

MPI - Lecture 7

Outline

- A more complicated group: Points in elliptic curves;
- Rings and fields;
- Finite fields in general;
- Binary fields.

Elliptic curves

Calculation on elliptic curves

On elliptic curves, we use points (x, y) with x and y being the residue classes modulo some prime number p .

The operation, which is usually denoted by $+$, is defined as follows:

Definition 1 (Don't even try to memorize it!). For two points $\mathcal{P} = (x_1, y_1)$ and $\mathcal{Q} = (x_2, y_2)$, we define $\mathcal{P} + \mathcal{Q} = (x_3, y_3)$ as:

$$\begin{aligned}x_3 &\equiv s^2 - x_1 - x_2 \pmod{p} \\ y_3 &\equiv s(x_1 - x_3) - y_1 \pmod{p}\end{aligned}$$

where

$$s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \pmod{p} & \text{if } \mathcal{P} \neq \mathcal{Q} \\ \frac{3x_1^2 + a}{2y_1} \pmod{p} & \text{if } \mathcal{P} = \mathcal{Q}. \end{cases}$$

The parameter a is taken from the equation of a given elliptic curve $y^2 \equiv x^3 + ax + b \pmod{p}$, with $a, b \in \mathbb{Z}_p$, which must be fulfilled by all points. The neutral element \mathcal{O} is “artificially” defined such that it has the properties of the neutral element.

To better understand what is happening on elliptic curves, we consider points (x, y) from the *continuous* plane \mathbb{R}^2 .

Elliptic curves
over the field
of real numbers
(1/3)

Definition 2. An *elliptic curve* is the set of points given by the equation

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

where the real coefficients a, b satisfy $4a^3 + 27b^2 \neq 0$.

The group operation can be defined by geometrical means (see [Wolfram Demonstrations Project](#)).

When we add two points $\mathcal{P} = (x_1, y_1)$ and $\mathcal{Q} = (x_2, y_2)$, we plot a line through \mathcal{P} and \mathcal{Q} and we look for intersections of this line and the elliptic curve.

Elliptic curves
over the field
of real numbers
(2/3)

Or if you don't like the drawings and really want the exact formula:

- If $\mathcal{P} \neq \mathcal{Q}$, the line going through \mathcal{P} and \mathcal{Q} has equation

$$y = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1) + y_1 = \frac{y_2 - y_1}{x_2 - x_1}(x - x_2) + y_2.$$

- If $\mathcal{P} = \mathcal{Q} = (x_1, y_1)$, a tangent line to the elliptic curve at $\mathcal{P} = \mathcal{Q}$ has slope given by the derivative of the curve $y = \sqrt{x^3 + ax + b}$ at x_1 , which is $\frac{3x_1^2 + a}{2\sqrt{x_1^3 + ax_1 + b}} = \{\text{for } x = x_1\} = \frac{3x_1^2 + a}{2y_1}$, and thus the line has equation

$$y = \frac{3x_1^2 + a}{2y_1}(x - x_1) + y_1.$$

Now, we are looking for intersections of some line $y = sx + d$, where s is the slope and $d \in \mathbb{R}$, and the elliptic curve $y^2 = x^3 + ax + b$.

Elliptic curves
over the field
of real numbers
(3/3)

This leads to solving the equation

$$(sx + d)^2 = x^3 + ax + b,$$

i.e., a polynomial equation of order 3, which can have 1, 2 or 3 real roots (we have always at least one solution; namely the points \mathcal{P} and \mathcal{Q}).

For instance, the situation where we obtain only two roots for distinct \mathcal{P} and \mathcal{Q} corresponds to $\mathcal{Q} = -\mathcal{P}$ and the result of the sum is the neutral element \mathcal{O} .

In general, the solution of the equation is obtained in this way: For two points $\mathcal{P} = (x_1, y_1)$ and $\mathcal{Q} = (x_2, y_2)$ define $\mathcal{P} + \mathcal{Q} = (x_3, y_3)$ as:

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

where

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

Elliptic curves
over a general
field

The previous three slides show how to define a group over the set of points in the plane $\mathbb{R} \times \mathbb{R}$.

