mathbb{R}_{>0}$. The **subexponential function** for the parameters a and c is:

$$L_N(a,c) := \exp(c \log(N)^a \log(\log(N))^{1-a}).$$

Let N be a k-bit integer, note that taking $a = 0$ gives $L_N(0,c) = \log(N)^c = k^c$ (polynomial) while taking $a = 1$ gives $L_N(1,c) = N^c = \exp(ck)$ (exponential). Hence $L_N(a,c)$ interpolates exponential and polynomial growth. An algorithm is called **subexponential** when it's complexity is $O(L_N(a,c))$ with $0 < a < 1$, for more context see chapter 15 in [9].

However it is common to use the name index calculus algorithm to refer to any algorithm that operates in the same fashion as the original Index Calculus algorithm, which solves the DLP by collecting relations index calculus algorithm and using linear algebra afterwards [10].

Definition 2.4.2. Index Calculus for ECDLP: Let E be an elliptic curve over a prime order field $GF(p)$, let P be a generator of E and for simplicity we assume $\#P$ is prime (if it's not the case we can using the Pohlig-Hellman idea and split the ECDLP into multiple ECDLPs in prime subgroups). Let $Q \in E$, we want to find an integer x such that $xP = Q$. The simplest version of index calculus algorithm consists of two main stages: the relation collection step and the linear algebra step. At first, we need to collect the relations:

1. Specify a factor base $\mathcal{F} \subset E$ such that we can effortlessly test the membership of an element to this factor base.

2. Generate a random linear combination of points P, Q:

$$R := uP + vQ, \quad u, v \text{ are random integers from } GF(\#P).$$

3. If possible, express R as a linear combination of the elements of the factor base $\mathcal{F}$:

$$R = uP + vQ = \sum_{k=1}^{|\mathcal{F}|} a_k P_k, \quad \forall k \in \{1, 2, \ldots, |\mathcal{F}|\} : P_k \in \mathcal{F},\ a_k \in GF(\#P),$$

$$\mathcal{O} = -uP - vQ + \sum_{k=1}^{|\mathcal{F}|} a_k P_k.$$

4. If R cannot be expressed in terms of the factor base $\mathcal{F}$, continue with step 2. Otherwise, store the coordinates of R with respect to $\mathcal{F}$ and integers u, v as a row in the relation matrix M. The row is stored in this form:
$$(a_1, a_2, \dots, a_{|\mathcal{F}|}, -u, -v).$$
5. We repeat this procedure (steps 2 to 4) until the end condition is met.

Some authors (see [10] page 2) suggest end condition to set to number of decomposed points R to be at least $|\mathcal{F}|$, but we need to state that this condition doesn't guarantee these relations are enough to solve the ECDLP. Another option, which guarantees we will be able to solve the ECDLP in the next step, is to collect relations until the rank of matrix M is $|\mathcal{F}| + 1$, which is also the maximum rank this matrix can have (assuming $Q \neq \mathcal{O}$). We will state a weaker (that usually requires less relations to be found) end condition in the following section **??**.

After collecting enough relations, the linear algebra step solves the ECDLP:

1. Matrix M is over $GF(\#P)$, we will reduce it to row echelon form (using some linear algebra technique, e.g. Gaussian Elimination Method), the last non-zero row of the reduced matrix will look like $(0, 0, \dots, 0, 1, -v')$, which describes a relation:
$$\begin{aligned} &\mathcal{O} = 1P \oplus (-v'Q) \\ &P = v'Q \implies x \equiv (v')^{-1} \pmod{\#P}. \end{aligned}$$
We can always recover this solution x, because order of $\#P$ is prime and $P \neq \mathcal{O} \implies v' \not\equiv 0 \pmod{\#P}$.

The main bottleneck of this algorithm lies in the decomposition of a point R into the factor basis $\mathcal{F}$, usually known as **point decomposition problem** (PDP). Therefore, in order for this algorithm to be efficient, we require the solution of the PDP to be efficient (including the case when R can't be decomposed into elements of $\mathcal{F}$) and we also require high success rate of the decomposition of R. Both there requirements are deeply affected by the choice of factor base $\mathcal{F}$ and its size [10].

2.4.1 Summation Polynomials

In 2004 Igor Semaev published an article introducing summation polynomials in order transform the PDP to a problem of finding a solution of a multivariate polynomial equation based on the group law of a specific elliptic curve, for more information see the original article [11].

