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 22, 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 22, 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 are going to define terms that will be used in the rest of this thesis. The first section is a revision of terms common in general algebra, the second section is focused on polynomials and Gröbner bases and the last section will deal with elliptic curves. This chapter is based mostly on book by David A. Cox [1], MI-MKY lecture notes [2] and my bachelor thesis [3]. Other sources will be cited individually at the 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 logically deduce other properties of said algebraic structure 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 an elementary algebraic structure called group.

Definition 1.1.1. A **group** G is an ordered pair $(M, \circ)$, where M is a nonempty 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 are gonna talk about an element g of a group G ($g \in G$) we are actually gonna mean that g is an element of the underlying set M ($g \in M$).

Groups satisfying 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 $(\mathbb{Z}, +)$, set of all integers equipped with standard addition. An example of a finite Abelian group is $\mathbb{Z}_n^+ = (\{0, 1, \ldots, n-1\}, +_n),\ n \in \mathbb{N}$, 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 exist just one unique identity element. Also for every element $q \in G$ there exists just one inverse element denoted q^{-1} in the multiplicative notation and $-q$ in the additive notation. 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 mostly concerned about commutative groups.

Identity element in the additive notation is called **zero** and denoted by 0, in the multiplicative notation **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:

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

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 it by $\#a = k$, 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 and in this thesis we are mostly interested in finite groups). Elements of finite order are sometimes called **torsion** elements.

Remark. Order of the identity element $\in G$ 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 exactly the same, therefore the identity element $e \in G$ has to be the 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. A **relation** $\mathcal{R}$ on a set M is any subset of the Cartesian product $M \times M$. Relation $\mathcal{R}$ on the set M is an **equivalence** on the set M if and only if $\mathcal{R}$ satisfies following requirements:

- $\forall x \in M : (x, x) \in \mathcal{R}$, (reflexivity)
- $\forall x, y \in M : (x, y) \in \mathcal{R} \implies (y, x) \in \mathcal{R}$, (symmetry)
- $\forall x, y, z \in M : \Big((x, y) \in \mathcal{R} \wedge (y, z) \in \mathcal{R}\Big) \implies (x, z) \in \mathcal{R}$. (transitivity)

Set of all elements equivalent to $x \in M$ is called an **equivalence class** of an element x and denoted by:

$$[x]_{\mathcal{R}} := \{y \in M \mid (x, y) \in \mathcal{R}\}.$$

Notational Remark. Let $\mathcal{R}$ be an equivalence relation on a set M, to denote the equivalence of $x, y \in M$ we will shorten the notation to $x \sim_{\mathcal{R}} y := (x, y) \in \mathcal{R}$.

For any subgroup H of a group G and an element $a \in G$, we define a **left coset** of H as $aH := \{ah \mid h \in H\}$. Similarly a **right coset** of H is defined as $Ha := \{ha \mid h \in H\}$. We also define an equivalence relation $\sim_{\mathcal{H}}$ by:

$$x, y \in G : (x \sim_{\mathcal{H}} y) \Leftrightarrow (\exists h \in H : x = yh).$$

The equivalence classes ($[a]_{\mathcal{H}} = \{ah \mid h \in H\}$) of the equivalence relation $\sim_{\mathcal{H}}$ are exactly the left cosets of H so we can write $[a]_{\mathcal{H}} = aH$. Thus the left cosets of H form a partition of G, see [4].

Remark. If G is an Abelian group and H is any subgroup of G, the left cosets of H are the same as the right cosets of H, H is then called **normal subgroup** of G.

$$\forall a \in G : aH = Ha.$$

In the case H is a normal subgroup of G we can extend the group law ($\circ$) of G to the the set of (left) cosets of H as follows:

$$\forall a, b \in G : [a]_{\mathcal{H}} \circ [b]_{\mathcal{H}} := [a \circ b]_{\mathcal{H}}.$$

Definition 1.1.7. The ordered pair $(\{[a]_{\mathcal{H}} \mid a \in G\}, \circ)$ forms a **factor group** (sometimes called a **quotient group**) of G with respect to H and we denote it by G/H.

Definition 1.1.8. 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 $a \in G$. Order of the group generated by the element a is the same as order of the element a.

