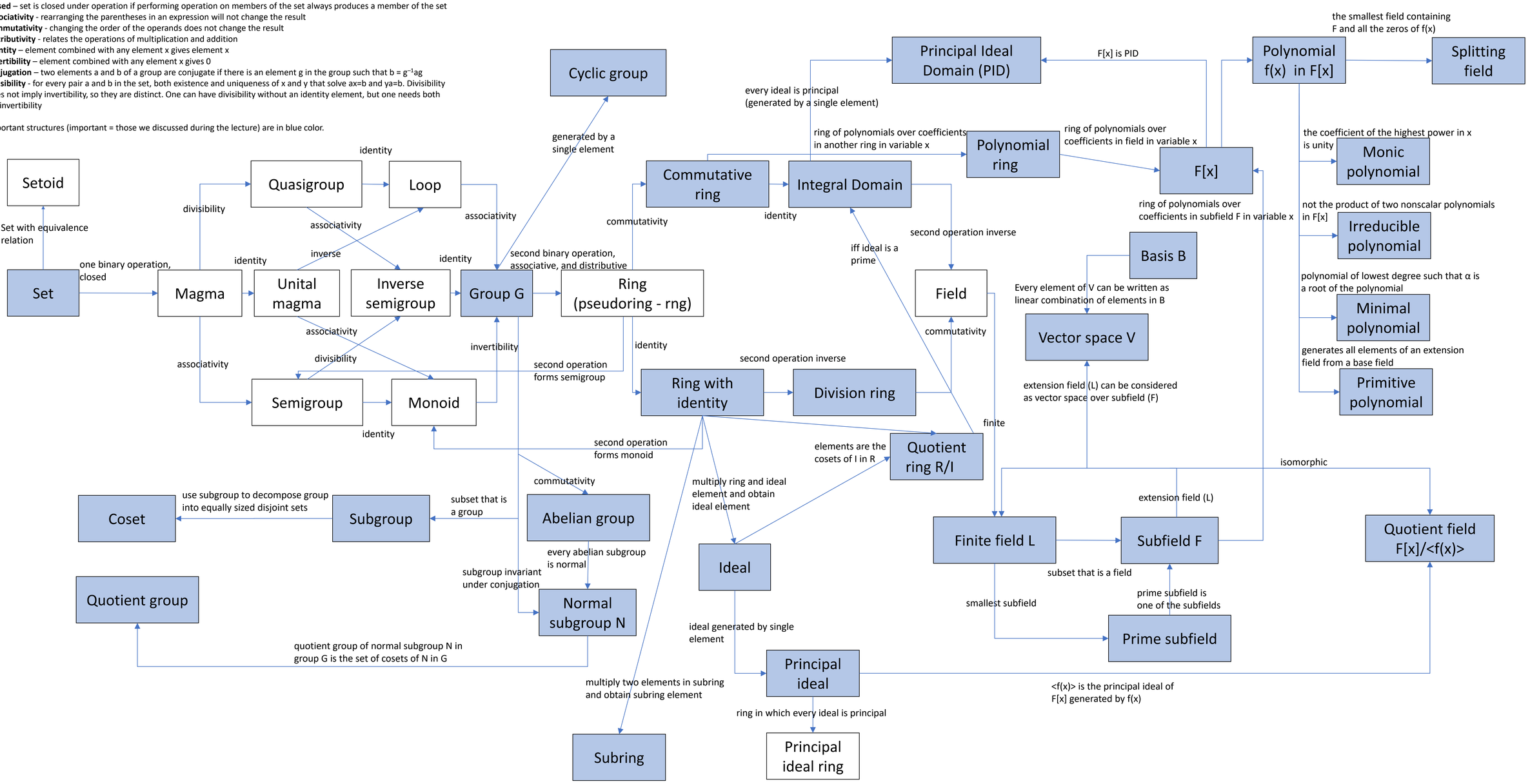
closed – set is closed under operation if performing operation on members of the set always produces a member of the set
associativity - rearranging the parentheses in an expression will not change the result
commutativity - changing the order of the operands does not change the result
distributivity - relates the operations of multiplication and addition
identity – element combined with any element x gives element x
invertibility – element combined with any element x gives 0
conjugation – two elements a and b of a group are conjugate if there is an element g in the group such that b = $g^{-1}ag$
divisibility - for every pair a and b in the set, both existence and uniqueness of x and y that solve ax=b and ya=b. Divisibility does not imply invertibility, so they are distinct. One can have divisibility without an identity element, but one needs both for invertibility

Important structures (important = those we discussed during the lecture) are in blue color.



Algebra & Cryptography CSE3230

Lecture 3 – Introduction to basic properties of integers

Stjepan Picek

Recap – Previous Lecture

- Basic notions on block ciphers and SPN networks
- Overview of AES
- Basic notions on public key ciphers
- Overview of RSA

Takeaway: Algebra plays a key role in modern ciphers, e.g.:

- Polynomials over the finite field $\mathbb{F}_{2^8}$ in the confusion and diffusion layer of AES
- Primality testing algorithms and the Extended Euclidean Algorithm to generate the public/private key pair in RSA

This Lecture

Goal: Introduction to basic properties and algorithms on integers

Outline:

- Greatest common divisor and Euclid's algorithm
- Prime factorization and fundamental theorem of arithmetic
- Congruences modulo m
- Fermat's little theorem

Basic Notation on Integers

- $\mathbb{N}$ denotes the set of all positive integers
- $\mathbb{Z}$ denotes the set of all integers
- We equip $\mathbb{Z}$ with the usual operations of sum and multiplication $+, \cdot$ over integer numbers
- Given $a, b \in \mathbb{Z}$, b *divides* a (denoted as $b|a$) if there exists $m \in \mathbb{Z}$ such that $a = bm$
- In this case b is called a divisor of a
- A positive integer a whose divisors are only 1 and itself is called a prime number

Euclidean Division for Integers

Theorem

For any $a, b \in \mathbb{Z}$ with $b > 0$, there exists a unique pair $q, r \in \mathbb{Z}$ with $0 \leq r < b$ such that $a = bq + r$.

Note: q and r are respectively called *quotient* and *remainder*

Proof (existence):

- Without loss of generality, we can assume $a \geq 0$ and $b > 0$
- Let $q_0 = 0$ and $r_0 = a$. Then $a = bq_0 + r_0$. If $r_0 < b$ then we are done, otherwise we define $q_1 = q_0 + 1$ and $r_1 = r_0 - b$. Then again $a = bq_1 + r_1$, with $0 \leq r_1 < r_0$
- We continue until we get $k < r_0$ such that $a = bq_k + r_k$ with $r_k < b$, which we reach in at most r_0 steps. Set $q = q_k$ and $r = r_k$

Euclidean Division for Integers

Theorem

For any $a, b \in \mathbb{Z}$ with $b > 0$, there exists a unique pair $q, r \in \mathbb{Z}$ with $0 \leq r < b$ such that $a = bq + r$

Proof (uniqueness):

- By contradiction, suppose there is a pair $(q', r') \neq (q, r)$ s.t.

$$a = bq + r \ , \ r < b$$
$$a = bq' + r' \ , \ r' < b$$

  and assume without loss of generality that $r' > r$
- Subtracting the two equations we get $b(q - q') = r' - r$
- Hence $b|(r' - r)$. Since $r < b$ and $r' < b$, we have $r' - r = 0$, thus $r' = r$ and it must be the case that $q' \neq q$
- But $b(q - q') = 0$, with $b \neq 0$. Hence $q - q' = 0 \Rightarrow q = q'$, obtaining a contradiction

Greatest Common Divisor (GCD)

Definition

The greatest common divisor of two nonzero integers $a, b \in \mathbb{Z}$ is the largest $d \in \mathbb{N}$ such that $d|a$ and $d|b$, and it is denoted as $\gcd(a, b)$

Theorem (Euclid's theorem)

Let $a, b \in \mathbb{Z}$ with $a = bq + r$. Then, $\gcd(a, b) = \gcd(b, r)$

Proof:

- Every divisor of a and b must be also a divisor of b and r (because $r = a - qb$), and vice versa
- Hence, (a, b) and (b, r) have the same set D of divisors
- The maximum of D is the gcd of both (a, b) and (b, r)

Euclid's Algorithm

- $\gcd(a,b)$ can in principle be computed by factoring a and b in prime factors and then comparing the factors
- Example: $\gcd(168,720) = \gcd(2^3 \cdot 3 \cdot 7, 2^4 \cdot 3^2 \cdot 5) = 24$
- This is not however an efficient way to calculate the $\gcd$
- We can use Euclid's theorem in an iterative way:

$$\gcd(a,b) = \gcd(b,r) = \cdots = \gcd(d,0) = 0$$

  that is, we continue to divide each previous remainder for the current remainder, until we hit 0
- By Euclid's theorem, the last remainder d before 0 is $\gcd(a,b)$

Euclid's Algorithm

Example: Compute $\gcd(2328, 2124)$

$$
\begin{aligned}
2328 &= 2124 \cdot 1 + 204 \\
2124 &= 204 \cdot 10 + 84 \\
204 &= 84 \cdot 2 + 36 \\
84 &= 36 \cdot 2 + 12 \\
36 &= 12 \cdot 3 + 0
\end{aligned}
$$

$$
\begin{aligned}
\gcd(2328, 2124) = \gcd(2124, 204) = \gcd(204, 84) = \\
= \gcd(84, 36) = \gcd(36, 12) = 12
\end{aligned}
$$

$\Rightarrow$ Hence the gcd of 2328 and 2124 is 12

Euclid's Algorithm

- We now formalize the observation above in pseudocode
- Let $a, b \in \mathbb{Z}$, with $b > 0$. *Euclid's algorithm* computes the $\gcd(a, b)$ by iteratively applying the Euclidean division:

  EUCLID(a, b) (assume $a > b$)

  while $b \neq 0$ **do**
    $r \leftarrow a\%b$
    $a \leftarrow b$
    $b \leftarrow r$
  end while
  return a

- $a\%b$ is the remainder of the integer division of a by b
- The penultimate remainder held by a is $\gcd(a, b)$

Bezout's Identity

Theorem (Bezout's Identity)

For any $a, b \in \mathbb{Z}$ there exists $x, y \in \mathbb{Z}$ such that

$$\gcd(a, b) = ax + by$$

Proof:

1. Apply Euclid's algorithm to find $\gcd(a, b)$
2. Express all equations with respect to the remainders
3. In the second-to-last equation, substitute the expression with that of the third-to-last and collect like terms
4. Repeat 3 with the other equations until the top is reached

Note: pay attention to the change of sign when substituting!

Bezout's Identity

Following the previous example: $\gcd(2328, 2124) = 12$

- Solve with respect to the remainders:

$$
\begin{aligned}
2328 &= 2124 \cdot 1 + 204 \Rightarrow 204 = 2328 - 2124 \cdot 1 \\
2124 &= 204 \cdot 10 + 84 \Rightarrow 84 = 2124 - 204 \cdot 10 \\
204 &= 84 \cdot 2 + 36 \Rightarrow 36 = 204 - 84 \cdot 2 \\
84 &= 36 \cdot 2 + 12 \Rightarrow 12 = 84 - 36 \cdot 2 \\
36 &= 12 \cdot 3 + 0
\end{aligned}
$$

- Substituting in second-to-last:

$$
\begin{aligned}
12 &= 84 - 36 \cdot 2 = 84 - (204 - 84 \cdot 2) \cdot 2 = 84 \cdot 5 - 204 \cdot 2 = \\
&= (2124 - 204 \cdot 10) \cdot 5 - 204 \cdot 2 = 2124 \cdot 5 - 204 \cdot 52 = \\
&= 2124 \cdot 5 - (2328 - 2124 \cdot 1) \cdot 52 = 2328 \cdot (-52) + 2124 \cdot 57
\end{aligned}
$$

- Hence, we have $x = -52$ and $y = 57$

Bezout's Identity

- The numbers x, y are not unique: any pair $(x + sb, y - sa)$ is a solution of the Bezout's identity for any $s \in \mathbb{Z}$
- Special case: if $a, b \in \mathbb{Z}$ are *relatively prime* (i.e. $\gcd(a, b) = 1$) then there are x, y such that $ax + by = 1$
- The converse holds: if $ax + by = 1$ for $x, y \in \mathbb{Z}$, then $d|a$ and $d|b$ implies $d|1$, and thus $\gcd(a, b) = 1$
- Euclid's algorithm can be modified to find x and y (*Extended Euclidean Algorithm – EEA*)
- We will look into EEA once we introduce multiplicative inverses (Relevance in RSA: compute the public key)

Prime Factorization

Lemma (Euclid's lemma)

Let $p \in \mathbb{N}$ be a prime number and $a, b \in \mathbb{Z}$. If $p|ab$, then $p|a$ or $p|b$.