Definition 2.4.3. Let E be the elliptic curve given by the short Weierstrass equation over a prime field $\mathbb{F} = GF(p),\ p > 3$. For any natural number $n \geq 2$ let $S_n = S_n(X_1, X_2, \ldots, X_n)$ be a polynomial in n variables which is related to the group operation on E. We call this polynomial the n-th **summation polynomial** and define it by the following property. Let $x_1, x_2, \ldots, x_n$ be any elements from $\overline{\mathbb{F}}$, the algebraic closure of the field $\mathbb{F}$, then $S_n(x_1, x_2, \ldots, x_n) = 0$ if and only if there exist $y_1, y_2, \ldots, y_n \in \overline{\mathbb{F}}$ such that points $(x_i, y_i), \forall i \in \{1, 2, \ldots, n\}$ are in the elliptic curve group defined by E over $\overline{\mathbb{F}}$ and their sum is the identity element of this elliptic curve group:

$$\mathcal{O} = \sum_{i=1}^{n} (x_i, y_i).$$

For $n = 2$ the summation polynomial is defined as:

$$S_2(X_1, X_2) := X_1 - X_2,$$

it comes from the fact that

$$\forall P, Q \in E(A, B, p) : P \oplus Q = \mathcal{O} \implies Q = \ominus P.$$

Based on the definition of the additive inverse in $E(A, B, p)$ we know, the points $P = (x_1, y_1)$ and $\ominus P = (x_1, -y_1)$ have the same x-coordinate which is equivalent to $S_2(x_1, x_2) = 0 \implies x_1 = x_2$. To determine $S_3(X_1, X_2, X_3)$, let (x_1, y_1) and (x_2, y_2) be two affine ($\neq \mathcal{O}$) points on $E(A, B, p$ such that $x_1 \neq x_2$. We denote their sum and difference by:

$$\begin{aligned}(x_3, y_3) &:= (x_1, y_1) \oplus (x_2, y_2), \\ (x_4, y_4) &:= (x_1, y_1) \ominus (x_2, y_2).\end{aligned}$$

We will use the group law $\oplus$ to express x_3 and x_4 in terms of x_1, x_2, y_1, y_2:

$$\begin{aligned}x_3 &= \lambda_3^2 - (x_1 + x_2), \text{ where } \lambda_3 = \frac{y_2 - y_1}{x_2 - x_1}, \\ x_4 &= \lambda_4^2 - (x_1 + x_2), \text{ where } \lambda_4 = \frac{y_2 + y_1}{x_2 - x_1}, \text{ since } \ominus (x_2, y_2) = (x_2, -y_2),\end{aligned}$$

To find a polynomial such that x_3 and x_4 are its roots, recall **Vieta's formulas**, let z_1, z_2 be two roots of the polynomial $p(z) = az^2 + bz + c$, then it has to satisfy following formulas:

$$z_1 + z_2 = -\frac{b}{a}, \quad z_1 z_2 = \frac{c}{a}.$$

Therefore, we want to find $x_3 + x_4$ and $x_3 x_4$:

$$\begin{aligned}
x_3 + x_4 &= \lambda_3^2 + \lambda_4^2 - 2(x_1 + x_2) \\
&= \frac{(y_2 - y_1)^2 + (y_2 + y_1)^2 - 2(x_1 + x_2)(x_2 - x_1)^2}{(x_2 - x_1)^2} \\
&= \frac{2y_2^2 + 2y_1^2 - 2(x_1 + x_2)(x_2 - x_1)^2}{(x_2 - x_1)^2}, \text{ (substite for } y_1^2, y_2^2 \text{ using } E \text{ eq.)} \\
&= \frac{2(x_1^3 + Ax_1 + B + x_2^3 + Ax_2 + B) - 2(x_1^3 + x_2^3 - x_1^2 x_2 - x_1 x_2^2)}{(x_2 - x_1)^2} \\
&= 2\frac{(Ax_1 + Ax_2 + 2B) + x_1^2 x_2 + x_1 x_2^2}{(x_2 - x_1)^2} \\
&= 2\frac{x_1(x_1 x_2 + A) + x_2(x_1 x_2 + A) + 2B}{(x_2 - x_1)^2} \\
&= 2\frac{(x_1 + x_2)(x_1 x_2 + A) + 2B}{(x_2 - x_1)^2}.
\end{aligned}$$