Generally, instead of the set \mathbb{R} we could take an arbitrary field, e.g., the field \mathbb{Z}_p , where the discrete logarithm problem is difficult to solve.

Field, what is that?

Generally speaking, it is a set with two binary operations (usually called *addition* and *multiplication*) which allow us to define analogues of common arithmetical operations such as subtracting, dividing, raising to the power, logarithm, etc.

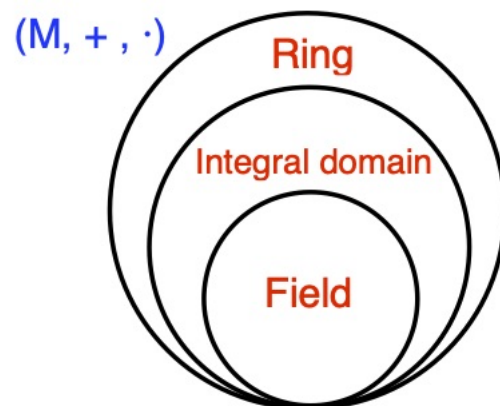
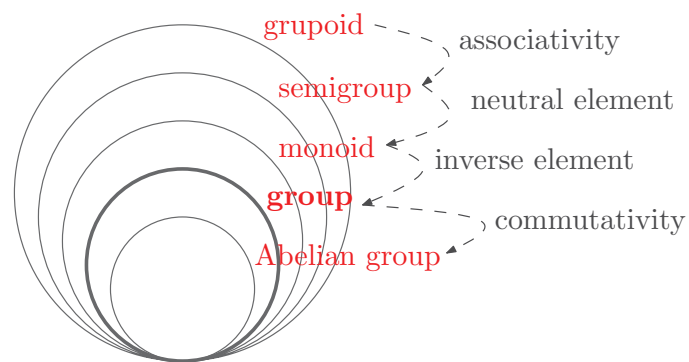
Rings and fields

Sets with one binary
operation

A nonempty set M with a binary operation \cdot (resp. $+$ for the additive notation).

Sets with
two binary
operations

For more sophisticated arithmetical operations with numbers we need **both** addition and multiplication.



Rings

Definition of a ring

Definition 3 (Ring). Let M be a nonempty set, and $+$ and \cdot two binary operations. We say that $R = (M, +, \cdot)$ is a *ring* if the following holds:

- $(M, +)$ is an *Abelian group*,
- (M, \cdot) is a *monoid*,
- both left and right *distributive law* hold:

$$(\forall a, b, c \in M) \text{ we have: } a(b + c) = ab + ac \quad \wedge \quad (b + c)a = ba + ca.$$

We respect the standard convention that the multiplication has a higher priority than the addition (and use the concatenation, instead of \cdot , when it is clear from the context).

Sometimes, (M, \cdot) is required to be only a semigroup (or even a groupoid).

Terminology

Let $R = (M, +, \cdot)$ be a ring.

- If \cdot is associative, R is an **associative ring**.
- If \cdot is commutative, R is a **commutative ring**.
- $(M, +)$ is called the **additive group** of the ring R .
- (M, \cdot) is called the **multiplicative groupoid/semigroup/monoid** of the ring R .
- The neutral element of the group $(M, +)$ is called the **zero element** and is denoted by 0 ; the inverse element to $a \in M$ is denoted as $-a$.
- Inside the ring **we can define the operation subtraction** by

$$a - b := a + (-b).$$

Examples

- $(\mathbb{N}, +, \cdot)$ is not a ring, because $(\mathbb{N}, +)$ is not a group.
- $(\mathbb{Z}, +, \cdot)$ is a ring.
- The **trivial ring** is $(\{0\}, +, \cdot)$ (if it holds that $0 \cdot 0 = 0$).
- The set $(\mathbb{R}^{n,n}, +, \cdot)$ of square real matrices with the usual addition and multiplication is a ring; the zero element is the zero matrix.

- The set of all polynomials (with complex / real / integer coefficients) is a ring; the zero element is the zero polynomial $p(x) = 0$.