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

Definition 1.1.9. An (unital) **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. operation $\cdot$)
- $\forall x, y, z \in M : x \cdot (y + z) = x \cdot y + x \cdot z$, (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 are gonna talk about an element r of a ring R ($r \in R$) we are actually gonna mean that r is an element of the underlying set M ($r \in M$).

Definition 1.1.10. Let $R = (M, +, \cdot)$ be an unital ring and $(M \setminus \{0\}, \cdot)$ be an Abelian group, then $\mathbb{F} = (M, +, \cdot)$ is a **field**. 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. 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 1.1.11. 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 $\mathrm{char}(\mathbb{F})$.

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 1.1.12. 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 $\mathbb{F}$. Field extension $\mathbb{T}$ 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 the field $\mathbb{F}$ by $\mathbb{F}^n$, $n \in \mathbb{N}$.

Remark. The finiteness of the 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

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 order of a zero polynomial is set to $-\infty$.

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

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 $\mathbb{Z}[x, y, z]$ and $\deg(f) = 9$.

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

Definition 1.2.4. 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 obviously symmetric.

Definition 1.2.5. 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 1.2.6. 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 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 1.2.7. Let R be an commutative ring, then any non-empty subset $I \subseteq R$ is called a (two-sided) **ideal** of R if it satisfies following requirements:

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

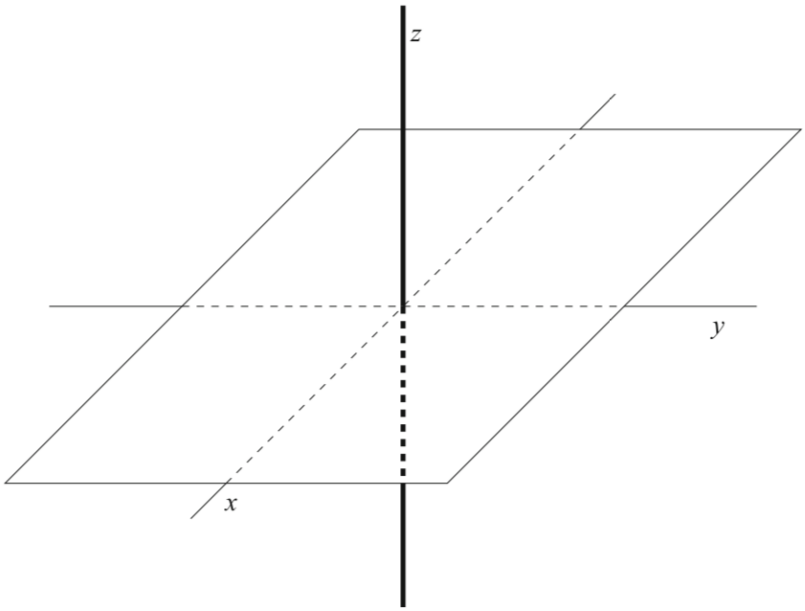

Figure 1.1: Affine variety defined by (xz, yz). Image source: ([1], page 9).

Definition 1.2.8. 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 these 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 1.2.9. 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:

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

1.2.1 Monomial Ordering

The notion of ordering of terms in polynomial is a key ingredient in many algorithms, e.g. 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 $X = (x_1, \ldots, x_n)$. 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 $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$. Based on this observation we can define an ordering $>$ on the space $\mathbb{Z}^n_{\geq 0}$ which will 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 will also say that $X^\alpha > X^\beta$. We will 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 1.2.10. A **monomial ordering** $>$ on $\mathbb{F}[X]$, where $X = (x_1, \ldots, x_n)$ is a relation $>$ on $\mathbb{Z}^n_{\geq 0}$ satisfying:

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

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

Now we will define a couple of standard monomial orderings.

Definition 1.2.11. 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 generalization 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 will 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 the thesis we will also assume $x >_{lex} y >_{lex} z$, unless stated otherwise.