$$\begin{aligned}
x_3 x_4 &= \frac{\Big((y_2 - y_1)^2 - (x_1^3 + x_2^3 - x_1^2 x_2 - x_1 x_2^2)\Big)\Big((y_2 + y_1)^2 - (x_1^3 + x_2^3 - x_1^2 x_2 - x_1 x_2^2)\Big)}{(x_2 - x_1)^4} \\
&= \frac{\Big(y_1^2 + y_2^2 - 2y_1 y_2 - x_1^3 - x_2^3 + x_1^2 x_2 + x_1 x_2^2\Big)\Big(y_1^2 + y_2^2 + 2y_1 y_2 - x_1^3 - x_2^3 + x_1^2 x_2 + x_1 x_2^2\Big)}{(x_2 - x_1)^4} \\
&= \frac{\Big(x_1^2 x_2 + x_1 x_2^2 + Ax_1 + Ax_2 - 2y_1 y_2 + 2B\Big)\Big(x_1^2 x_2 + x_1 x_2^2 + Ax_1 + Ax_2 + 2y_1 y_2 + 2B\Big)}{(x_2 - x_1)^4} \\
&= \frac{-4y_1^2 y_2^2 + x_1^2 x_2^4 + 2x_1^3 x_2 A + 4x_1^2 x_2^2 A + 2x_1 x_2^3 A + x_1^2 A^2 + 2x_1 x_2 A^2 + x_2^2 A^2}{(x_2 - x_1)^4} \\
&+ \frac{4x_1^2 x_2 B + 4x_1 x_2^2 B + 4x_1 AB + 4x_2 AB + 4B^2 + x_1^4 x_2^2 + 2x_1^3 x_2^3}{(x_2 - x_1)^4} \\
&= \frac{\Big((x_1 - x_2)^2\Big)\Big(x_1^2 x_2^2 - 2x_1 x_2 A + A^2 - 4x_1 B - 4x_2 B\Big)}{(x_2 - x_1)^4}, \text{ (substited for } y_1^2, y_2^2 \text{ using } E \text{ eq.)} \\
&= \frac{(x_1 x_2 - A)^2 - 4B(x_1 + x_2)}{(x_2 - x_1)^2}.
\end{aligned}$$

Therefore, the x_3 and x_4 are roots of the polynomial:

$$f(X) := (x_2 - x_1)^2 X^2 - 2\Big((x_1 + x_2)(x_1 x_2 + A) + 2B\Big)X + \Big((x_1 x_2 - A)^2 - 4B(x_1 + x_2)\Big).$$

In the case $x_1 = x_2$ one of points $(x_3, y_3), (x_4, y_4)$ is $2(x_1, y_1)$ and the other one has to be $\mathcal{O}$, without loss of generality, let's consider $(x_3, y_3) = 2(x_1, y_1)$

we will show that x_3 is the root of the polynomial $f(X)$.

$$\begin{aligned}
x_1 = x_2 :\ f(X) &= -2\Big(2x_1(x_1^2+A)+2B\Big)X + \Big((x_1^2-A)^2 - 8Bx_1\Big),\\
X &= \frac{(x_1^2-A)^2-8Bx_1}{4(x_1^3+Ax_1+B)}\\
X &= \frac{x_1^4-2Ax_1^2-8Bx_1+A^2}{4(x_1^3+Ax_1+B)}.\\
x_3 &= \lambda^2 - 2x_1, \quad \lambda = \frac{3x_1^2+A}{2y_1}\\
x_3 &= \frac{9x_1^4+6Ax_1^2+A^2-8x_1y_1^2}{4y_1^2}, \text{ (substitute for } y_1^2 \text{ using } E \text{ eq.)}\\
x_3 &= \frac{9x_1^4+6Ax_1^2+A^2-8x_1^4-8x_1^2A-8Bx_1}{4(x_1^3+Ax_1+B)}\\
x_3 &= \frac{x_1^4-2Ax_1^2-8Bx_1+A^2}{4(x_1^3+Ax_1+B)}.
\end{aligned}$$

Therefore we can define the third summation polynomial as follows:

$$\begin{aligned}
S_3(X_1,X_2,X_3) := (X_2-X_1)^2X_3^2 &- 2\Big((X_1+X_2)(X_1X_2+A)+2B\Big)X_3\\
&+ (X_1X_2-A)^2 - 4B(X_1+X_2).
\end{aligned}$$