Basic properties
of rings

In an arbitrary ring $(M, +, \cdot)$, the following holds.

- Left and right distributive law for subtracting, i.e.,

$$c(b - a) = cb - ca.$$

Indeed:

$$ca + c(b - a) = c(a + b - a) = cb \implies c(b - a) = cb - ca.$$

□

- Multiplying by the zero element returns the zero element, i.e.,

$$\forall a \in M \quad a \cdot 0 = 0 \quad \wedge \quad 0 \cdot a = 0.$$

Indeed:

$$a \cdot 0 = a(a - a) = aa - aa = 0.$$

□

Integral domains

Integral domain

Definition 4 (zero divisors). *Let $R = (M, +, \cdot)$ be a ring. Two arbitrary **nonzero** elements $a, b \in M$ such that*

$$a \cdot b = 0$$

*are called **zero divisors**.*

Definition 5 (integral domain). A commutative ring **without** zero divisors is called an *integral domain*.

Examples of integral domains

- $(\mathbb{Z}, +, \cdot)$ is an integral domain.
- Each number ring $(M, +, \cdot)$, where $M \subset \mathbb{C}$ and $+$ and \cdot are classical, is an integral domain.
- The ring $(\mathbb{R}^{n,n}, +, \cdot)$ is **not** an integral domain for $n \geq 2$, because it is not commutative; moreover, it has zero divisors:

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Fields

Definition of field

Definition 6 (field). A ring $T = (M, +, \cdot)$ is a *field* if $(M \setminus \{0\}, \cdot)$ is an Abelian group. This group is called the *multiplicative group* of the field T .

Why do we have to remove the zero element?

Because the zero has no inverse (with respect to the multiplication), i.e., it is not possible to divide by zero: $0^{-1} = ?!$.

We can divide by all other elements of the field!

dividing := multiplying by the inverse element

$$\frac{a}{b} := a \cdot b^{-1} \quad \text{for } b \neq 0.$$

Examples of fields

- The ring of integers $(\mathbb{Z}, +, \cdot)$ is **not** a field, because $(\mathbb{Z} \setminus \{0\}, \cdot)$ misses some inverse elements.
- The ring of rational numbers $(\mathbb{Q}, +, \cdot)$ is a field. Moreover, it is the smallest number field (with the common arithmetical operations).
- The smallest field is the so-called **trivial field** $(\{0, 1\}, +, \cdot)$, with operations given by the following tables:

$$\begin{array}{c|c|c}
 + & 0 & 1 \\
 \hline
 0 & 0 & 1 \\
 \hline
 1 & 1 & 0 \\
 \hline
 \end{array}
 \quad \text{and} \quad
 \begin{array}{c|c|c}
 \cdot & 0 & 1 \\
 \hline
 0 & 0 & 0 \\
 \hline
 1 & 0 & 1 \\
 \hline
 \end{array}$$

The first table corresponds to the bit operation **XOR** and the latter to **AND**, or, alternatively, to the addition and multiplication modulo 2.

Some properties

In each field all usual arithmetical operations are defined: *addition, subtraction, multiplication, division*, and all operations derived from them such as *rising to the power, root extractions, logarithm, ...*

Using the trivial field we have all these operations over one bit. Later we will show how to extend them to any number of bits.

Theorem 7. *Each field is an integral domain.*

Proof. Since the multiplicative group of the field $(M \setminus \{0\}, \cdot)$ is closed under multiplication, for all nonzero a, b it holds that their product $a \cdot b \in M \setminus \{0\}$ is again nonzero. \square

Homomorphisms

Definition 8. A mapping f from the ring (resp. field) R_1 to the ring (resp. field) R_2 is a *homomorphism* if f is a homomorphism of the corresponding additive and multiplicative groupoids (resp. groups).

If, moreover, f is bijective (injective and surjective), it is an *isomorphism*.

Homomorphism
and isomor-
phism

Finite fields

Definitions

A field with finite number of elements is called *finite*.

The number of elements is said to be the *order* of the field.