Proof: Suppose $p \nmid a$. Then $\gcd(p, a) = 1$ and by Bezout's identity there are $x, y \in \mathbb{Z}$ s.t. $px + ay = 1$. Hence $b = p(bx) + (ab)y$, and the right hand side of this expression is divisible by p. Hence $p|b$

Theorem (Fundamental theorem of arithmetic)

Any integer $n \geq 2$ can be written as a product of a finite number of primes, and the factorization is unique up to the order of the factors

Proof (existence): By strong induction on n

- Base case: $n = 2$. Since 2 is prime, the theorem holds
- Induction step: Assume the theorem holds for $2, \cdots n-1$. If n is prime, the theorem holds. If n is not prime, we can write it as $n = ab$, with a, b both admitting a prime factorization

Prime Factorization

Theorem (Fundamental theorem of arithmetic)

Any integer $n \geq 2$ can be written as a product of a finite number of primes, and the factorization is unique up to the order of the factors

Proof (uniqueness):

- Suppose n has two prime factorizations $p_1 \cdots p_k$ and $q_1 \cdots q_t$
- By Euclid's lemma, $p_1 | q_i$ for one of the q_i, let's say q_1 (we can relabel the factors q_i)
- Hence $p_1 = q_1$ and $p_2 \cdots p_k = q_2 \cdots q_t$
- This argument can be repeated until the result is obtained

Congruences modulo m

Definition

Let $m \in \mathbb{N}$. Then $a, b \in \mathbb{Z}$ are *congruent modulo m* if $m|a-b$. We denote this relation as $a \equiv b \mod m$

Example: $m = 15$, $a = 73$, $b = 28$. $a - b$ equals 45, which is divisible by 15 hence $73 \equiv 28 \mod 15$

Remark: The congruence relation modulo m (abbreviated as $\equiv_m$) is an *equivalence relation*, meaning that $\equiv_m$ is:

- **reflexive**: $a \equiv a \mod m$
- **symmetric**: $a \equiv b \mod m \Rightarrow b \equiv a \mod m$
- **transitive**: $a \equiv b \mod m$ and $b \equiv c \mod m \Rightarrow a \equiv c \mod m$

Congruences modulo m

- **Residue classes for** $\equiv_m$: $[a] = \{b = a + km : k \in \mathbb{Z}\}$ contains all those integers such that $a \equiv b \mod m$
- The set of all residue classes $[0], [1], \cdots, [m-1]$ induces a *partition* of $\mathbb{Z}$, that is:

$$\mathbb{Z} = [0] \cup [1] \cup \cdots \cup [m-1], \text{ and } [i] \cap [j] = \varnothing \text{ for all } i \neq j$$

- We define $\mathbb{Z}_m = \{[0], [1], \cdots, [m-1]\}$. For ease of notation, often we will write a instead of $[a]$
- $\mathbb{Z}_m$ is equipped with the following addition and multiplication:

$$[a] + [b] = [a + b] \text{ and } [a] * [b] = [ab]$$

- In the next lecture, we will see that $(\mathbb{Z}_m, +, *)$ is a *ring*

Fermat's Little Theorem

Theorem

Let $p \in \mathbb{N}$ be a prime number. Then for any integer $a \in \mathbb{Z}$ the following relation holds:

$$a^p \equiv a \mod p$$

Proof: By induction on a.

- Base case: for $a = 0$ the claim trivially holds
- Induction step: suppose $a > 0$ and $a^p \equiv a \mod p$. Then, using the binomial expansion theorem:

$$\begin{aligned}(a+1)^p &= \binom{p}{0}a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a + \binom{p}{p}a^0 \\ &= a^p + \underbrace{\binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a}_{\equiv 0 \mod p} + 1 \equiv a^p + 1 \equiv a + 1\end{aligned}$$

Fermat's Little Theorem

Proof (continued):

- The central part of the binomial expansion is congruent to 0 mod p because it is a sum of multiples of p. Indeed:

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p \cdot (p-1) \cdot \ldots \cdot (p-i+1)}{i \cdot (i-1) \cdot \ldots \cdot 2 \cdot 1}$$

  for any $0 < i < p$, and since p is prime, it cannot be divided by any of the denominator's terms.

- Hence we have $(a+1)^p \equiv a^p + 1 \mod p$, and by induction hypothesis $a^p \equiv a \mod p$, obtaining:

$$(a+1)^p \equiv a+1 \mod p$$

Fermat's Little Theorem

- If $a \not\equiv 0 \mod p$, then $a^p \equiv a \mod p \Leftrightarrow a^{p-1} \equiv 1 \mod p$
- It can be used to compute powers modulo a prime p
- Contrapositive of the theorem:

$$a^p \not\equiv a \mod p \text{ for a } \in \mathbb{Z} \Rightarrow p \text{ is not a prime number}$$

- The contrapositive can be used to show that a number is composite
- The converse is not true: if $a^p \equiv a \mod p$ then p is not necessarily a prime number

Algebra & Cryptography CSE3230

Lecture 4 – Groups, Rings and Fields

Stjepan Picek

Recap – Previous Lecture

- Greatest common divisor and Euclid's algorithm
- Prime factorization and fundamental theorem of arithmetic
- Congruences modulo m and Fermat's little theorem

Relevance in crypto: all operations and data in RSA are represented in the set of residue classes $\mathbb{Z}_m$

This Lecture

Goal: Introduction to basic algebraic structures such as groups, rings and fields

Outline:

- Basic definitions on groups
- Multiplicative inverses and Extended Euclidean Algorithm
- Basic definitions on rings and fields
- Chinese Remainder Theorem

Definition of Group

A **binary operation** over a nonempty set S is a function $\circ : S \times S \to S$ over a nonempty set S that associates to each pair of elements in S another element in S

Definition

Let G be a nonempty set and $\circ : G \times G \to G$ a binary operation over G. Then G is a *group* under $\circ$ if:

- $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in G$ (*associativity*)
- There exists $e \in G$ such that $a \circ e = e \circ a = a$ for all $a \in G$ (*existence of identity*)
- For each $a \in G$ there exists $a' \in G$ such that $a \circ a' = a' \circ a = e$ (*existence of inverses)*

Abelian group: a group G where $\circ$ is commutative, that is $a \circ b = b \circ a$ for all $a, b \in G$

Basic Properties of Groups

We will use two main notations for the group operation:

- *additive*: $\circ \Rightarrow +$, hence $a + b$. Inverse of a is $-a$
- *multiplicative*: $\circ \Rightarrow \cdot$, hence $a \cdot b$ (or ab). Inverse of a is a^{-1}

A group G satisfies the following properties:

1. The identity element e is unique
2. The inverse of each element $a \in G$ is unique
3. Left and right cancellation rules hold:
   - $ab = ac \Rightarrow b = c$ (left cancellation)
   - $ba = ca \Rightarrow b = c$ (right cancellation)

Exercise: prove the three properties above (hint: proceed by contradiction for 1 and 2, use 2 to show 3)

Examples of Groups

In what follows, $+$ and $\cdot$ respectively denote sum and multiplication over the relevant set

- $\langle \mathbb{N}, + \rangle$ is *not* a group (why?)
- $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{Q}, + \rangle$, $\langle \mathbb{R}, + \rangle$ are all examples of infinite additive groups
- $\langle \mathbb{Z}, \cdot \rangle$ is *not* a group
- $\langle \mathbb{Q} \setminus \{0\}, \cdot \rangle$, $\langle \mathbb{R} \setminus \{0\}, \cdot \rangle$ are multiplicative groups (why do we need to remove 0?)

Congruences mod m and additive groups

- Recall that $a \equiv b \mod m$ if $m|a-b$
- $\mathbb{Z}_m$ is defined as the set of all residue classes modulo m:

$$\mathbb{Z}_m = \{[0],[1],\cdots,[m-1]\}$$
$$[a] = \{b = a + km : k \in \mathbb{Z}\} \ , \ 0 \leq a \leq m-1$$

- Sum and multiplication are defined for all $a, b \in \mathbb{Z}_m$ as

$$[a]+[b] = [a+b] \text{ and } [a]\cdot[b] = [ab]$$

- $\langle \mathbb{Z}_m, + \rangle$ is a group: indeed,
  - $([a]+[b])+[c] = [a+b]+[c] = [a+b+c] = [a]+[b+c] = [a]+([b]+[c])$
  - $[0]$ is the identity
  - For all $[a] \in \mathbb{Z}_m$, $-a = [m-a]$

Definition of Ring

Definition

A set R with two binary operations $\circ, *$ is called a *ring* if the following conditions hold:

- $\langle R, \circ \rangle$ is an abelian group (with $0 \in R$ denoting the identity)
- $(a * b) * c = a * (b * c)$ for all $a, b, c \in R$ (associativity on $*$)
- $a * (b \circ c) = a * b \circ a * c$ and $(b \circ c) * a = b * a \circ c * a$ (distributivity of $*$)

Further, a ring $\langle R, \circ, * \rangle$ is called:

- *commutative* if $*$ is commutative, $a * b = b * a$ for all $a, b \in R$
- *with unity* if there is $1 \in R$ s.t. $a * 1 = 1 * a = a$ for all $a \in R$

Examples of Rings

- $\langle \mathbb{Z}, +, \cdot \rangle$, $\langle \mathbb{Q}, +, \cdot \rangle$ and $\langle \mathbb{R}, +, \cdot \rangle$ are all examples of infinite commutative rings with unity
- $\langle \mathbb{Z}_m, +, \cdot \rangle$ is an example of finite commutative ring with unity
- $\mathbb{Z}$ has an additional property, namely:

$$a \cdot b = 0 \Rightarrow a = 0 \text{ or } b = 0$$

- What about $\mathbb{Z}_m$? For example, let $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$.
- If we take [2] and [3], we have $[2] \cdot [3] = [0] \Rightarrow$ but both [2] and [3] are different from [0]!

Zero Divisors and Integral Domains

Definition

A commutative ring with unity R is an integral domain if $a * b = 0$ implies $a = 0$ or $b = 0$ (i.e. there are no *zero divisors*)

- Therefore $\mathbb{Z}$ is an integral domain, but in general $\mathbb{Z}_m$ is not

Theorem

$\mathbb{Z}_m$ is an integral domain if and only if m is prime.

Proof:

- $\Rightarrow$: Suppose that $\mathbb{Z}_m$ is an integral domain but $m = kl$ for $1 < k, l < m$. Then $[k] \cdot [l] = [kl] = [0]$, obtaining a contradiction
- $\Leftarrow$: If m is prime, by Euclid's lemma $m|ab$ implies $m|a$ or $m|b$, or equivalently $ab \equiv 0 \mod m$ implies $a \equiv 0$ or $b \equiv 0 \mod m$

Unit in a commutative ring

Definition

Given R a commutative ring with unity 1, an element $a \in R$ is called a *unit* if there exists $b \in R$ s.t. $ab = ba = 1$

- a and b are multiplicative inverses in the above definition
- In $\mathbb{Z}$ the only units are 1 and -1
- What about $\mathbb{Z}_m$?