Definition 1.2.12. 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 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 $|\alpha| = 18 > |\beta| = 17$.
- $(7, 5, 3, 1) >_{grlex} (7, 5, 1, 3)$, since $|\alpha| = 16 = |\beta|$ and $\alpha >_{lex} \beta$.
- The variables $x_1, \ldots, x_n$ are ordered 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 1.2.13. 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 $x_1, \ldots, x_n$ are ordered the same way as by $>_{lex}$ order:

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

Now we will 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 those standard monomial orderings.

- With respect to the lex order, we would reorder the terms of f in decreasing order:

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

- With respect to grlex order:

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

- With respect to 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 1.2.14. 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:

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

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

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

  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 that 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 can be read as **q divides p**.

Definition 1.2.15. 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

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

The algorithm itself will be presented in the chapter **??**. Unfortunately, the remainder is not uniquely characterized 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 will try to describe a "good" basis of the ideal I, such that the remainder r on division by the polynomials of this basis will be uniquely determined and that the condition $r = 0$ will be equivalent to the membership in the ideal. Exactly those good properties have Gröbner bases which we are gonna describe in the following section.

1.3 Gröbner Bases

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 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 $I = \langle X^{\alpha(1)}, \ldots, X^{\alpha(s)} \rangle$, $s \in \mathbb{N}$, where $\alpha(1), \ldots, \alpha(s) \in A$. In particular, I has a finite basis $(X^{\alpha(1)}, \ldots, X^{\alpha(s)})$.

Definition 1.3.2. A monomial ideal $I \subseteq \mathbb{F}[X]$ has a finite basis $(X^{\alpha(1)}, \ldots, X^{\alpha(s)})$ 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 ordering 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 $g_1, \ldots, g_t \in I$, $t \in \mathbb{N}$, such that:
$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle.$$

Definition 1.3.4. Fix a monomial order on $\mathbb{F}[X]$, therefore every polynomial $f \in \mathbb{F}[X]$ has an unique leading term. A finite subset $G = \{g_1, \ldots, g_t\}$ of an

ideal $I \subseteq \mathbb{F}[X],\ I \neq \{0\}$ is said to be a **Gröbner basis** (or **standard basis**) if:

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

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. The theory of Gröbner bases was developed by B. Buchberger in his PhD thesis (1965) and named after 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 $G = \{g_1, \ldots, g_t\}$ be a Gröbner basis of I. Then for any $f\mathbb{F}[X]$, there is an unique polynomial r with those two properties:

- No term of r is divisible by any of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$.
- $\exists g \in I :\ f = g + r$. 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 $f \in \mathbb{T}[X]$ be an polynomial and let $F = (f_1, \ldots, f_s) \subseteq \mathbb{T}[X]$ 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 $\langle f_1, \ldots, f_s \rangle$, then we can regard F as a set without any particular order, because the remainder on the division by a Gröbner basis is unique.

Chapter 2

Elliptic Curves and Discrete Logarithm Problem

2.1 Elliptic Curves

This section's main focus will be elliptic curves and groups of points on those elliptic curves. At first we are going to define what is a general elliptic curve, after that we will define an operation on the set of points on elliptic curve that with "the point in infinity" form an Abelian group. 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:

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

where $A, B \in GF(p)$ are **coefficients of the elliptic curve** and the **discriminant** of the elliptic curve, denoted by Δ, is non-zero. Point $\mathcal{O}$ is called the **point at infinity** (in the projective plane).

$$\Delta = -16(4A^3 + 27B^2) \neq 0.$$

Curves satisfying this condition are called **non-singular** and the right-hand-side polynomial $(x^3 + Ax + B)$ in x has 3 distinct roots.

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 can now state the explicit formula for the point $\ominus P$, we know its x-coordinate is x_1, and we will 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 and we already know one of its roots, which is y_1, the other root has to be $-y_1$, therefore point $\ominus P = (x_1, -y_1)$.

- 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 $\frac{\mathrm{d}E}{\mathrm{d}X}, \frac{\mathrm{d}E}{\mathrm{d}Y}$ is the derivative 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, or if we want to explicitly mention the coefficients A, B and the prime field $GF(p)$, we use $E(A, B, p)$.

