



**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 16, 2019

Acknowledgements

THANKS (remove entirely in case you do not wish 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 16, 2019

.....

Czech Technical University in Prague

Faculty of Information Technology

© 2019 Matyáš Hollmann. All rights reserved.

This thesis is school work as defined by Copyright Act of the Czech Republic. It has been submitted at Czech Technical University in Prague, Faculty of Information Technology. The thesis is protected by the Copyright Act and its usage without author's permission is prohibited (with exceptions defined by the Copyright Act).

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

Introduction	1
1 Mathematical background	3
1.1 Introduction to general algebra	3
1.2 Multivariate polynomials	7
1.3 Gröbner bases	15
2 Discrete logarithm problem on elliptic curves	17
3 State-of-the-art	19
4 Algorithms	21
5 Analysis and design	23
6 Realisation	25
Conclusion	27
Bibliography	29
A Acronyms	31
B Contents of enclosed CD	33

List of Figures

1.1	Example of an affine variety	9
-----	--	---

Introduction

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 location.

1.1 Introduction to general algebra

Definition 1.1.1. A **group** G is an ordered pair (M, \circ) , where M is a non-empty set and binary operation $\circ : M \times M \rightarrow M$ (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 $\mathbb{Z}_n^+ = (\{0, 1, \dots, n-1\}, +_n)$, $n \in \mathbb{N}$, 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 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:

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

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

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

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 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. 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)
- $\forall x, y, z \in M : \left((x, y) \in \mathcal{R} \wedge (y, z) \in \mathcal{R} \right) \implies (x, z) \in \mathcal{R}$. (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 1.1.6. 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 1.1.7. Group G is called a **cyclic group** if and only if there exists an element $g \in G$ such that:

1. MATHEMATICAL BACKGROUND

- $G = \langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$, (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 1.1.8. An (unital) **ring** $R = (M, +, \cdot)$ is a set equipped with two binary operations $+: M \times M \rightarrow M$ and $\cdot: M \times M \rightarrow M$ 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 1.1.9. 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 1.1.10. 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 $n \in \mathbb{N}$:

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

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 $\text{char}(\mathbb{F})$.

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 $(\{0, 1, \dots, p-1\}, +_p, \cdot_p)$.

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

Definition 1.1.11. 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, \dots, x_n is a product of the form:

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

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

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

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

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

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

1. MATHEMATICAL BACKGROUND

Definition 1.2.3. A **polynomial** f over a field \mathbb{F} in variables $X = (x_1, x_2, \dots, x_n)$ 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 $\alpha = (\alpha_1, \dots, \alpha_n)$, 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 $X = (x_1, \dots, x_n)$) can be viewed as a function $f(x_1, \dots, x_n) : \mathbb{F}^n \rightarrow \mathbb{F}$.

Definition 1.2.4. A polynomial $f \in \mathbb{F}[X]$ is called **symmetric** if and only if:

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

for every possible permutation x_{i_1}, \dots, x_{i_n} of the variables x_1, \dots, 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, \dots, f_s , $s \in \mathbb{N}$, be polynomials in $\mathbb{F}[x_1, \dots, x_n]$. Then the set of their common zeroes:

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

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

Thus, an affine variety $\mathcal{V}(f_1, \dots, f_s) \subseteq \mathbb{F}^n$ is the set of all solutions of the system of equations $f_1(x_1, \dots, x_n) = \dots = f_s(x_1, \dots, x_n) = 0$ 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.

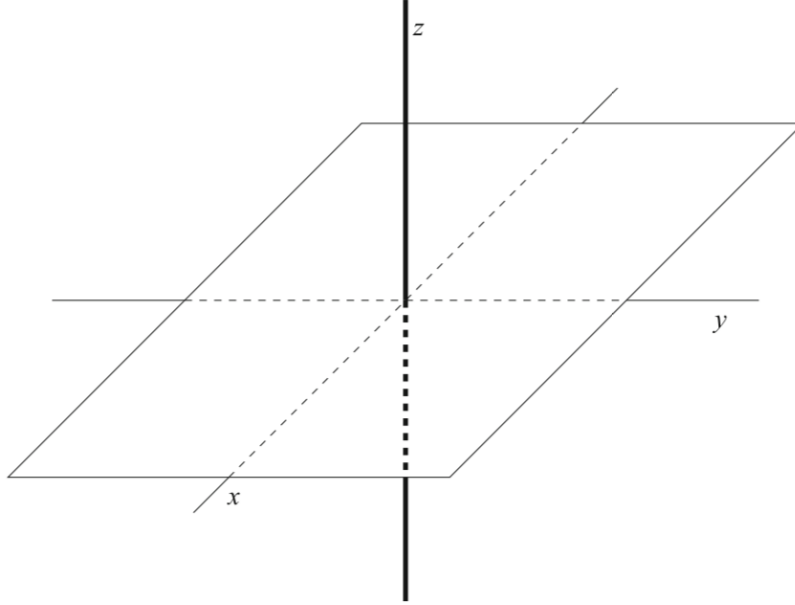


Figure 1.1: Affine variety defined by (xz, yz) . Image source: ([1], page 9).