S_3 is symmetric polynomial of degree 2 in each variable X_1, X_2, X_3. S_3 is absolutely irreducible, for a proof and more information about summation polynoamials see [11]. In the same article Semaev also defined n-th summation polynomials (using resultant) for an arbitrary n as follows:

$$\begin{aligned}
&\forall k, n \in \mathbb{N},\ n \geq 4,\ n-3 \geq k \geq 1 :\ S_n(X_1, X_2, \ldots, X_n) :=\\
&\mathrm{Res}_y\Big(S_{n-k}(X_1,\ldots,X_{n-k-1},y),\ S_{k+2}(X_{n-k},\ldots,X_n,y)\Big).
\end{aligned}$$

For example,

$$\begin{aligned}
S_4(X_1, X_2, X_3, X_4) &= \operatorname{Res}_y\Big(S_3(X_1, X_2, y),\ S_3(X_3, X_4, y)\Big),\\
S_3(X_1, X_2, y) &= c_0 y^2 + c_1 y + c_2,\ \text{where}\\
c_0 &= (X_2 - X_1)^2,\\
c_1 &= -2\Big((X_1 + X_2)(X_1X_2 + A) + 2B\Big),\\
c_2 &= (X_1X_2 - A)^2 - 4B(X_1 + X_2),\\
S_3(X_3, X_4, y) &= d_0 y^2 + d_1 y + d_2,\ \text{where}\\
d_0 &= (X_4 - X_3)^2,\\
d_1 &= -2\Big((X_3 + X_4)(X_3X_4 + A) + 2B\Big),\\
d_2 &= (X_3X_4 - A)^2 - 4B(X_3 + X_4),\\
S_4(X_1, X_2, X_3, X_4) &= \det\begin{pmatrix} c_0 & 0 & d_0 & 0\\ c_1 & c_0 & d_1 & d_0\\ c_2 & c_1 & d_2 & d_1\\ 0 & c_2 & 0 & d_2 \end{pmatrix}.
\end{aligned}$$

If we recall that resultant of two polynomials with respect to variable y is zero if and only if both polynomials (over an algebraically closed field) have a common root. We can see that summation polynomials $S_{n-k}(X_1, \dots, X_{n-k-1}, y)$ and $S_{k+2}(X_{n-k}, \dots, X_n, y)$ are tied together with variable y, because if there exist $x_1, \dots, x_n, y_0$ (y_0 is the common root of $S_{n-k}(y)$ and $S_{k+2}(y)$) such that:

$$\begin{aligned}
S_{n-k}(x_1, \dots, x_{n-k-1}, y_0) = 0 \wedge S_{k+2}(x_{n-k}, \dots, x_n, y_0) = 0 &\implies\\
\exists P_1, \dots, P_n, (y_0, y_1) \in E(\overline{\mathbb{F}}) : P_1 \oplus \cdots \oplus P_{n-k-1} \oplus (y_0, y_1) = \mathcal{O}&,\\
\exists v \in \{0, 1\} : P_{n-k} \oplus \cdots \oplus P_n \oplus (-1)^v (y_0, y_1) = \mathcal{O} &\implies\\
P_1 \oplus \cdots \oplus P_{n-k-1} \oplus (-1)^{v+1}\Big(P_{n-k} \oplus \cdots \oplus P_n\Big) = \mathcal{O} &\implies\\
S_n(x_1, \dots, x_n) = 0&.
\end{aligned}$$

Summation polynomials for $n \geq 3,\ n \in \mathbb{N}$ are symmetric, absolutely irreducible and of degree 2^{n-2} in each variable $X_i,\ i \in \{1, \dots, n\}$.

However, the higher summation polynomials are hardly practical (compared to S_3), because the growth of their degrees (in each variable) is exponential with respect to n. In 2015 Semaev himself presented a *splitting trick*, a way how to transform n-th summation polynomial into a polynomial system of S_3 summation polynomials which can be solved more efficiently [12]. This trick is based on the resultant properties and the idea of tying multiple polynomial equations together with **bounding variables**.