Theorem

$a \in \mathbb{Z}_m$ is a unit if and only if $\gcd(a, m) = 1$

Proof: $ab \equiv 1 \mod m \Leftrightarrow ab = 1 + km \Leftrightarrow ab - km = 1 \Leftrightarrow$ There are x, y s.t. $ax + my = 1 \Leftrightarrow \gcd(a, m) = 1$

Definition of Field

Definition

A set F with two binary operations $+, \cdot$ is called a *field* if it is a commutative ring with unity where every nonzero element is a unit

Equivalently, $\langle F, +, \cdot \rangle$ is a field if it is a commutative ring with unity and moreover:

- Every $a \in F^* = F \setminus \{0\}$ has a multiplicative inverse
- $\langle F^*, \cdot \rangle$ is a multiplicative group

Examples:

- $\mathbb{Q}$ and $\mathbb{R}$ are examples of fields
- $\mathbb{Z}$ is *not* a field
- What about $\mathbb{Z}_m$?

$\mathbb{Z}_m$ as a Field

Theorem

$\mathbb{Z}_m$ is a field if and only if m is prime

Proof:

- $\Rightarrow$: Suppose $\mathbb{Z}_m$ is a field but $m = kl$ for $1 < k, l < m$. Since $\mathbb{Z}_m$ is a field, k must have a multiplicative inverse x such that

$$kx \equiv 1 \mod m \Rightarrow kxl \equiv l \mod m$$

  But $kl \equiv 0 \mod m \Rightarrow l \equiv 0 \mod m$, obtaining a contradiction
- $\Leftarrow$: Suppose m is prime. Then $\gcd(a, m) = 1$ for all $1 \leq a \leq m$, and by the previous theorem a is a unit

Relevance in crypto: Several public key protocols represent messages, keys and ciphertexts as elements of $\mathbb{Z}_p$ with p prime (e.g. Diffie-Hellman key exchange, Elgamal cryptosystem)

Euclid's Algorithm and Multiplicative Inverses

- Suppose we want to check if b has a multiplicative inverse b^{-1} modulo a. It suffices to check if $\gcd(a, b) = 1$
- Hence, if Euclid's algorithm returns 1, b^{-1} exists. But how can we compute it?
- Recall *Bezout's identity*: let $r = \gcd(a, b)$. Then there exist $s, t \in \mathbb{Z}$ such that $r = as + bt$

Proposition

Suppose $\gcd(a, b) = 1$. *Then* b^{-1} *mod* $a = t$ *mod* a

Proof:

- by Bezout's identity, we have $1 = \gcd(a, b) = as + bt$
- Reducing modulo a, we obtain $bt \bmod a = 1$

Extended Euclidean Algorithm

- The *Extended Euclidean Algorithm* (EEA) can be used to obtain r, s, t (and thus the multiplicative inverse $b^{-1} = t$ if $\gcd(a, b) = 1$)
- **Relevance in crypto**: Determine the public key in RSA, which is the multiplicative inverse of the private key

EXT-EUCLID(a, b) (assume $a > b$)

$a_0 \leftarrow a$; $b_0 \leftarrow b$; $t_0 \leftarrow 0$; $t \leftarrow 1$
$s_0 \leftarrow 1$; $s \leftarrow 0$; $q \leftarrow \lfloor a/b \rfloor$; $r \leftarrow a_0 - qb_0$
while $r > 0$ **do**
  $temp \leftarrow t_0 - qt$; $t_0 \leftarrow t$; $t \leftarrow temp$; $temp \leftarrow s_0 - qs$
  $s_0 \leftarrow s$; $s \leftarrow temp$; $a_0 \leftarrow b_0$;
  $b_0 \leftarrow r$; $q = \lfloor a_0/b_0 \rfloor$; $r = a_0 - qb_0$;
end while
$r \leftarrow b_0$
return (r, s, t)

Chinese Remainder Theorem (CRT)

- The CRT is used to solve congruence systems of the kind:

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \\ \quad \vdots \\ x \equiv a_r \bmod m_r \end{cases}$$

- The name comes from the following puzzle described in a Chinese mathematics book dating back to the 3rd century AD:

  «We have things of which we do not know the number; if we count them by threes, the remainder is 2; if we count them by fives, the remainder is 3; if we count them by sevens, the remainder is 2. How many things are there?»

Chinese Remainder Theorem (CRT)

Theorem

Let $m_1, m_2, \cdots m_r \in \mathbb{N}$ *such that* $\gcd(m_i, m_j) = 1$ *for all* $i \neq j$. *Then the system of congruences*

$$\begin{cases} x \equiv a_1 \ mod \ m_1 \\ x \equiv a_2 \ mod \ m_2 \\ \quad \vdots \\ x \equiv a_r \ mod \ m_r \end{cases}$$

has a unique solution x, *with* $0 \leq x < M = m_1 m_2 \cdots m_r$

For the proof, we first construct a solution for the system and then show it is unique

Chinese Remainder Theorem (CRT)

Proof (existence):

- For all $1 \leq i \leq r$, let $M_i = \frac{M}{m_i}$. Then $\gcd(M_i, m_i) = 1$ since $\gcd(m_i, m_j) = 1$ for $i \neq j$
- We then use the EEA to find the multiplicative inverse y_i of M_i modulo m_i.
- Next, define x as the sum

$$x = \sum_{i=1}^{r} a_i M_i y_i \mod M \ .$$

- Since $m_k | M_j$ for all $k \neq j$, we have $M_j \equiv 0 \mod m_k$ and $a_j M_j y_j \equiv 0 \mod m_k$
- Hence, $x \equiv a_k M_k y_k \equiv a_k \mod m_k$, since $M_k y_k \equiv 1 \mod m_k$
- Therefore, x is a solution of the system

Chinese Remainder Theorem (CRT)

Proof (uniqueness):

- Let $0 \leq x_1, x_2 < M$ be two solutions of the system
- We first want to show that $x_1 \equiv x_2 \mod M$
- For each k, we have $x_1 \equiv x_2 \mod m_k$, and thus $m_k | x_1 - x_2$
- From here, it follows that $x_1 \equiv x_2 \mod M$, since $M = m_1 m_2 \cdots m_r$ and $\gcd(m_i, m_j) = 1$ for all $i \neq j$
- $x_1 \equiv x_2 \mod M$ only if $x_1 = x_2$, since $0 \leq x_1, x_2 < M$

Relevance for crypto:

- Optimized implementations of RSA
- Certain attacks in RSA

Chinese Remainder Theorem (CRT) - Example

Consider the following system:

$$\begin{cases} x \equiv 5 \bmod 7 \\ x \equiv 4 \bmod 11 \\ x \equiv 3 \bmod 13 \end{cases}$$

By the CRT the solution is $x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$, where:

- $a_1 = 5$, $a_2 = 4$, $a_3 = 3$
- $m_1 = 7$, $m_2 = 11$, $m_3 = 13$
- $M = m_1 \cdot m_2 \cdot m_3 = 1001$.
- $M_1 = \frac{M}{m_1} = 143$, $M_2 = \frac{M}{m_2} = 91$, $M_3 = \frac{M}{m_3} = 77$.
- y_1, y_2, y_3 are the multiplicative inverses of M_1, M_2, M_3 modulo respectively m_1, m_2, m_3.

Chinese Remainder Theorem (CRT) - Example

- To find y_1, y_2, y_3, we apply the EEA on the pairs (m_1, M_1), (m_2, M_2) and (m_3, M_3)
- M_1, M_2, M_3 are respectively reduced modulo $m_1 = 7$, $m_2 = 11$, $m_3 = 13$, hence the pairs are $(7,3)$, $(11,3)$, $(13,12)$
- The table reports the three executions of the EEA:

a_0	b_0	t_0	t	q	r	$temp$
7	3	0	1	2	1	–
3	1	1	$\underline{-2}$	3	0	5
11	3	0	1	3	2	–
3	2	1	8	1	1	8
2	1	8	$\underline{4}$	2	0	4
13	12	0	1	1	1	–
12	1	1	$\underline{-1}$	12	0	12

Chinese Remainder Theorem (CRT) - Example

- The multiplicative inverse is the last value held by t in the EEA (underlined numbers in the table)
- **Note:** t needs to be reduced modulo the respective m_i
- Thus the first and the third underlined t values in the table becomes $-2 \equiv 5 \mod 7$ and $-1 \equiv 12 \mod 13$
- Hence we obtain $y_1 = 5$, $y_2 = 4$ and $y_3 = 12$
- The solution to the system is thus:

$$x = (5 \cdot 143 \cdot 5 + 4 \cdot 91 \cdot 4 + 3 \cdot 77 \cdot 12) \mod 1001 = 796$$

Algebra & Cryptography CSE3230

Lecture 4 examples – Calculating multiplicative inverse

Stjepan Picek

Extended Euclidean Algorithm

What is the greatest common divisor of 53 and 17?
gcd(53,17) = 17*3 + 2
gcd(17,2) = 2*8 + 1
gcd(2,1) = 2*1 + 0
Since gcd(53,17)=1, we can find multiplicative inverse. Let's express remainders as the difference:
1 = 17*1 - 2*8 = 17*1 - (53*1 -17*3)*8
1 = 25*17 -8*53.
Now, the multiplicative inverse of 17 mod 53 is 25 and multiplicative inverse of 53 mod 17 is -8.
You can easily check it by calculating that 25*17 = 1 mod 53.

Euclid-Wallis Algorithm

What is the greatest common divisor of 53 and 17?
Let us start with two columns:
1 0
0 1
53 17
Now, above each next column write the floor of the quotient of the base of the previous column divided with the base of the column before that.
Next, compute the next column by subtracting that number times the previous column from the column before that.
Note that the procedure works (of course) regardless what number is denoted first. For readability, we assume the first number is always larger.

Euclid-Wallis Algorithm

		$\lfloor 53/17 \rfloor = 3$	$\lfloor 17/2 \rfloor = 8$	$\lfloor 2/1 \rfloor = 2$
1	0	1 = 1-0*3	-8=0-1*8	17=1-(-8)*2
0	1	-3=0-1*3	25=1-(-3)*8	-53=-3-25*2
53	17	2=53-17*3	1=17-2*8	0=2-1*2

Now, looking at the penultimate column, we see that -8 is the multiplicative inverse of 53, and 25 is multiplicative inverse of 17. What is more, if we look at the last column, we see that the smallest values resulting in 53*x+17*y=0 are x=17 and y=-53. Finally, looking at the top column, we obtain continued fractions for 53/17:

$$a_0 + \frac{1}{a_1 + \frac{1}{a2}} = 3 + \frac{1}{8 + \frac{1}{2}} = 3.1176$$

Algebra & Cryptography CSE3230

Lecture 5 – Polynomial Rings

Stjepan Picek

Recap – Previous Lecture

- Basic definitions on groups
- Basic definitions on rings and fields
- Extended Euclidean Algorithm (EEA)
- Chinese Remainder Theorem (CRT)

Relevance in crypto: EEA is used to determine the public key in RSA, CRT can be used to optimize the implementation of RSA and also to execute certain attacks on it

This Lecture

Goal: Introduce polynomial rings and Euclidean division for polynomials

Outline:

- Ideals, principal ideal domains (PID), factor rings
- Basic definitions and properties of polynomials
- Polynomial rings and Euclidean division
- Roots in polynomials, remainder and factor theorems
- Irreducible polynomials and greatest common divisor
- Euclidean algorithm for polynomials

References and reading material

- S. Huczynska, *Finite fields*, course notes available at: `http://www.math.rwth-aachen.de/~Max.Neunhoeffer/Teaching/ff2012/ff2012.pdf`, in particular:
  - Section 2, page 8 onwards for ideals and PIDs (skip the part on ring homomorphisms and characteristic of a finite field)
  - Section 3, pages 10-14 for the part on polynomials
- Further reading: R. Lidl, H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge University Press, 1994. In particular, Section 1.3 on polynomials, pages 18–28
- Further reading: J. Fraleigh, *A First Course in Abstract Algebra*, Pearson, 2003 (7th edition)

Subrings and Ideals

Definition

Let $\langle R, \circ, * \rangle$ be a ring. Then:

- $S \subseteq R$ is a *subring* if $\langle S, \circ, * \rangle$ is a ring
- $I \subseteq R$ is an *ideal* if it is a subring and

$$i * r \in I \text{ and } r * i \in I$$

for all $i \in I$ and $r \in R$ (*absorption* property)