Notational Remark. Let $P \in E$ be a point on an elliptic curve E with group operation $\oplus$. To shorten the notation of the repeated application of the group law we will use the notation introduced in chapter 1. To remind our readers: **multiplication** of a point on the elliptic curve E by an integer has the following meaning:

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

Remark. The complexity of arithmetic operations on E is based on the complexity of operations in the underlying finite field $GF(p)$. Exact number of arithmetic operations depends on the used algorithm and on the architecture of the CPU where it's executed. Table 2.1 provides a brief summary of the relationship between the operations on elliptic curve E and number of arithmetic operations in the underlying finite field $GF(p)$. Addition in $GF(p)$ is denoted by a_p, multiplication in $GF(p)$ is denoted by $\cdot_p$, 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 the arithmetic operations on the elliptic curve E over $GF(p)$.

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 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 the Lagrange's theorem 1.1.5.

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

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.

Definition 2.1.4.

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: $x = \log_b(y)$, 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 x_0, evaluate b^{x_0},

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

compare it with y and we would immediately know whether the solution x is bigger/equal/lesser than x_0.

If we were given the same problem in a finite group, instead of over the real numbers, the situation would be significantly more complicated.

Definition 2.2.1. Let $G = (M, \cdot)$ be a 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 $x \in \{1, 2, \ldots, \#G\}$. 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 have decided to demand 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 $GF(19)$. $G = (\{1, 2, \ldots, 18\}, \cdot_{19})$ 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 $3^k \equiv 4 \pmod{19}$.

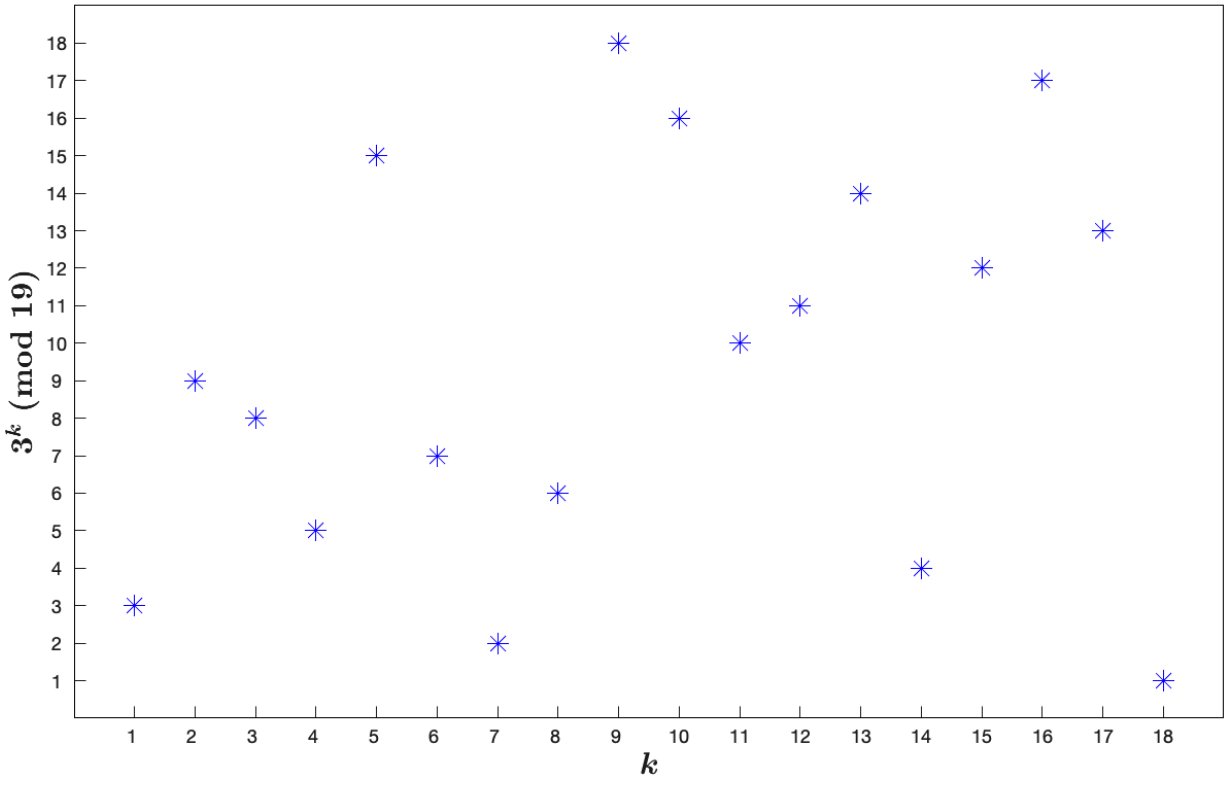

Figure 2.1: Powers of the generator $g = 3$ in $GF(19)^\times$. Image was created by the author himself.