Definition 2.4.4. (The splitting trick): The roots of the n-th summation polynomial $S_n(X_1, \dots, X_n)$ in $\overline{\mathbb{F}}[X_1, \dots, X_n]$ are equivalent to the solutions of the following polynomial system:

$$\begin{aligned}
&S_3(X_1, X_2, U_1) = 0, \\
&S_3(X_{k+2}, U_k, U_{k+1}) = 0, \quad 1 \leq k \leq n-4,\ k \in \mathbb{N}, \\
&S_3(X_{n-1}, X_n, U_{n-3}) = 0.
\end{aligned}$$

We call the variables $U_i,\ i \in \{1, \dots, n-3\}$ bounding variables. Therefore, by introducing $n-3$ new variables we obtain a polynomial system that consists of $n-2$ symmetric polynomials (each only in three variables) of degree two in each its variable instead of a single polynomial in n variables of degree 2^{n-2} in each of its n variables.

Summation polynomials reduce the PDP to the solution of a system of multivariate polynomial equations which are usually solved by calculating the Gröbner basis of the ideal generated by those polynomial equations. This ideal I is zero-dimensional, the set of common zeroes of the polynomials in I is finite in $\overline{\mathbb{F}}$, which is equivalent to the fact that, for each variable $X_i,\ i \in \{1, \dots, n\}$ there is a polynomial in the Gröbner basis for i, with a power of X_i as a leading monomial [13]. Reduced Gröbner basis of the ideal spanned by those polynomial equations is either calculated with respect to the lexicographic order of monomials or is calculated with respect to some other order and then then converted using the FGLM algorithm to a Gröbner basis for the same ideal with respect to a different monomial order, for detailed information about this algorithm see [13].

Definition 2.4.5. Let $G = \{g_1, \dots, g_s\}$ be the reduced basis for a zero-dimensional ideal $I \subset \mathbb{F}[X_1, \dots, X_n]$ with respect to lex order with $X_1 >_{\text{lex}} \cdots >_{\text{lex}} X_n$ and ordered so that every $\text{LT}(g_j) >_{\text{lex}} \text{LT}(g_{j+1})$. Then for each $i \in \{1, \dots, n\}$ there is some $j = j(i)$ for which $\text{LT}(g_j) = x_i^{d_i}$ for some $d_i > 0$. This is called the **triangular form** and is especially convenient for finding all the points that lie in the affine variety defined by the polynomials $g_1, \dots, g_n$.

The last polynomial in the Gröbner basis G is univariate: $g_s = g_s(X_n)$, we find its roots and substitute them into other polynomials in G, after such substitution, at least one of the earlier polynomials $g_i,\ i \in \{1, \dots, s-1\}$ is univariate in X_{n-1}. This is called **backsolving** or **backsubstitution**, for more information see [14].

In the next chapter we describe specific algorithms solving ECDLP that were implemented and tested by us. The experimental results are in the chapter 5.

Chapter 3

Specialized Algorithms Solving ECDLP

In this chapter we first describe four specialized algorithms for solving ECDLP that are based on the theoretical concepts presented in the previous chapters. Afterwords, we follow up with the actual implementation's details. The experimental results are presented in chapter 5.

3.1 Algorithm 1 (Semaev 2015)

Algorithm 1 is based on the Semaev's algorithm presented in [12], few changes had to be made to make the algorithm work for ECDLP over finite fields $GF(p),\ p$ prime. Semaev's algorithm works best over prime field extensions, where the base field is of prime characteristic $q,\ q \leq 2^{10}$ (approximately).

Let P be a generator of the prime order ($\#P = r$) group $E(p)$, where E is an elliptic curve defined over prime field $GF(p)$, p prime. We are restricting this algorithm to the case where $E(p)$ is a group of prime order, because if it's not the case, we can use the Pohlig-Hellman algorithm to split the initial ECDLP in the group of composite order to a multiple smaller ECDLPs in prime order subgroups, where algorithm 1 can be used to find the solution. The ECDLP is given a generator P and some other point $Q \in E(p)$, find an integer k such that $kP = Q$, since $E(p)$ is a finite group of prime order r we are interested in the solution $k \pmod r$. For large p, $r \approx p$. Algorithm 1, which computes this integer k, works in multiple steps and is described below.

1. Define the decomposition constant $m \geq 2,\ m \in \mathbb{N}$, and a factor base $\mathcal{F} \subset GF(p)$ of size $\left\lceil \sqrt[m]{r} \right\rceil$, where $\lceil \cdot \rceil$ is the ceiling function. The factor base $\mathcal{F}$ might consist of random x-coordinates of points on the elliptic

curve E (non-deterministic):

$$\mathcal{F} := \Big\{ x \;\Big|\; x \in GF(p),\ \exists y \in GF(p) : (x, y) \in E(p) \Big\},$$

or we can take the $|\mathcal{F}|$ smallest x-coordinates of points on the elliptic curve E (deterministic).