- **Remark**: from now on we will only consider commutative rings with unity. Hence the condition above for ideals becomes $i * r \in I$ for all $i \in I$ and $r \in R$
- **Motivation**: Ideals are important for the construction of finite fields, which are used in block ciphers

Subrings and Ideals

Theorem

Let $\langle R, +, \cdot \rangle$ be a ring. The subset $S \subseteq R$ is a subring if and only if $a + b$, $-a$ and $ab \in S$ for all $a, b \in S$

Proof: Exercise

Examples:

- $\mathbb{Z}$ is a subring of $\langle \mathbb{Q}, +, \cdot \rangle$ but it is *not* an ideal: take e.g. any $\frac{p}{q} \in \mathbb{Q}$ where p, q are prime and $z \in \mathbb{Z}$ with $z \neq q$ as a counterexample: $\frac{p}{q} \cdot z$ is not an integer number!
- $\{[0], [2], [4]\}$ is a subring of $\mathbb{Z}_6$
- $(2) = \{2z : z \in \mathbb{Z}\}$, the set of all even integers, is a subring and also an ideal of $\langle \mathbb{Z}, +, \cdot \rangle$
- More in general, given a ring $\langle R, \circ, * \rangle$ and $a \in R$, the *principal ideal* generated by a is the set $(a) = \{a * r : r \in R\}$

Principal Ideal Domains (PID)

Definition

A ring $\langle R, \circ, * \rangle$ is called a *principal ideal domain* (PID) if every ideal in it is principal

Example: $\mathbb{Z}$ is a PID. In fact, let $I \subseteq \mathbb{Z}$ be an ideal of $\mathbb{Z}$. Then:

- Take the smallest positive element $b \in I$ and consider (b)
- Obviously, $(b) \subseteq I$ because I is an ideal
- Let $a \in I$. By Euclidean division there are $q, r \in \mathbb{Z}$ with $0 \leq r < b$ s.t. $a = bq + r$.
- $r = a - bq$, with $a \in I$ and $b \in I$. Hence $bq \in I$ and thus $a - bq = r \in I$
- But b is smallest positive integer in I, hence $r = 0$
- Hence $a = bq$ for all $a \in I$, from which $a \in (b)$
- To conclude, we have that $I \subseteq (b)$

Congruences m and Ideals

- Recall: two integers $a, b \in \mathbb{Z}$ are *congruent modulo* $m \in \mathbb{Z}$ if m divides $a - b$:

$$a \equiv b \mod m \iff m | a - b \iff \exists k \in \mathbb{Z} : \; a - b = km$$

- We can reformulate this relation in terms of the ideal $(m) = \{mz : z \in \mathbb{Z}\}$:

$$a \equiv b \mod m \iff a - b \in (m)$$

- Hence, a principal ideal (m) induces the equivalence relation mod m, and as such it partitions the set $\mathbb{Z}$ in disjoint classes:

$$[a] = \{b \in \mathbb{Z} : a - b \in (m)\} = \{b \in \mathbb{Z} : a - b = mz, \; z \in \mathbb{Z}\}$$

  i.e., the residue classes we already saw in last lecture

Quotient rings

- **Note:** In what follows, we denote the two operations of an abstract ring as $+$ and $\cdot$ instead of $\circ$ and $*$
- Let $\langle R, +, \cdot \rangle$ be a ring and $I \subseteq R$ an ideal of R. The relation $a \sim b$ if and only if $a - b \in I$ is an equivalence relation
- An equivalence class for an element $a \in R$ is denoted as $a + I = \{a + i : i \in I\}$
- Given two classes $a + I$ and $b + I$, we can define the following addition and multiplication operations:
  - $(a + I) + (b + I) = (a + b) + I$
  - $(a + I) \cdot (b + I) = (ab) + I$

Quotient rings

Theorem

The set Q of equivalence classes $a + I$ with addition and multiplication defined as in the previous slide is a ring, and it is called the quotient ring of R modulo the ideal I (notation: $Q = R/I$)

Examples:

- $R = \mathbb{Z}$, $I = (m)$. Then, $\mathbb{Z}/(m)$ is an equivalent formulation of the residue class ring $\mathbb{Z}_m$ seen in the previous lecture
- Thus, $\mathbb{Z}/(p)$ is a field if and only if p is prime
- $R = \mathbb{Z}_6$, $I = (2)$. Then, $\mathbb{Z}_6/(2) = \{0 + (2), 1 + (2)\}$ (it is essentially equivalent to the ring $\mathbb{Z}_2$)

Polynomials

- **Motivation:** apply the theory of quotient rings developed so far to rings of *polynomials*
- **Why?** Polynomials can be conveniently described as arrays in programming, and they are useful in block ciphers

Definition

A *polynomial* over a ring $\langle R, +, \cdot \rangle$ is an expression

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n \ ,$$

where for all $0 \leq i \leq n$ the *coefficient* a_i belongs to R, while x is the *indeterminate*.

- We assume that $a_n \neq 0$, and thus n is the *degree* of f

Operations on Polynomials

Let $f = \sum_{i=0}^{n} a_i x^i$ and $g = \sum_{i=0}^{m} b_i x^i$ be two polynomials over a ring R. Then we define the two operations:

- **Addition:** assuming that $m \leq n$, we have

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i \text{ , where } b_i = 0 \ \forall i > m$$

- **Multiplication:** setting $d = m + n$, we have

$$f(x)g(x) = \sum_{k=0}^{d} c_k x^k$$

where c_k is defined for all $0 \leq k \leq d$ as

$$c_k = \sum_{\substack{i+j=k, \\ 0 \leq i \leq n \\ 0 \leq j \leq m}} a_i b_j, \text{ or equivalently, } c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

Polynomial rings

Theorem

Let $R[x]$ denote the set of all polynomials in the indeterminate x over a ring R. Then, $R[x]$ with addition and multiplication defined as in the previous slide is a ring, namely the polynomial ring over R

Proof: Exercise (just verify that all ring axioms hold for $R[x]$)

Example: The ring of polynomials $\mathbb{Z}_2[x]$ over the ring $\mathbb{Z}_2$. Let $f(x) = x^3 + x + 1$ and $g(x) = x^2 + x$. Then:

- $f(x) + g(x) = x^3 + x^2 + 2x + 1 = x^3 + x^2 + 1$
- $f(x)g(x) = x^5 + x^4 + x^3 + 2x^2 + x = x^5 + x^4 + x^3 + x$

Remark: from now on, we will only deal with polynomial rings $F[x]$ with coefficients in a *field* F

Euclidean Division for Polynomials

- Recall Euclidean division on integers: given $a, b \in \mathbb{Z}$, with $b \neq 0$, there exist $q, r \in \mathbb{Z}$, $0 \leq r < |b|$ s.t. $a = bq + r$
- An analogous result exists for polynomials over a field
- Let $f, g \in F[x]$ be two polynomials over a field F. Then g *divides* f (notation: $g|f$) if there is $h \in F[x]$ s.t. $f = gh$

Theorem

Let F be a field. Given two polynomials $f, g \in F[x]$ with $g \neq 0$, there exist two polynomials $q, r \in F[x]$ such that

$$f = gq + r, \text{ where } 0 \leq deg(r) < deg(g)$$

Polynomial long division – Example

Let $F = \mathbb{Z}_2$, $f(x) = x^7 + x^6 + x^4 + x^3 + 1$, $g(x) = x^3 + 1$

Polynomial long division – Example

Let $F = \mathbb{Z}_2$, $f(x) = x^7 + x^6 + x^4 + x^3 + 1$, $g(x) = x^3 + 1$

1. Write $g(x)$ to the left of the vertical bar and $f(x)$ to the right, leaving spaces for missing powers

$$x^3 + 1 \,\Big|\, x^7 \quad +x^6 \quad\quad +x^4 \quad +x^3 \quad\quad\quad +1$$

Polynomial long division – Example

Let $F = \mathbb{Z}_2$, $f(x) = x^7 + x^6 + x^4 + x^3 + 1$, $g(x) = x^3 + 1$

2. Divide the highest degree term of f by the highest degree term of g, and write the result above the horizontal bar

$$\begin{array}{r|l} & x^4 \\ \hline x^3+1 & x^7 + x^6 + x^4 + x^3 + 1 \end{array}$$

Polynomial long division – Example

Let $F = \mathbb{Z}_2$, $f(x) = x^7 + x^6 + x^4 + x^3 + 1$, $g(x) = x^3 + 1$

3. Multiply the result x^4 by g, and write the result $x^7 + x^4$ below f, putting again spaces according to the missing powers

$$
\begin{array}{r|lllll}
 & & & x^4 & & \\
\hline
x^3+1 & x^7 & +x^6 & +x^4 & +x^3 & +1 \\
 & x^7 & & +x^4 & & \\
\cline{2-4}
\end{array}
$$

Polynomial long division – Example

Let $F = \mathbb{Z}_2$, $f(x) = x^7 + x^6 + x^4 + x^3 + 1$, $g(x) = x^3 + 1$

4. Subtract f by the polynomial $x^7 + x^4$. **Note:** we are in the ring $\mathbb{Z}_2$, hence addition and subtraction coincide

$$
\begin{array}{r|llllll}
 & & & x^4 & & & \\
\hline
x^3+1 & x^7 & +x^6 & +x^4 & +x^3 & & +1 \\
 & x^7 & & +x^4 & & & \\
\hline
 & & x^6 & & +x^3 & & +1
\end{array}
$$

Polynomial long division – Example

Let $F = \mathbb{Z}_2$, $f(x) = x^7 + x^6 + x^4 + x^3 + 1$, $g(x) = x^3 + 1$

5. $deg(x^6 + x^3 + 1) > deg(g)$. Hence, divide the highest degree term of $x^6 + x^3 + 1$ by the highest degree term of g

$$
\begin{array}{r|l}
 & \quad\quad\quad\quad\quad\quad x^4 \quad +x^3 \quad\quad\quad\quad \\
\hline
x^3 + 1 & \; x^7 \quad +x^6 \quad\quad +x^4 \quad +x^3 \quad\quad\quad +1 \\
 & \; x^7 \quad\quad\quad\quad +x^4 \\
\cline{2-2}
 & \quad\quad\quad\quad x^6 \quad\quad\quad\quad +x^3 \quad\quad\quad +1
\end{array}
$$

Polynomial long division – Example

Let $F = \mathbb{Z}_2$, $f(x) = x^7 + x^6 + x^4 + x^3 + 1$, $g(x) = x^3 + 1$

6. Multiply the result x^3 by g, and write the result $x^6 + x^3$ below $x^6 + x^3 + 1$

$$
\begin{array}{rl|lllll}
 & & & & x^4 & +x^3 & \\
\hline
x^3+1 & & x^7 & +x^6 & +x^4 & +x^3 & +1 \\
 & & x^7 & & +x^4 & & \\
\cline{3-5}
 & & & x^6 & & +x^3 & +1 \\
 & & & x^6 & & +x^3 & \\
\cline{4-6}
\end{array}
$$

Polynomial long division – Example

Let $F = \mathbb{Z}_2$, $f(x) = x^7 + x^6 + x^4 + x^3 + 1$, $g(x) = x^3 + 1$

7. Subtract ($\equiv$ sum in $\mathbb{Z}_2$) the polynomial $x^6 + x^3 + 1$ by the polynomial $x^6 + x^3$

$$
\begin{array}{rl|llllll}
 & & & & x^4 & +x^3 & & \\
\hline
x^3+1 & | & x^7 & +x^6 & +x^4 & +x^3 & & +1 \\
 & & x^7 & & +x^4 & & & \\
\cline{3-5}
 & & & x^6 & & +x^3 & & +1 \\
 & & & x^6 & & +x^3 & & \\
\cline{3-6}
 & & & & & & & 1
\end{array}
$$