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.

Definition 1.2.8. Let $X = (x_1, \dots, x_n)$ be an ordered n -tuple of formal variables and let $f_1, \dots, f_s \in \mathbb{F}[X]$ be an s -tuple of polynomials. Then we set

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

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

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

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

and we say that these polynomials f_1, \dots, f_s form a **basis** of I . Note that a given ideal I may have many different bases. If we have two different bases $B_1 = (f_1, \dots, f_s)$, $s \in \mathbb{N}$, and $B_2 = (g_1, \dots, g_t)$, $t \in \mathbb{N}$, 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 $X = (x_1, \dots, x_n)$ 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 $\mathbf{I}(\mathcal{V}(f_1, \dots, f_s)) = \langle f_1, \dots, f_s \rangle$. The answer, unfortunately, is not always yes, but the following set inclusion holds:

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

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:

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

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 $X^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}$ from the n -tuple of exponents $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$. Based on this observation we can define an ordering $>$ on the space $\mathbb{Z}_{\geq 0}^n$ which will

also gives us an ordering on the monomials $\in \mathbb{F}[X]$. If for some $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$ 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:

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

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

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

Which in terms of the exponent vectors means:

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

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

Definition 1.2.10. A **monomial ordering** $>$ on $\mathbb{F}[X]$, where $X = (x_1, \dots, x_n)$ is a relation $>$ on $\mathbb{Z}_{\geq 0}^n$ satisfying:

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

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

Now we will define a couple of standard monomial orderings.

Definition 1.2.11. Let $\alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$. **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:

1. MATHEMATICAL BACKGROUND

- $(10, 4, 3) >_{lex} (10, 3, 4)$, 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, \dots, x_n are ordered in the usual way by the lexicographic order:

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

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

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

Definition 1.2.12. Let $\alpha = (\alpha_1, \dots, \alpha_n)$, $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$. **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, \dots, x_n are ordered the same way as by $>_{lex}$ order:

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

Definition 1.2.13. Let $\alpha = (\alpha_1, \dots, \alpha_n)$, $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$. **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 the same way as by $>_{lex}$ order:

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

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 $xy^2z >_{\text{grevlex}} x^2z^2$ 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:

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

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:

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

1. MATHEMATICAL BACKGROUND

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 let's use $>_{\text{grevlex}}$ order.

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

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 $\mathbb{Z}_{\geq 0}^n$, let $F = (f_1, \dots, f_s)$ be an ordered s -tuple of polynomials in $\mathbb{F}[X]$, where $\bar{X} = (x_1, \dots, x_n)$. Then every $f \in \mathbb{F}[X]$ can be written as:

$$f = q_1f_1 + \dots + q_sf_s + r,$$

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 $\text{LT}(f_1), \dots, \text{LT}(f_s)$. We call polynomial r a **remainder** of f on division by F . Furthermore, if $q_if_i \neq 0$, then

$$\text{multideg}(f) \geq \text{multideg}(q_if_i).$$

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 $f, f_1, \dots, f_s \in \mathbb{F}[X]$ and let $I = \langle f_1, \dots, f_s \rangle$ 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 $F = (f_1, \dots, f_s)$ 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 $A \subseteq \mathbb{Z}_{\geq 0}^n$ 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^{β} , $\beta \in \mathbb{Z}_{\geq 0}^n$, 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 $I = \langle X^{\alpha(1)}, \dots, X^{\alpha(s)} \rangle$, $s \in \mathbb{N}$, 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 ordering on $\mathbb{F}[X]$. Then:

- We denote by $\text{LT}(I)$ the **set of leading terms** of non-zero elements of I .

$$\text{LT}(I) = \{cX^{\alpha} \mid \exists f \in I \setminus \{0\} : \text{LT}(f) = cX^{\alpha}\}.$$

- We denote by $\langle \text{LT}(I) \rangle$ the **ideal of leading terms** of I . $\langle \text{LT}(I) \rangle$ is a monomial ideal, therefore there exist a finite set $g_1, \dots, g_t \in I$, $t \in \mathbb{N}$, such that:

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

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 $G = \{g_1, \dots, g_t\}$ of an ideal $I \subseteq \mathbb{F}[X]$, $I \neq \{0\}$ is said to be a **Gröbner basis** (or **standard basis**) if:

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

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.

Discrete logarithm problem on elliptic curves

State-of-the-art

Algorithms

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

Analysis and design

Realisation

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>

Acronyms

GUI Graphical user interface

XML Extensible markup language

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