2. Construct a relation matrix $M \in GF(r)^{|\mathcal{F}|+1 \times |\mathcal{F}|+2}$, r is prime, therefore there exists a finite field of order r. Lets order elements of $\mathcal{F}$ and denote the i-th element of the factor base $\mathcal{F}$ by $\mathcal{F}_i,\ i \in \{0, \ldots, |\mathcal{F}| - 1\}$.

$$M := \begin{array}{cccccc} \mathcal{F}_\mathbf{0} & \mathcal{F}_\mathbf{1} & \ldots & \mathcal{F}_{\mathcal{F}-\mathbf{1}} & \mathbf{a} & \mathbf{b} \\ \end{array}$$

$$M := \left(\begin{array}{cccccc} m_{1,1} & m_{1,2} & \ldots & m_{1,|\mathcal{F}|} & a_1 & b_1 \\ \vdots & \vdots & \ldots & \vdots & \vdots & \vdots \\ m_{|\mathcal{F}|+1,1} & m_{|\mathcal{F}|+1,2} & \ldots & m_{|\mathcal{F}|+1,|\mathcal{F}|} & a_{|\mathcal{F}|+1} & b_{|\mathcal{F}|+1} \end{array} \right),$$

where all elements of the matrix M are in $GF(r)$. Each row of this matrix represents a relation in the group $E(p)$:

$$\forall j \in \{1, \ldots, |\mathcal{F}| + 1\} : a_j P \oplus b_j Q \oplus \sum_{i=1}^{\mathcal{F}} m_{j,i}(\mathcal{F}_{i-1}, y_{i-1}) = \mathcal{O},$$

where $y_k,\ k \in \{0, \ldots, |\mathcal{F}| - 1\}$ is smaller of the y-coordinates of the points on E with x-coordinate equal to $\mathcal{F}_k$ (if there is a point $(\mathcal{F}_k, y)$ in $E(p)$ there is also its additive inverse $(\mathcal{F}_k, -y) = (\mathcal{F}_k, p - y)$ in $E(p)$. We take smaller of these two values as $y_k := \min(y, p - y)$.

The matrix M is initialized as a zero matrix and we gradually fill it with relations. And initialize the row index $rowID = 1$ telling us where to insert the next found relation.

3. For random integers $a, b \in \{0, \ldots, r - 1\}$ compute point $R = aP \oplus bQ$. If $R = \mathcal{O}$ and $b \neq 0$ we can immediately solve the ECDLP:

$$k \equiv (-a)(b)^{-1} \pmod r.$$

Otherwise, R has affine coordinates (R_x, R_y). If $R_x = \mathcal{F}_k$, for some $k \in \{0, \ldots, |\mathcal{F}| - 1\}$, then we have a relation and we add to the relation matrix M.

$$M_{rowID,\ k} = \begin{cases} 1, & R_y < \frac{p}{2}, \\ r - 1, & R_y > \frac{p}{2}. \end{cases}$$

$$M_{rowID,\ |\mathcal{F}|+1} = a_{rowID} = a \pmod r,$$

$$M_{rowID,\ |\mathcal{F}|+2} = b_{rowID} = b \pmod r,$$

$$rowID = rowID + 1.$$

Otherwise, we try to decompose this point as a sum of factor base $\mathcal{F}$ points by solving following multivariate polynomial system, compute $x_1, \ldots, x_m \in \mathcal{F}$ and $u_1, \ldots, u_{m-2} \in GF(p)$ such that:

$$\begin{aligned} S_3(x_1, x_2, u_1) &= 0, \\ S_3(x_{k+2}, u_k, u_{k+1}) &= 0, \quad 1 \leq k \leq m-3,\ k \in \mathbb{N}, \\ S_3(x_m, R_x, u_{m-2}) &= 0, \\ \left[\prod_{i=0}^{|\mathcal{F}|-1} \Big(x_j - \mathcal{F}_i\Big)\right] &= 0, \quad j \in \{1, \ldots, m\}, \end{aligned}$$

the last m products is used to restrict found solutions $x_1, \ldots, x_m$ to lie in the factor base $\mathcal{F}$.
Semaev also suggested adding the **field equations**:

$$x_j^p - x_j = 0, \quad j \in \{1, \ldots, m\},$$

which is not computationally feasible for large p (approximately $p \geq 2^{10}$), so we won't generally use them (unless stated otherwise). Lets denote the set of the polynomials described above as T. Ideal $I = \langle T \rangle$ is a zero-dimensional ideal. Therefore, we can compute its Gröbner basis G with respect to lexicographic order $X_1 >_{lex} >_{lex} \cdots >_{lex} X_n$ and by definition 2.4.5 it will be in a triangular form, so we can easily find the affine variety $\mathcal{V}(G) = \mathcal{V}(T)$, the set of the common zeroes of the polynomials in the set T. For every found solution $(s_1, \ldots, s_m) \in GF(p)^m$ we add update one row in the relation matrix, we first need to determine the signs $v_i,\ i \in \{1, \ldots, m\}$, such that:

$$\left[\sum_{i=1}^{m} (-1)^{v_i} (s_i, y_i)\right] = \mathcal{O},$$

where $y_i = \min(y_i,\ p - y_i)$ is the (smaller) y-coordinate of a point on E with x-coordinate equal to s_i. After determining the signs v_i we update the matrix M (we start with a row of zeroes):

$$\forall i \in \{1, \ldots, m\} : M_{rowID,\ i} = M_{rowID,\ i} + \begin{cases} 1, & v_i = 0, \\ r-1, & v_i = 1. \end{cases}$$

$$\begin{aligned} M_{rowID,\ |\mathcal{F}|+1} &= a_{rowID} = a \pmod{r}, \\ M_{rowID,\ |\mathcal{F}|+2} &= b_{rowID} = b \pmod{r}, \\ rowID &= rowID + 1. \end{aligned}$$

4. We repeat step 3. until the end condition is met. The end condition could obviously just be that the matrix M has a full rank $\mathcal{F} + 1$, but in reality we need way less relations so it's not efficient to always generate

that many relations. To solve the ECDLP we just need to transform one row of the matrix M to this form: $(0, \ldots, 0, a', b')$ using only elementary row operations (we expect our reader is familiar with the Gaussian elimination algorithm and the definition of the matrix rank, otherwise feel free to consult your nearest textbook of linear algebra).

We can state the end condition as follows. Lets denote the matrix M without last two columns by M'. We proceed to step 5 if $\operatorname{rank}(M) > \operatorname{rank}(M')$, which implies that if we reduce M to its **row echelon form**, meaning the first non-zero element in each row, called the **leading entry**, is 1. Each leading entry is in a column to the right of the leading entry in the previous row and zero rows are below rows having a non-zero element. We will have a leading entry in the $(\mathcal{F} + 1)$-th column corresponding to **a**, we don't consider the degenerate case when $Q = \mathcal{O}$ in which case a leading entry could be in the very last column as well.

5. We reduce M to its row echelon form, as described above, as denote it by M_R. We can now solve the ECDLP using the last non-zero row of M_R which has to be in the following form:

$$(0, \ldots, 0, 1, b') \implies P \oplus b'Q = \mathcal{O} \implies k \equiv (-b')^{-1} \pmod{r}.$$

This multiplicative inverse of $(-b')$ always exists, since r is a prime and $b' \not\equiv 0 \pmod{r}$, because $P \neq \mathcal{O}$. If we denote the rank of the matrix M by d, then the last non-zero row of the matrix M_R is the d-th row. Integer k is the solution to the ECDLP.

3.2 Algorithm 2 (Amadori et al. 2017)

Algorithm 2 is based on the algorithm by Amadori, Pintore and Sala presented in [10], the main difference to the algorithm 1 is using a factor base with known decomposition of each of its elements as a linear combination of P, Q, so we only need to find one relation to solve the ECDLP.

Chapter **4**

Realisation in SageMath

Chapter 5

Experimental Results

poly division alg Pohling-Hellmann Pollard-Rho BsGs Groebner basic F4, F5 Groebner SumPoly

Conclusion

Bibliography

[1] COX, David A., John LITTLE and Donal O'SHEA. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Fourth Edition. New York: Springer, 2015. Undergraduate texts in mathematics. ISBN 978-3-319-16721-3.