Polynomial long division – Example

Let $F = \mathbb{Z}_2$, $f(x) = x^7 + x^6 + x^4 + x^3 + 1$, $g(x) = x^3 + 1$

8. $deg(1) = 0 < 3 = deg(x^3 + 1)$. Hence we stop. The quotient is above the horizontal bar while the remainder is in the last row

$$
\begin{array}{rl|lllll}
 & & & x^4 & +x^3 & & \\
\hline
x^3+1 & | & x^7 & +x^6 & +x^4 & +x^3 & +1 \\
 & & x^7 & & +x^4 & & \\
\cline{3-5}
 & & & x^6 & & +x^3 & +1 \\
 & & & x^6 & & +x^3 & \\
\cline{4-5}
 & & & & & & 1
\end{array}
$$

The result of the division $f = gq + r$ is thus:

$$x^7 + x^6 + x^4 + x^3 + 1 = (x^3 + 1)(x^4 + x^3) + 1$$

Polynomial factorization and roots

- Let F be a field. An element $a \in F$ is a *root* of a polynomial $f \in F[x]$ if $f(a) = 0$

Theorem (Factor theorem)

Given a field F, an element $a \in F$ is a root of a polynomial $f \in F[x]$ if and only if $x - a$ divides $f(x)$

Proof:

- By Euclidean division, we have $f = q(x-a) + c$, with $q \in F[x]$ and $c \in F$ (because the degree of $(x-a)$ is 1, hence the degree of c must be 0, i.e. $c(x) = c_0$, with $c_0 \in F$)
- Replacing x with a, we get $f(a) = c$, thus $f = q(x-a) + f(a)$
- The theorem follows from the previous identity

Polynomial factorization and roots

Theorem

Given a field F, a polynomial $f \in F[x]$ of degree n has at most n roots in the field F

Proof:

- By contradiction, suppose that f has $n+1$ distinct roots $a_1, \cdots, a_{n+1}$ in F
- By the factor theorem, we can rewrite f as:

$$f = (x - a_1)(x - a_2) \cdots (x - a_{n+1})g$$

  for some polynomial $g \in F[x]$
- But this contradicts the fact that f has degree n

Polynomial factorization and roots

- Hence, there is a relationship between factorization and roots of a polynomial
- **Example:** Let $F = \mathbb{Z}_3$, and $f = x^2 + 2 \in \mathbb{Z}_3[x]$
  - The roots of f are 1 and 2, since $1 + 2 = 3$ and $2^2 + 2 = 6$, which are both multiple of 3 and thus are 0 modulo 3
  - f can thus be factored as:

$$f(x) = (x - 1)(x - 2)$$

- The example above is a particular case where *all* roots are in the ground field F
- What about $F = \mathbb{Z}_2$, $f = (x^2 + x + 1)(x + 1) = x^3 + 1$?
- In this case 1 is a root of f, but there are no roots in $\mathbb{Z}_2$ for the $x^2 + x + 1$ factor

Irreducible polynomials

Definition

Let F be a field and $f \in F[x]$ with $deg(f) \geq 2$. Then f is called *reducible* over F if there are two polynomials $g, h \in F[x]$ such that $f = gh$. If no such polynomials exist, then f is *irreducible*

Examples:

- $x^2 - 2$ is irreducible over $\mathbb{Q}$ but reducible in $\mathbb{R}$
- $x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$
- We will see in the next lecture that irreducible polynomials over a field F becomes reducible over their *splitting field*
- Intuitively: the splitting field K of f is the smallest field containing F such that *all* roots of f are in K

Polynomial factorization

- A polynomial $f \in F[x]$ is called *monic* if its leading coefficient (i.e. the coefficient of the highest degree term) is 1
- **Remark**: over $\mathbb{Z}_2$, all polynomials are monic

Theorem (Factoring polynomials)

Let $f \in F[x]$ be a polynomial over a field F. Then, f can be factored as follows:

$$f = a p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

where $a \in F[x]$, $p_1, \cdots, p_k \in F[x]$ are distinct monic irreducible polynomials, and $e_1, \cdots e_k \in \mathbb{N}$

- Monic irreducible polynomials over $F[x]$ play a role analogous to prime numbers in $\mathbb{Z}$

Greatest Common Divisor for Polynomials

Let $f, g \in F[x]$ not both equal to zero. Then $d \in F[x]$ is a *greatest common divisor* (gcd) of f and g if:

- d is monic
- d divides both f and g
- if h divides both f and g, then h divides d

Theorem

The gcd $f, g \in F[x]$ (not both identically zero) is unique

$\gcd(f, g)$ can be computed with the Euclidean algorithm

Theorem (Bezout's identity)

For any pair $f, g \in F[x]$ not both equal to zero there exist $k, l \in F[x]$ such that $\gcd(f, g) = kf + lg$

Euclid's algorithms for Polynomial gcd

- Euclid's algorithm for polynomials stands on the same observation for integers: if $f, g \in F[x]$, and $f = gq + r$, then

$$gcd(f, g) = gcd(g, r)$$

- **Example:** $F = \mathbb{Z}_2$, $f(x) = x^4 + x^3 + x^2 + 1$, $g(x) = x^3 + 1$
- At each step of Euclid's algorithm, we apply polynomial long division as we saw in the previous example

$$\begin{aligned} x^4 + x^3 + x^2 + 1 &= (x^3 + 1)(x + 1) + (x^2 + x) \\ x^3 + 1 &= (x^2 + x)(x + 1) + (x + 1) \\ x^2 + x &= (x + 1)x + 0 \end{aligned}$$

- The gcd is the last nonzero remainder, hence

$$\gcd(x^4 + x^3 + x^2 + 1, x^3 + 1) = x + 1$$

Algebra & Cryptography CSE3230

Lecture 6 – Finite fields

Stjepan Picek

Recap – Previous Lecture

- Ideals, principal ideal domains (PID), quotient rings
- Basic definitions and properties of polynomials
- Polynomials rings, Euclidean division for polynomials
- Roots in polynomials, remainder and factor theorems
- Irreducible polynomials and greatest common divisor

Relevance in crypto: polynomials are useful in the design of several block ciphers, since they can be easily represented as arrays

This Lecture

Goal: Develop the theory of fields, with particular focus on fields defined as quotients of a polynomial ring modulo an irreducible polynomial

Outline:

- Polynomial congruences
- Ideals and quotient rings in a polynomial ring
- Extension fields
- Splitting fields

References and reading material

- S. Huczynska, *Finite fields*, course notes available at: `http://www.math.rwth-aachen.de/~Max.Neunhoeffer/Teaching/ff2012/ff2012.pdf`, in particular:
  - Section 3, pp. 12-13
  - Section 4
- Further reading: R. Lidl, H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge University Press, 1994.
- Further reading: J. Fraleigh, *A First Course in Abstract Algebra*, Pearson, 2003 (7th edition)

Polynomial congruences

- Recall the definition of congruences over integers: for $a, b, m \in \mathbb{Z}$, we say that $a \equiv b \mod m$ if $m|a-b$
- We can also use *ideals* in $\mathbb{Z}$ to describe this congruence: $a \equiv b \mod m$ iff $a-b$ is in the ideal $(m) = \{mz : z \in \mathbb{Z}\}$
- **Example**: $m = 5$, $a = 18$, $b = 3$. We have that $5|(18-3)$, hence $18 \equiv 3 \mod 5$. Alternatively, $18 \equiv 3 \mod 5$ because $18-3 = 15 \in (5) = \{5z : z \in \mathbb{Z}\}$
- The ring of residue classes $\mathbb{Z}_m$ is equal to the factor ring $\mathbb{Z}/(m)$, and $\mathbb{Z}_m$ is a (finite) field iff m is prime
- **Example**: $\mathbb{Z}_5 = \mathbb{Z}/(5) = \{[0], [1], [2], [3], [4]\}$ is a field
- In this case, $\mathbb{Z}_m$ is also called a *prime field*, and it is also denoted by $\mathbb{F}_m$

Polynomial congruences

- **Remark:** From a practical (programming) point of view, we can consider a residue class $[a]$ as the integer number $a \in \mathbb{Z}$
- Sum and multiplication in $\mathbb{Z}_m$ are the same as in $\mathbb{Z}$, except that after evaluating them we need to reduce the result modulo m
- **Problem**: the fact that m must be prime to get a finite field is too limiting for our needs in crypto!
- Ideally, we would like a finite field where the number of elements is a power of a prime, in particular a power of 2
- **Why?** A set with 2^n elements can be easily encoded with bit vectors of length n

Polynomial congruences

- **How to achieve this**? We need to develop a theory of congruences for polynomials analogous to that of integers
- Assume that $\mathbb{F}_p$ is a prime field (hence $p \in \mathbb{N}$ is prime), and consider the polynomial ring $\mathbb{F}_p[x]$
- Given a nonzero polynomial $f \in \mathbb{F}_p[x]$, by $(f) = \{g \in \mathbb{F}_p[x] : f|g\}$ we denote the set of all polynomials g that are divisible by f
- **Example:** $p = 2$, $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$

$$(f) = \{x^2 + x + 1, x^3 + 1, x^4 + x^2 + 1, \cdots\}$$

- The set (f) is a principal ideal of $\mathbb{F}_p[x]$ (exercise: prove it)

Polynomial congruences

Definition

Let $f, g, h \in \mathbb{F}_p[x]$, with f a nonzero polynomial. We say that g is congruent to h modulo f if $g - h \in (f)$, or equivalently if $f|(g-h)$:

$$g \equiv h \mod f \Leftrightarrow g - h = kf,\ k \in \mathbb{F}_p[x]$$

- **Example:** $p = 2$, $f(x) = x^2 + x + 1$, $g(x) = x^5 + x^3 + x^2$, $h(x) = x^5 + x^2 + 1 \in \mathbb{F}_2[x]$

$$x^5 + x^3 + x^2 \equiv x^5 + x^2 + 1 \mod x^2 + x + 1$$

Indeed, recalling that in $\mathbb{F}_2$ sum and subtraction coincide:

$$g(x) - h(x) = x^5 + x^3 + x^2 + x^5 + x^2 + 1 = \\ = x^3 + 1 = (x+1)(x^2 + x + 1)$$

Thus $g - h = kf$ with $k = x + 1$

Quotient Polynomial Rings and Fields

- Let $f \in \mathbb{F}_p[x]$ and consider the ideal (f)
- When is the quotient ring $\mathbb{F}_p[x]/(f)$ a field?

Theorem

Let $f \in \mathbb{F}_p[x]$ be a nonzero polynomial over the prime field $\mathbb{F}_p$. The quotient ring $\mathbb{F}_p[x]/(f)$ is a field if and only if f is irreducible over $\mathbb{F}_p$

- Hence, irreducible polynomials play the same role of prime numbers for prime fields
- **Example:** $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{F}_2$, (since neither 0 nor 1 are roots), and thus $\mathbb{F}_2[x]/(x^2 + x + 1)$ is a field

Quotient Polynomial Rings and Fields

- What are the elements of the field $\mathbb{F}_2[x]/(x^2+x+1)$?
- Recall that the equivalence classes of a congruence in a ring R modulo an ideal I have the form $a+I=\{a+i : i \in I\}$, $a \in R$
- Here i are all the polynomials that are divisible by x^2+x+1. What about a?
- In the case of $\mathbb{Z}_m$, the residue classes $[a]$ are represented by the m integers $0, \cdots, m-1$ less than m,
- Similarly, in $\mathbb{F}_2[x]/(x^2+x+1)$ the representatives are *all polynomials in* $\mathbb{F}_2[x]$ *with degree less than* 2:

$$a \in \{0, 1, x, 1+x\},$$

since $deg(x^2+x+1)=2$

Quotient Polynomial Rings and Fields

- Thus for $f = x^2 + x + 1$ the field $\mathbb{F}_2[x]/(f)$ contains the following 2^2 elements:

$$\mathbb{F}_2[x]/(f) = \{0 + (f), 1 + (f), x + (f), 1 + x + (f)\}$$

- In practice, we can consider the elements in the field $\mathbb{F}_2[x]/(f)$ as the representative polynomials, dropping the "$+(f)$"
- **Remember:** When doing operations in $\mathbb{F}_2/(f)$, if the result has degree $\geq deg(f)$ we need to reduce the result mod f
- **Example**: $a = x$, $b = x + 1$

$$ab = x(x+1) = x^2 + x \Rightarrow x^2 + x \mod x^2 + x + 1 = 1$$

Quotient Polynomial Rings and Fields

- Addition table for $\mathbb{F}_2[x]/(f)$:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