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 $k \in \{0, 1, \ldots, 17\}$ and find the answer. 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 $xP = Q \in G,\ x \in \{0, 1, \ldots, \#E - 1\}$, 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.
- $0P = \mathcal{O}, P, 2P, \ldots, (n-1)P,$ (baby-step phase)
  next generate multiples of Q and try to find it in the list generated in the baby-step phase.
- $Q \oplus (0 \cdot n \ominus P) = Q, Q \oplus (1 \cdot n \ominus P), Q \oplus (2 \cdot n \ominus P), \ldots, Q \oplus ((n-1) \cdot n \ominus P),$ 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:

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

The algorithm is deterministic and is guaranteed to find the solution, because it basically tries all the possible values of x. Every number in $\{0, 1, \ldots, N-1\}$ can be expressed as $i + jn,\ n = \left\lceil \sqrt{N} \right\rceil, i, j \in \{0, 1, \ldots, n-1\}$. 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 idea): 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.

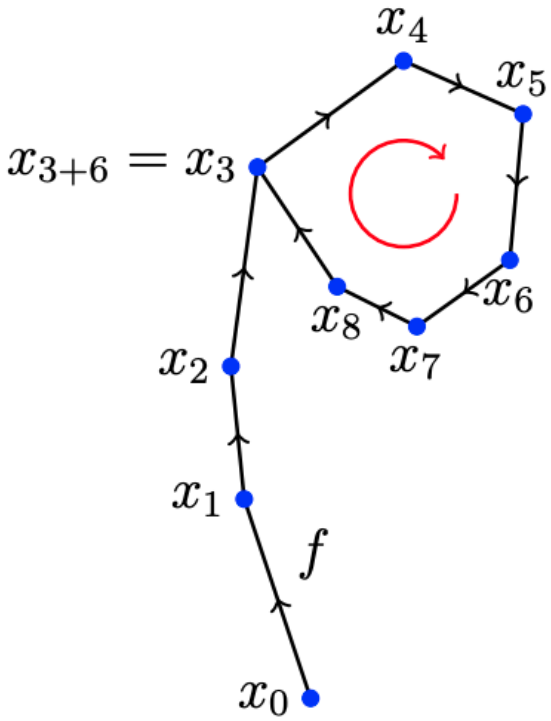

Figure 2.2: Graphical illustration of the idea behind the Pollard ρ algorithm. $T = 3$, length of the cycle $M = 6$. Image source: ([2], page 70).

Definition 2.3.3. The Pollard ρ idea might be used to solve the ECDLP. Let E be an elliptic curve group with points' coordinates $\in GF(p)$, let P be its 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 $k \in \mathbb{Z}_{\geq 0}$:

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

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

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 $y \bmod(\frac{N}{d})$ in the same fashion:

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

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.

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.

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 $17P = (13, 26) = Q$.

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 developed by Stephen Pohlig and Martin Hellman in 1978 in their article [8].

Definition 2.3.4. Let $m_i \in \mathbb{N},\ i \in \{1, \ldots, k\}$, be mutually relatively prime integers, and $N = \prod_i = 1^k m_i,\ a_i \in \mathbb{Z},\ i \in \{1, \ldots, k\}$.. The following system of congruences:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \quad \vdots \\ x &\equiv a_k \pmod{m_k}, \end{aligned}$$

has a solution c:

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

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.

2.4 Specific algorithms for solving ECDLP

Chapter 3

Realisation in SageMath

Chapter 4

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] BRAY, Nicolas. *Coset.* From MathWorld-A Wolfram Web Resource [online], created by Eric W. Weisstein. [Accessed on 16-04-2019]. Available at : `http://mathworld.wolfram.com/Coset.html`

[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 logarithms.* 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.

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

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