[2] KALVODA, Tomáš, Ivo PETR and Štěpán STAROSTA. Matematika pro kryptologii [online]. KAM FIT ČVUT. [Praha], Updated on 20-02-2019 [Accessed on 16-04-2019]. Available at: `https://courses.fit.cvut.cz/MI-MKY/media/lectures/mi-mky-poznamky-v17.pdf`

[3] HOLLMANN, Matyáš. *Implementace násobení na neasociativních (nekomutativních) algebrách.* Praha, 2017. Bakalářská práce. České vysoké učení technické v Praze, Fakulta informačních technologií. Vedoucí práce Jiřina Scholtzová. Available at: `https://dspace.cvut.cz/bitstream/handle/10467/69263/F8-BP-2017-Hollmann-Matyas-thesis.pdf`

[4] BUCHBERGER, Bruno. Bruno Buchberger's PhD thesis 1965: An Algorithm for Finding the Basis Elements of the Residue Class Ring of a Zero Dimensional Polynomial Ideal. Journal of Symbolic Computation. 2006, 41(03), 475-511. DOI: `https://doi.org/10.1016/j.jsc.2005.09.007`

[5] COHEN, Henri, Gerhard FREY and Roberto AVANZI. *Handbook of elliptic and hyperelliptic curve cryptography.* Boca Raton: Taylor & Francis, 2006. ISBN 978-1-58488-518-4.

[6] SHOUP, Victor. *Lower Bounds for Discrete Logarithms and Related Problems.* Advances in Cryptology — EUROCRYPT '97. EUROCRYPT 1997. Springer, Berlin, Heidelberg, 1997. DOI: `https://doi.org/10.1007/3-540-69053-0_18`.

[7] BOS, Joppe W., Alina DUDEANU and Dimitar JETCHEV. *Collision bounds for the additive Pollard rho algorithm for solving discrete log-*

arithms. Journal of Mathematical Cryptology. 2014, 8(1), 71-92. ISSN (Online) 1862-2984. DOI: `https://doi.org/10.1515/jmc-2012-0032`.

[8] POHLIG, S. a M. HELLMAN. *An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance (Corresp.).* IEEE Transactions on Information Theory. 1978, 24(1), 106-110. ISSN (Online) 1557-9654 DOI: `https://doi.org/10.1109/TIT.1978.1055817`.

[9] GALBRAITH, Steven D. *Mathematics of public key cryptography.* New York: Cambridge University Press, 2012. ISBN 978-1-107-01392-6.

[10] AMADORI, Alessandro, Federico PINTORE and Massimiliano SALA. *On the discrete logarithm problem for prime-field elliptic curves.* Finite fields and their applications. 2018, 51(May), 168-182. DOI: `https://doi.org/10.1016/j.ffa.2018.01.009`.

[11] SEMAEV, Igor. *Summation polynomials and the discrete logarithm problem on elliptic curves.* Cryptology ePrint Archive, Report 2004/031, 2004. Also available at `https://eprint.iacr.org/2004/031`.

[12] SEMAEV, Igor. *New algorithm for the discrete logarithm problem on elliptic curves.* Cryptology ePrint Archive, Report 2015/310, 2015. Also available at `https://eprint.iacr.org/2015/310`.

[13] FAUGÉRE, J.C., P. GIANNI, D. LAZARD and T. MORA. *Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering.* Journal of Symbolic Computation. 1994, 11(1-000). Also available at `https://www-polsys.lip6.fr/~jcf/Papers/FGLM.pdf`.

[14] BROWN, Gavin. *Zero-dimensional ideals.* Chapter 9 in Polynomials in Several Variables - MA574 (course notes) [online]. 2016. [Accessed on 16-04-2019]. Available at `https://www.kent.ac.uk/smsas/personal/gdb/MA574/week11.pdf`.

Appendix A

Acronyms

EEA Extended Euclidean algorithm

DLP Discrete logarithm problem

ECDLP Elliptic curve discrete logarithm problem

BsGs Baby-step giant-step (algorithm)

CRT Chinese remainder theorem

PDP Point decomposition problem

Appendix B

Contents of enclosed CD

- `readme.txt` .... the file with CD contents description
- `exe` .... the directory with executables
- `src` .... the directory of source codes
  - `wbdcm` .... implementation sources
  - `thesis` .... the directory of LaTeX source codes of the thesis
- `text` .... the thesis text directory
  - `thesis.pdf` .... the thesis text in PDF format
  - `thesis.ps` .... the thesis text in PS format