- Multiplication table for $\mathbb{F}_2[x]/(f)$:

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Quotient Polynomial Rings and Fields

- As an example of a quotient ring that is *not* a field, just take the ideal generated by any *reducible* polynomial
- **Example:** Let $f(x) = x^2 + 1 \in \mathbb{F}_2[x]$
- The quotient ring $\mathbb{F}_2[x]/(f)$ is *not* a field because it is not even an integral domain
- In fact, if we take $a = b = x + 1$, their product gives

$$ab = (x+1)(x+1) = x^2 + 1 \Rightarrow x^2 + 1 \mod x^2 + 1 = 0$$

but both a and b are nonzero polynomials. Hence $x + 1$ is a *zero divisor* in $\mathbb{F}_2[x]/(x^2 + 1)$

- This is similar to the situation of the ring $\mathbb{Z}_6$, which is not a field because 2 and 3 are zero divisors

Quotient Polynomial Rings and Fields

- **Remark:** Given a prime field $\mathbb{F}_p$, the number of polynomials over $\mathbb{F}_p$ with degree less than n is p^n
- Indeed, any such polynomial is of the form

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$$

  where each coefficient a_i is an element of $\mathbb{F}_p$
- Hence, the finite field $\mathbb{F}_p[x]/(f)$ for $f \in \mathbb{F}_p[x]$ irreducible is composed of p^n elements
- Setting $q = p^n$, we also denote $\mathbb{F}_p[x]/(f)$ by $\mathbb{F}_q$ or $\mathbb{F}_{p^n}$

Extension Fields

Definition

Let $\langle F, +, \cdot \rangle$ be a field. A subset $K \subseteq F$ is called a *subfield* if $\langle K, +, \cdot \rangle$ is itself a field. Conversely, F is called an *extension* of K

- Let $f(x) \in F[x]$ be an irreducible polynomial over F
- In the previous lecture we have seen that the irreducibility of f implies that F does not contain a root of f

Theorem

Let F be a field and $f \in F[x]$ be an irreducible polynomial over F. Then $F[x]/(f)$ is an extension field of F that contains a root of f

Extension Fields

- Let F be a field, E an extension of F and $\alpha \in E \setminus F$. We denote by $F(\alpha)$ the *smallest* subfield of E that contains F and α

$$F(\alpha) = \bigcap_{\substack{G \subseteq E:\ G \text{ subfield},\\ F \subseteq G,\ \alpha \in G}} G$$

- Let F be a field and $f \in F[x]$ an irreducible polynomial over F
- If α is a root of f in an extension E of F, then $F(\alpha)$ is equivalent to the field $F[x]/(f)$
- In this case, if $deg(f) = n$, then every element in $F(\alpha)$ is uniquely written in the form

$$c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}$$

with $c_i \in F$ for $0 \leq i \leq n-1$

Splitting Fields

Definition

Let F be a field. An extension E of F is a *splitting field* for a polynomial $f \in F[x]$ if there exist $\alpha_1, \cdots, \alpha_n \in E$ and $a \in F$ such that

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

- In other words, a splitting field for a polynomial f over a field F is the *smallest* extension of F that contains all roots of f
- Does any irreducible polynomial have a splitting field?

Theorem

Let F be a field and $f \in F[x]$ a polynomial over F. Then there exists a splitting field E for f. Moreover, such a splitting field is unique

Vector Spaces

- We now recall the concept of vector space to give a characterization of extension fields

Definition

Let F be a field. A *vector space* over F is a set V equipped with two operations:

- Vectorial sum: $(u, v) \mapsto u + v$ for $u, v \in V$
- Scalar multiplication $(a, v) \mapsto av \in V$ for $a \in F$, $v \in V$

Such that:

- $\langle V, + \rangle$ is an abelian group
- $a(u + v) = au + av$ for all $a \in F$ and $u, v \in V$
- $(c + d)u = cu + du$ for all $c, d \in F$ and $u \in V$
- $(cd)u = c(du)$ for all $c, d \in F$ and $u \in V$
- $1u = u$ for all $u \in V$

Vector Spaces

- Given a vector space V over a field F, a subset $B = \{v_1, \cdots, v_n\} \subseteq V$ is called a *basis* of V if:
  - The vectors in B are *linearly independent*, that is:

$$c_1 v_1 + c_2 v_2 + \cdots + c_n v_n = 0 \Leftrightarrow c_1 = c_2 = \cdots = c_n = 0$$

  - B *spans* V, that is any $v \in V$ can be uniquely written as a linear combination of the vectors in B:

$$v = c_1 v_1 + c_2 v_2 + \cdots + c_n v_n,\ c_i \in F$$

- Any basis of V has the same number of elements n, which is the *dimension* of V

Vector Spaces

- **Example:** Let $F = \mathbb{F}_2 = \{0, 1\}$ the finite field with two elements. The set $\mathbb{F}_2^3$ is composed of all 3-bit vectors:

$$\mathbb{F}_2^3 = \{(0,0,0),(0,0,1),(0,1,0),(0,1,1),\\ (1,0,0),(1,0,1),(1,1,0),(1,1,1)\}$$

- Equipped with the following two operations:
  - $(u, v) \mapsto u + v = (u_1 + v_1, u_2 + v_2, u_3 + v_3)$ for $u, v \in \mathbb{F}_2^3$
  - $(a, v) \mapsto av = (a \cdot v_1, a \cdot v_2, a \cdot v_3)$ for $a \in \mathbb{F}_2$, $v \in \mathbb{F}_2^3$

  is a vector space over $\mathbb{F}_2$ (exercise: prove it)
- A basis of $\mathbb{F}_2^3$ is $B = \{(0,0,1),(0,1,0),(1,0,0)\}$, and thus the dimension is 3
- In general, for any $n \in \mathbb{N}$ the dimension of $\mathbb{F}_2^n$ is n

Algebraic Extensions and Minimal Polynomials

- Given an extension E of a field F, $\alpha \in E$ is *algebraic over* F if it is a root of a polynomial in $F[x]$, that is if

$$p_0 + p_1\alpha + \cdots + p_{n-1}\alpha^{n-1} + p_n\alpha^n = 0$$

  for some $p_0, p_1, \cdots, p_n \in F$
- An extension E of a field F is called an *algebraic extension* if every element of E is algebraic over F
- Let $\alpha \in E$ be algebraic over F and define the set

$$J = \{f \in F[x] : f(\alpha) = 0\}$$

Algebraic Extensions and Minimal Polynomials

- In other words, the set $J = \{f \in F[x] : f(\alpha) = 0\}$ contains all polynomials having α as a root
- J is a principal ideal of $F[x]$, and the unique polynomial $m_\alpha(x)$ that generates J is called the *minimal polynomial* of α

Theorem

Let F be a field and E an extension of F. Moreover, let $\alpha \in E$ be algebraic over F and denote by $m_\alpha(x)$ the minimal polynomial of α. Then:

- *$m_\alpha(x)$ is irreducible in $F[x]$*
- *$m_\alpha(x)$ divides every polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$*

Extension Fields as Vector Spaces

Theorem

Let F be a field and E an extension of F. Then E is a vector space over F. The degree of E is the dimension of the vector space E over F, and it is denoted as $[E : F]$

- Minimal polynomials can be used to characterize the basis of the vector space of the extension E:

Theorem

Let $E = F(\alpha)$ for some algebraic element α over F, and let $m_\alpha(x)$ be the minimal polynomial of α. Assuming that $deg(m_\alpha(x)) = n$, it follows that:

- *The degree of E is $[E : F] = n$*
- *$\{1, \alpha, \alpha^2, \cdots \alpha^{n-1}\}$ is a basis of E*

Extension Fields as Vector Spaces

- Thus, the elements of the extension $F(\alpha)$ can be uniquely expressed as linear combinations of the form:

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}, \text{ for some } c_i \in F$$

- **Example:** Let $F = \mathbb{F}_2$ and $f(x) = x^2 + x + 1$, which is irreducible in $\mathbb{F}_2$. Let α be a root of f, i.e. $\alpha^2 + \alpha + 1 = 0$
- Hence, $deg(f) = 2$, $\alpha^2 = \alpha + 1$, and the basis is $\{1, \alpha\}$
- To find the elements of the extension $\mathbb{F}_4$ we need to compute all linear combinations $c_0 + c_1\alpha$, with $c_0, c_1 \in \mathbb{F}_2$
- Thus we obtain $\mathbb{F}_4 = \{0, 1, \alpha, 1 + \alpha\}$, which is a vector space of dimension 2 over $\mathbb{F}_2$
- Indeed, $\mathbb{F}_4$ is equivalent to $\mathbb{F}_2^2 = \{(0,0), (1,0), (0,1), (1,1)\}$
- By "equivalent" here we mean "isomorphic". We will cover this notion in detail in Lecture 8

Algebra & Cryptography CSE3230

Lecture 7 – Groups

Stjepan Picek

Recap – Previous Lecture

- Polynomial congruences
- Ideals and quotient rings in a polynomial ring
- Extension fields
- Splitting fields

Relevance in crypto: Finite fields are fundamental in block ciphers, and to efficiently represent and manipulate elements in them we need quotient polynomial rings

This Lecture

Goal: Look more into the details of group theory, with particular attention to subgroups and cyclic groups

Outline:

- Review basic definitions and properties of groups
- Euler's totient function ϕ
- Order of element in a group, cyclic (sub)groups
- Group cosets, Lagrange's theorem, Euler's theorem

References and reading material

- S. Huczynska, *Finite fields*, course notes available at: `http://www.math.rwth-aachen.de/~Max.Neunhoeffer/Teaching/ff2012/ff2012.pdf`, in particular:
  - Section 1, pp. 3–6
- Further reading: R. Lidl, H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge University Press, 1994.
  - Section 1, pp. 2–11
- Further reading: J. Fraleigh, *A First Course in Abstract Algebra*, Pearson, 2003 (7th edition)

Definition of Group

A **binary operation** over a nonempty set S is a function $\circ : S \times S \to S$ over a nonempty set S that associates to each pair of elements in S another element in S

Definition

Let G be a nonempty set and $\circ : G \times G \to G$ a binary operation over G. Then G is a *group* under $\circ$ if:

- $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in G$ (*associativity*)
- There exists $e \in G$ such that $a \circ e = e \circ a = a$ for all $a \in G$ (*existence of identity*)
- For each $a \in G$ there exists $a' \in G$ such that $a \circ a' = a' \circ a = e$ (*existence of inverses)*

Abelian group: a group G where $\circ$ is commutative, that is $a \circ b = b \circ a$ for all $a, b \in G$

Basic Properties of Groups

We will use two main notations for the group operation:

- *additive*: $\circ \Rightarrow +$, hence $a + b$. Inverse of a is $-a$
- *multiplicative*: $\circ \Rightarrow \cdot$, hence $a \cdot b$ (or ab). Inverse of a is a^{-1}

A group G satisfies the following properties:

1. The identity element e is unique
2. The inverse of each element $a \in G$ is unique
3. Left and right cancellation rules hold:
   - $ab = ac \Rightarrow b = c$ (left cancellation)
   - $ba = ca \Rightarrow b = c$ (right cancellation)

Examples of (Abelian) Groups

- $\langle \mathbb{N}, + \rangle$ is *not* a group: $+$ it is associative and has an identity element (0), but no element except 0 has an inverse
- $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{Q}, + \rangle$, $\langle \mathbb{R}, + \rangle$ are all examples of infinite groups
- $\langle \mathbb{Z}, \cdot \rangle$ is *not* a group: again $\cdot$ is associative and has a multiplicative identity (1), but only $-1, 1$ have an inverse

Denoting $R^* = R \setminus \{0\}$ the set of nonzero elements in a ring $\langle R, +, \cdot \rangle$, moreover:

- $\langle \mathbb{Q}^*, \cdot \rangle$, $\langle \mathbb{R}^*, \cdot \rangle$ are multiplicative groups
- More in general: given any field $\langle F, +, \cdot \rangle$, the structure $\langle F^*, \cdot \rangle$ is a multiplicative group
- $\langle \mathbb{Z}_m^*, \cdot \rangle$ is a group if and only if m is prime

The Group of Invertible Elements in $\langle \mathbb{Z}_m^*, \cdot \rangle$

- Let us consider the case of $\langle \mathbb{Z}_m^*, \cdot \rangle$ when m is not prime: then, some elements in $\mathbb{Z}_m$ do not have a multiplicative inverse
- **Example**: Let $\mathbb{Z}_6^* = \{1,2,3,4,5\}$. Then, the elements $2,3$ and 4 do not have a multiplicative inverse
- 1 and 5 are invertible because they are *coprime* with 6, i.e. $\gcd(1,6) = \gcd(5,6) = 1$. In fact $1^{-1} = 1$ and $5^{-1} = 5$ in $\mathbb{Z}_6^*$
- Let U_m denote the subset of invertible elements in $\langle \mathbb{Z}_m^*, \cdot \rangle$
- **Remark:** Clearly, $U_m = \mathbb{Z}_m^*$ if m is prime

Theorem

For all $m > 1$, $\langle U_m, \cdot \rangle$ is an Abelian group

Proof: Exercise

Euler's totient function ϕ

- **Question:** how many elements does U_m include?
- By definition, this is the number of elements between 0 and m that are coprime to m
- Their number is given by *Euler's totient function* ϕ:

$$\phi : \mathbb{N} \to \mathbb{N} \text{ s.t. } \forall n \in \mathbb{N}, \phi(n) = |\{i : 0 < i < n, \gcd(i, n) = 1\}|$$

- **Examples:** $\phi(5) = 4$, $\phi(6) = 2$, $\phi(10) = 4$
- How do we compute effectively $\phi(n)$?

Theorem (Product formula for ϕ)

For each $n \in \mathbb{N}$ with $n > 1$ it holds that

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

where the product is taken over all primes p that divide n

Euler's totient function ϕ

Examples:

$$\phi(430) = 430 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{43}\right) =$$
$$= 430 \cdot \frac{1}{2} \cdot \frac{4}{5} \cdot \frac{42}{43} = 1 \cdot 4 \cdot 42 = 168$$
$$\phi(720) = 720 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right)$$
$$= 720 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 24 \cdot 1 \cdot 2 \cdot 4 = 192$$
$$\phi(101) = 101 \cdot \left(1 - \frac{1}{101}\right) = 101 \cdot \frac{100}{101} = 100$$

Euler's totient function ϕ

- More in general, for every prime p we clearly have that:

$$\phi(p) = p - 1$$

- ϕ is also multiplicative, that is if $\gcd(p, q) = 1$ then

$$\phi(pq) = \phi(p) \cdot \phi(q)$$

- In particular if p and q are prime this means that

$$\phi(pq) = (p-1)(q-1)$$

- **Relevance in crypto**: Euler's ϕ plays a fundamental role in RSA, particularly during the key generation phase

Order of a (element of a) group

Definition

Let $\langle G, \circ \rangle$ be a group. Then:

- The *order* of G, denoted $|G|$, is the number of elements in G
- The *order* of an element $g \in G$, denoted $|g|$, is the smallest $n \in \mathbb{N}$ such that

$$\underbrace{g \circ g \circ \cdots \circ g}_{n \text{ times}} = e$$

  If no such element exists then $|g| = \infty$

Remark:

- If $\circ = +$ (i.e. G is an additive group), then $|g|$ is the smallest n such that $ng = 0$
- If $\circ = \cdot$ (i.e. G is a multiplicative group), then $|g|$ is the smallest n such that $g^n = 1$

Order of a (element of a) group

Examples of orders of groups:

- $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{Q}, \cdot \rangle$, $\langle \mathbb{R}, \cdot \rangle$ all have infinite order
- For any $m \in \mathbb{N}$, the order of $\langle \mathbb{Z}_m, + \rangle$ is m
- For any $p \in \mathbb{N}$ prime, the order of $\langle \mathbb{Z}_p^*, \cdot \rangle$ is $p-1$

Examples of orders of elements in a group:

- In the group $\langle \mathbb{Z}_6, + \rangle$, we have that $|[2]| = 3$, since $2+2+2 = 6 \in [0]$
- The group $\langle U_8, \cdot \rangle$ is formed by the elements $\{[1], [3], [5], [7]\}$
- The order of $[3]$ in U_8 is $|[3]| = 2$, because $3 \cdot 3 = 9 = (8 \cdot 1) + 1 \in [1]$
- Similarly, the order of $[7]$ in U_8 is $|[7]| = 2$ since $7 \cdot 7 = 49 = (8 \cdot 6) + 1 \in [1]$

Subgroups

Definition

Let $\langle G, \circ \rangle$ be a group. A subset $H \subseteq G$ is called a *subgroup* (denoted as $H \leq G$) if H is also a group under the same operation $\circ$

- Similarly to subrings, the following result gives an easy criterion to check if a subset of a group is a subgroup:

Theorem (Subgroup criterion)

Let $H \subseteq G$ be a subset of a group $\langle G, \cdot \rangle$ in multiplicative notation. Then $H \leq G$ if and only if $1 \in H$, $ab \in H$ and $a^{-1} \in H$ for all $a, b \in H$

- In other words, it suffices to check that H is closed under multiplication and inverses

Subgroups

Examples:

- In any group G, the singleton $\{e\}$ and G itself are subgroups of G (these are called *trivial* subgroups)
- $\langle \mathbb{Z}, + \rangle$ is a subgroup of $\langle \mathbb{Q}, + \rangle$
- $\langle \mathbb{Q}^*, \cdot \rangle$ is a subgroup of $\langle \mathbb{R}^*, \cdot \rangle$
- Let $U_9 = \{[1], [2], [4], [5], [7], [8]\}$ be the group of invertible elements in $\mathbb{Z}_9$
- $H = \{[1], [8]\} \leq U_9$. Indeed, $[1] \in H$, $[8]^{-1} = [8] \in H$ and $[1] \cdot [8] = [8] \in H$
- $H = \{[1], [4], [7]\} \leq U_9$. Proof: exercise

Cyclic (sub)groups

- Let G be a group in multiplicative notation and $g \in G$ an element of G. We define $\langle g \rangle$ as the set $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$

Theorem

$\langle g \rangle$ is a subgroup of G. Moreover, $\langle g \rangle$ is the smallest subgroup containing g.

Proof:

- We use the subgroup criterion theorem. The identity 1 is in $\langle g \rangle$ since $g^0 = 1$ for any $g \in G$
- Let $a, b \in \langle g \rangle$. Then $a = g^m$ and $b = g^n$ for $m, n \in \mathbb{Z}$
- Hence $ab = g^m \cdot g^n = g^{m+n}$, which means that $ab \in \langle g \rangle$
- Given $a = g^m$, clearly $a^{-1} \in \langle g \rangle$ since $a^{-1} = g^{-m}$
- Any subgroup $H \leq G$ including a includes also all powers of a by closure of $\cdot$. Thus $\langle a \rangle$ is the smallest subgroup containing a

Cyclic (sub)groups

- $\langle g \rangle$ is called the *cyclic* subgroup of G generated by g
- A group G is called *cyclic* if $G = \langle g \rangle$ for some $g \in G$

Examples:

- $\langle \mathbb{Z}, + \rangle$ is a cyclic group, generated by -1 and 1. Indeed, we can write any integer number $z \in \mathbb{Z}$ by repeatedly adding or subtracting 1
- For any $m \in \mathbb{N}$, the group $\langle \mathbb{Z}_m, + \rangle$ is cyclic. In fact, the unit $[1]$ acts as a generator, since $\langle [1] \rangle = \{n[1] : n \in \mathbb{Z}\}$
- The multiplicative group of invertible elements U_m in general is *not* cyclic
- Example: $U_8 = \{[1], [3], [5], [7]\}$, and no element generates U_8
- Actually each element in U_8 except for $[1]$ generates only itself and the identity since $|[3]| = |[5]| = |[7]| = 2$

Cyclic (sub)groups

Theorem

Let G be a cyclic group with $|G| = n$ and let a be a generator of G. Then:

- $a^i = a^j \Leftrightarrow i \equiv j \mod n$
- $|a^t| = \frac{n}{\gcd(t,n)}$

- **Corollary:** a^t is a generator of G if and only if t and n are coprime, i.e. $\gcd(t,n) = 1$
- **Example:** Let $U_{10} = \{[1],[3],[7],[9]\}$. Then [3] is a generator of U_{10}, since:

$$3^0 = 1;\ 3^1 = 3;\ 3^2 = 9;\ 3^3 = 27 = (2 \cdot 10) + 7 \equiv 7 \mod 10$$

- $3^3 = 7$ and the exponent 3 is coprime to $4 = |U_{10}|$. Thus [7] is also a generator of U_{10} (exercise: verify it)

Cyclic (sub)groups

Theorem

Let G be a cyclic group generated by g with $|G| = n$. Then:

- *For any subgroup $H \leq G$, H is cyclic as well*
- *For any subgroup $H \leq G$, $|H|$ divides n*
- *For each positive divisor t of n there is exactly one subgroup $H \leq G$ such that $|H| = t$, and $H = \langle g^{\frac{n}{t}} \rangle$*

Example: Let $G = U_{14} = \{[1], [3], [5], [9], [11], [13]\}$

- We have that $|G| = 6$ and $[3]$ is a generator of G, in fact:

$$3^0 = 1;\ 3^1 = 3;\ 3^2 = 9;\ 3^3 = (14 \cdot 1) + 13$$
$$3^4 = (14 \cdot 5) + 11;\ 3^5 = (14 \cdot 17) + 5$$

- 3 is a divisor of 6. Hence the subgroup of G of order 3 is generated by $3^{\frac{6}{3}} = 3^2 = 9$, and it is $H = \{[1], [9], [11]\}$

Cosets

Definition

Let $\langle G, \cdot \rangle$ be a group and $H \leq G$ a subgroup of G. For any $g \in G$:

- The set $gH = \{gh : h \in H\}$ is called a *left coset* of H
- The set $Hg = \{hg : h \in H\}$ is called a *right coset* of H

- **Remark:** If G is abelian, then left and right cosets coincide
- **Example**: Let $G = U_9\{1,2,4,5,7,8\}$, and $H = \{1,8\}$. The three cosets of H are:
  - $1H = \{1,8\} = H$
  - $2\text{H} = \{2 \cdot 1, 2 \cdot 8\} = \{2, (9 \cdot 1) + 7\} = \{2,7\}$
  - $4\text{H} = \{4 \cdot 1, 4 \cdot 8\} = \{4, (9 \cdot 3) + 5\} = \{4,5\}$

Cosets

From now on we assume that the groups we consider are always abelian. As a convention, we state the following properties for left cosets of a subgroup $H \leq G$:

- $a \in aH$ for all $a \in G$
- $aH = H$ if and only if $a \in H$
- $aH \leq G$ if and only if $a \in H$
- For all $a, b \in G$, we have that $aH = bH$ or $aH \cap bH = \emptyset$
- For all $a \in G$, the order of aH equals the order of H

Lagrange's theorem

Theorem

Let G be a finite group and $H \leq G$ a subgroup of G. Then the order of H divides the order of G, and $\frac{|G|}{|H|}$ corresponds to the index $[G : H]$ of G, that is the number of left (right) cosets of H in G

Proof:

- Given $g \in G$, let $\gamma : H \to gH$ be the function that associates to each element $h \in H$ its element in the coset gH, i.e. $\gamma(h) = gh$
- γ is bijective, hence H and gH have the same cardinality
- The group G is partitioned into $[G : H]$ left cosets
- Since each coset has cardinality $|H|$, it follows that $|G| = |H| \cdot [G : H]$

Euler's theorem

Some simple corollaries of Lagrange's theorem are the following:

Corollary

Let G be a finite group and $a \in G$. Then:

(a) $|a|$ *divides* $|G|$

(b) $a^{|G|} = e$, *with* e *being the identity of* G

Corollary (b) in particular implies the following important result:

Theorem (Euler's theorem)

Let a, n be integers with $n > 0$ and $\gcd(a, n) = 1$ *Then*

$$a^{\phi(n)} \equiv 1 \mod n$$

Euler's theorem and Fermat's little theorem

Proof:

- Recall that $|U_n| = \phi(n)$ with ϕ being Euler's totient function
- By Corollary (b), we have that $a^{|U_n|} = a^{\phi(n)} = 1$ for all $a \in U_n$
- Thus, in particular, $a^{\phi(n)} \equiv 1 \mod n$

Remark: what happens if we take $n = p$ with p prime?