An example of finite field is the set (of residue classes modulo p)

$$\mathbb{Z}_p = \{0, 1, \dots, p-1\}$$

with operations modulo a **prime** p (see previous lectures).

E.g., for $p = 5$ we obtain the field with following operations:

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

and

\cdot_5	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

\mathbb{Z}_p

Additive group
($\mathbb{Z}_p, +_p$)

- The order of the group $\mathbb{Z}_p^+ = (\mathbb{Z}_p, +_p)$ is the prime number p .
- Each nonzero element is a generator (this holds for all groups with prime order).

- $(\mathbb{Z}_p, +_p)$ is a group even when p is not prime.

Multiplicative
group
 $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$

- The order of the group $\mathbb{Z}_p^\times = (\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ is $p - 1$ and this is never a prime number for $p \neq 3$!
- \mathbb{Z}_p^\times is cyclic (i.e., there exists a generator).
- The number of generators depends on $p - 1$, and is equal to the number of numbers coprime to $p - 1$, i.e., $\varphi(p - 1)$.
- If k with $k < p$ divides $p - 1$, then there exists a subgroup in \mathbb{Z}_p^\times of order k and it contains just the elements for which $a^k = 1$.

Order of fields

Orders of fields?

We have shown a construction of a finite field of order p with p prime.

Are there fields of any arbitrary order?

Theorem 9. *Any finite field has **order** p^n , where p is a prime number and n is a positive natural number. The prime number p is called the **characteristic** of the field.*

Furthermore, all fields of order p^n are isomorphic.

Additionally, the multiplicative group of a finite field is cyclic.

Consequence: There are no fields of order 6, 10, 12, 14, ...

If we chose $p = 2$ and $n = 8$, we obtain the field providing us with arithmetic on 1 byte (8 bits)!

Binary fields

Symmetric cryptography

Symmetric
cryptography

Secure exchange of longer text performed by asymmetric ciphers (RSA, Diffie-Hellman and others) is not effective.

That is why the **symmetric ciphers** are used: symmetric ciphers assume that (and take advantage of) Alice and Bob share some secret key.

Asymmetric ciphers are used only for exchanging this private key.

A very common method is the block cipher called **Advanced Encryption Standard (AES)**.

Here we get acquainted with the mathematics underlying this method.

AES block cipher

The text we want to securely transfer is divided into (e.g.) blocks having 8 bits. Then, these blocks are encoded using the shared key so that the decoding can be easily made using the same key.

This cipher AES is based on the fact that arithmetic operations with $n = 8$ bits can be understood as operations in a finite field with 2^n elements for $n = 8$.

The fields with 2^n elements are called **binary fields** and are denoted $GF(2^n)$ (as *Galois Fields*).

We now explain how to define addition and multiplication in these fields.

Addition and multiplication

The wrong way

Consider a field $GF(2^8)$. Each element can be represented as an 8 bit string, e.g., 11010110, 01100011, etc.

Addition: Addition can be defined component-wise modulo 2. i.e.

$$11010110 + 01100011 = (1 +_2 0)(1 +_2 1) \cdots (0 +_2 1) = 10110101.$$

The neutral (zero) element is 00000000, and each element is inverse to itself.

We have an additive group.

Multiplication: Multiplication cannot be defined component-wise: The neutral element would be 11111111 and the inverse to (e.g.) 11111110 would not exist.

Multiplication must be defined in a different way!

Polynomials

In order to be able to add, subtract, and multiply a polynomial of the form $\sum_i a_i x^i$, we only need to know how to add, subtract, and multiply the coefficients.

In general, we can construct a ring of polynomials over an arbitrary ring or field similar to the one we know from real or complex numbers.

Definition 10. Let K be a ring. The *commutative ring of polynomials over K* , denoted $K[x]$, is the set of polynomials with coefficients in K together with operations of addition and multiplication defined as:

$$\begin{aligned} \left(\sum_{i=0}^n a_i x^i \right) + \left(\sum_{i=0}^n b_i x^i \right) &= \sum_{i=0}^n (a_i + b_i) x^i; \\ \left(\sum_{i=0}^n a_i x^i \right) \cdot \left(\sum_{i=0}^m b_i x^i \right) &= \sum_{i=0}^{n+m} \left(\sum_{j+k=i} a_j b_k \right) x^i. \end{aligned}$$

Rings of polynomials over a ring / field

Irreducible polynomial

Definition 11. Let K be a field and $P(x) \in K[x]$ be of degree at least 1.

We say that $P(x)$ is *irreducible over K* if, for any two polynomials $A(x)$ and $B(x)$ from $K[x]$, it holds that

$$A(x) \cdot B(x) = P(x) \quad \Rightarrow \quad (\text{degree of } A(x) = 0 \quad \vee \quad \text{degree of } B(x) = 0).$$

Irreducible polynomials are primes among polynomials!

Their definition is analogous as well as their properties.

Example: Whereas $x^2 + 1$ is irreducible over the field \mathbb{Q} , the polynomial $x^2 - 1 = (x + 1)(x - 1)$ is not.

Remark: $x^2 + 1$ is irreducible over the field \mathbb{Q} , but not over the field \mathbb{Z}_2 , where the coefficients are added and multiplied modulo 2:

$$x^2 + 1 = (x + 1)(x + 1) = x^2 + 2x + 1.$$

Irreducible polynomial as a modulus

We define **modulo polynomial** as:

$A(x) \pmod{P(x)} :=$ the remainder of the division of $A(x)$ by $P(x)$.

The result is always a polynomial of degree less than the degree of $P(x)$.

Example: for $A(x) = x^3$ and $P(x) = x^2 + 1$ we have $A(x) = x(x^2 + 1) + (-x)$ and thus

$$x^3 \equiv -x \pmod{x^2 + 1}.$$

If $P(x)$ is irreducible (with respect to the field from which the coefficients are taken), the remainders after division by $P(x)$ form a group (if we again remove the zero polynomial).

$GF(2^4)$

Field $GF(2^4)$

The elements $GF(2^4)$ are represented as polynomials of order at most 3 with coefficients h_i from the field \mathbb{Z}_2 :

$$h_3x^3 + h_2x^2 + h_1x + h_0 \approx (h_3h_2h_1h_0)_2.$$

Thus, the 16 elements of $GF(2^4)$ are:

$$0, 1, x, x + 1, \dots, x^3 + x^2 + x + 1$$

or

$$0000, 0001, 0010, 0011, \dots, 1111.$$

Addition component-wise modulo 2:

$$(x^3 + x + 1) + (x^2 + x + 1) = x^3 + x^2.$$

Field $GF(2^4)$ –
multiplication

Multiplication modulo a chosen irreducible polynomial, e.g., $x^4 + x + 1$.

Example: multiplication $A(x) \cdot B(x)$ for $A(x) = x^3 + x^2 + 1 \approx 1101$ and $B(x) = x^2 + x \approx 0110$.

1. Multiply $A(x) \cdot B(x)$ classically and rewrite coefficients mod 2:

$$A(x) \cdot B(x) = x^5 + 2x^4 + x^3 + x^2 + x = x^5 + x^3 + x^2 + x.$$

2. Find the remainder after division by $P(x)$. Since

$$x^5 = x(x^4 + x + 1) + (x^2 + x), \quad \text{it holds } x^5 \equiv x^2 + x \pmod{x^4 + x + 1},$$

and we have

$$x^5 + x^3 + x^2 + x \equiv (x^2 + x) + (x^3 + x^2 + x) \equiv x^3 \pmod{x^4 + x + 1}.$$

Hence we get that $1101 \cdot 0110 = 1000 \pmod{x^4 + x + 1}$.

According to the specification of AES, the multiplication is done modulo

$$x^8 + x^4 + x^3 + x + 1.$$

General finite field

In general, we construct a finite field $GF(p^k)$ using polynomials as follows.

Let $m(x) \in \mathbb{Z}_p[x]$ be an irreducible polynomial of degree k .

$$GF(p^k) = \left(\{q(x) \in \mathbb{Z}_p[x] : \deg(q) < k\}, +, \cdot \text{ mod } m(x) \right).$$