- By definition of ϕ we have $\phi(p) = p - 1$
- Euler's theorem thus becomes:

$$a^{p-1} \equiv 1 \mod p$$

- Therefore, Euler's theorem is a generalization of Fermat's little theorem that we have seen in Lecture 3

Let $a,b \in U_m$. $\gcd(a,m)=\gcd(b,m)=1$

By Bézout: $\exists x,y \in \mathbb{Z} : ax+my=1$

Closure:

$\left.\begin{array}{l} a \equiv 1 \pmod m \\ b \equiv 1 \pmod m \end{array}\right\} \Rightarrow ab \equiv b \equiv 1 \pmod m$

We want to show $a \cdot b \in U_m \ \forall a,b \in U$

$\forall a,b \in U_m (a \cdot b = a \cdot b = b \cdot a = b \cdot a)$

$U_m \subseteq \mathbb{Z}$

We show that $\exists e \in U_m \ \forall a \in U_m (e \cdot a = a \cdot e = a)$

$a \in U_m \Rightarrow \exists x,y \in \mathbb{Z} : ax+my=1 \Rightarrow ax \equiv 1 \pmod m$

	1	2	3
1	2	1	3
2	1	3	2
3	3	2	1

$1 \cdot 1 = 2 \neq 1$
$2 \cdot 2 = 3 \neq 2$
$3 \cdot 3 = 1 \neq 3$
} NO IDENTITY $\Rightarrow$ NO INVERSE

$\forall a,b,c \in \{1,2,3\}$

$ac = ab \Rightarrow c = b$ (LEFT CANC)
$ca = ba \Rightarrow c = b$ (RIGHT CANC)

$a,b \in U_m \Rightarrow \left\{\begin{array}{l} ax \equiv 1 \pmod m \\ by \equiv 1 \pmod m \end{array}\right.$ for some $x,y \in \mathbb{Z}$

$ax(by) \equiv by \pmod m$

$\Downarrow$

$(ab)(xy) \equiv 1 \pmod m$

Notes on Group of Invertible Elements U_m

Algebra and Cryptography CSE3230

Notes by Luca Mariot

These notes summarize the proof done during lecture 7. Recall that $\mathbb{Z}_m = \{[0], \cdots, [m-1]\}$ is the ring of residue classes modulo $m \in \mathbb{N}$, with addition and multiplication respectively defined as

$$[a] + [b] = [a + b] \ , \ \ [a] \cdot [b] = [a \cdot b] \ ,$$

for all $[a], [b] \in \mathbb{Z}_m$. In other words, we can perform operations on elements of $\mathbb{Z}_m$ (which formally are equivalence classes) by just considering their residue class representatives. Thus, we can effectively consider $\mathbb{Z}_m$ behaving as the set $\{0, 1, \cdots, m-1\}$ equipped with addition and multiplication modulo m, and in the following we will drop the square brackets [] when referring to an element in Z_m. We will cover more in detail this notion of equivalence in lecture 8, when we will introduce homomorphisms between algebraic structures.

Let now denote by $\mathbb{Z}_m^* = \mathbb{Z}_m \setminus \{0\}$, that is, the ring $\mathbb{Z}_m$ with the additive identity removed. We define $U_m \subseteq \mathbb{Z}_m^*$ as the set of *units* of $\mathbb{Z}_m^*$, which are the elements that have multiplicative inverse. Formally, we can write:

$$U_m = \{a \in \mathbb{Z}_m^* : \ \exists a' \in \mathbb{Z}_m^* : a \cdot a' = 1\} \ .$$

Recall from Lecture 4 (slide 11) that $a \in \mathbb{Z}_m^*$ is a unit if and only if it is *coprime* to m, that is $\gcd(a, m) = 1$. We want to prove the following claim:

Claim 1. *For any $m > 1$, U_m (with the multiplication operation inherited from Z_m) is an abelian group.*

To this end, we need to prove that the following five properties hold:

1. *Closure*: for any $a, b \in U_m$, we have that $ab \in U_m$.
2. *Commutativity*: for any $a, b \in U_m$, we have that $ab = ba$.
3. *Associativity*: for any $a, b, c \in U_m$, it holds that (ab)c = a(bc).
4. *Identity*: there exists $e \in U_m$ such that for any $a \in U_m$ it follows that $ae = ea = a$.
5. *Inverse*: for any $a \in U_m$ there exists $a' \in U_m$ such that $aa' = a'a = e$.

First, remark that the properties are well-defined: since we assumed that $m > 1$, we know that $\mathbb{Z}_m^*$ always contains at least one element. Let us start with the closure property. We know (again, by the theorem in Lecture 4, slide 11) that $a, b \in U_m$ if and only if $\gcd(a, m) = \gcd(b, m) = 1$. What we want to show then is that $gcd(ab, m)$ is also equal to 1, because this is logically equivalent to saying that ab has a multiplicative inverse modulo m. We now apply *Bezout's identity* (Lecture 3, slide 11) to both (a, m) and (b, m), thus obtaining that there exist $x, y \in \mathbb{Z}$ and $s, t \in \mathbb{Z}$ such that $ax + my = 1$ and $bs + mt = 1$. Using the definition of congruences, we can rewrite these two equations as follows:

$$\begin{cases} ax \equiv 1 \bmod m \\ bs \equiv 1 \bmod m \end{cases}$$

By multiplying the two congruences we obtain:

$$(ax)(bs) \equiv 1 \text{ mod } m \ .$$

Now, a, b, x, s are all integer numbers, whose multiplication is commutative and associative. Hence we can rearrange the terms as

$$(ab)(xs) \equiv 1 \text{ mod } m \ ,$$

which means that xs is the multiplicative inverse of ab. Thus, we proved that $ab \in U_m$, which settles closure.

Associativity, identity element, commutativity and existence of inverse all follows from the way U_m is defined and the closure property proved above. In particular, associativity, commutativity and identity follow from the properties of $\mathbb{Z}_m^*$: if we get $a, b, c \in U_m$, then we have that $(ab)c = a(bc)$ in reason of the fact that both (ab) and (bc) have multiplicative inverses (because of closure), and because the multiplication of residue classes is associative. A similar reasoning stands for commutativity, and 1 acts as the multiplicative identity of U_m. Finally, regarding the existence of inverses, remark that we defined U_m as the set of elements in $\mathbb{Z}_m^*$ that have multiplicative inverse. Thus for any $a \in U_m$ we know there exists $a' \in \mathbb{Z}_m^*$ such that $aa' = a'a = 1$. But then, if we take a', we know that its inverse is a. Therefore, a' belongs to U_m as well.

Algebra & Cryptography CSE3230

Lecture 8 – Homomorphisms, representation of finite fields

Stjepan Picek

Recap – Previous Lecture

- Review basic definitions and properties of groups
- Euler's totient function ϕ
- Order of element in a group, cyclic (sub)groups
- Group cosets, Lagrange's theorem, Euler's theorem

Relevance in crypto: Group theory is especially important in public key crypto protocols (e.g. key generation in RSA, key exchange in Diffie-Hellmann)

This Lecture

Goal: Overview homomorphisms of algebraic structures, representations of finite fields

Outline:

- Group and ring homomorphisms
- Characteristic and order of a finite field
- Primitive element in a finite field and primitive polynomial
- Representation of a finite field

References and reading material

- S. Huczynska, *Finite fields*, course notes available at: `http://www.math.rwth-aachen.de/~Max.Neunhoeffer/Teaching/ff2012/ff2012.pdf`
- Further reading: R. Lidl, H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge University Press, 1994.
- Further reading: J. Fraleigh, *A First Course in Abstract Algebra*, Pearson, 2003 (7th edition)

Homomorphisms

- During the previous lectures, we said in several occasions that some algebraic structure is "equivalent" to another one
- **Examples:**
  - $R = \mathbb{Z}$, $I = (m)$. Then, the quotient ring $\mathbb{Z}/(m)$ is equivalent to the residue class ring $\mathbb{Z}_m$
  - If α is a root of an irreducible polynomial f in an extension E of a field F, then $F(\alpha)$ is equivalent to the field $F[x]/(f)$
- This "equivalence" can be precisely described by the notion of *homomorphism* of algebraic structures
- Intuitively: map an algebraic structure to another set with analogous operations
- **Relevance in crypto:** efficient implementation of operations on algebraic structures used in cryptosystems

Group Homomorphisms

Definition

Let $\langle G, \circ \rangle$ and $\langle H, * \rangle$ be two groups. A mapping $\varphi : G \to H$ is called a *group homomorphism* if, for all $a, b \in G$,

$$\varphi(a \circ b) = \varphi(a) * \varphi(b)$$

Types of homomorphisms:

- an *epimorphism* if φ is onto (i.e., surjective)
- an *isomorphism* if φ is bijective. In this case we say that G and H are *isomorphic*, and write $G \cong H$
- an *endomorphism* if $\varphi : G \to G$, i.e. if φ is a homomorphism from G to itself
- an *automorphism* if φ is a bijective endomorphism, i.e. an isomorphism from G to itself

Group Homomorphisms - Examples

Example 1: $\mathbb{Z}$ and $\mathbb{Z}_m$

- Consider the additive groups $\langle \mathbb{Z}, + \rangle$ and $\langle \mathbb{Z}_m, + \rangle$ (notice the two "+" signs refer to different operations)
- Then the mapping $\varphi : \mathbb{Z} \to \mathbb{Z}_m$ defined for all $a \in \mathbb{Z}$ as $\varphi(a) = [a]$ is a homomorphism. Indeed for all $a, b \in \mathbb{Z}$ we have

$$\varphi(a+b) = [a+b] = [a] + [b] = \varphi(a) + \varphi(b)$$

- In fact, φ is an epimorphism, since each class $[a] \in \mathbb{Z}_m$ has a counterimage, namely the representative $a \in \mathbb{Z}$
- However φ is not an isomorphism, since $\mathbb{Z}$ is infinite while $\mathbb{Z}_m$ is finite for all $m \in \mathbb{N}$

Group Homomorphisms - Examples

Example 2: $\langle \mathbb{Z}_4, + \rangle$ and $\langle U_{10}, \cdot \rangle$

- Recall that $U_{10} = \{[1], [3], [7], [9]\}$ is the group of elements that are invertible under multiplication in $\mathbb{Z}_{10}$
- Define $\varphi : \mathbb{Z}_4 \to U_{10}$ as $\varphi(a) = 3^a$ for all $a \in \mathbb{Z}_4$
- Then φ is a homomorphism, since for all $a, b \in \mathbb{Z}_4$

$$\varphi(a+b) = 3^{a+b} = 3^a \cdot 3^b = \varphi(a) \cdot \varphi(b)$$

- Moreover φ is an isomorphism, since 3 is a generator of U_{10} (see previous lecture). Thus $\mathbb{Z}_4 \cong U_{10}$
- More in general: any generator g of U_n induces an isomorphism $\varphi(a) = g^a$ from U_n to $\mathbb{Z}_m$, with $m = \phi(n)$

Group Homomorphisms - Examples

Example 3: Let $\langle G, \cdot \rangle$ be any group in multiplicative notation with identity element e

- Let $a \in G$, and define $\varphi : G \to G$ as

$$\varphi_a(b) = aba^{-1} \text{ for all } b \in G$$

- Then φ_a is an automorphism of G, since for all $b, c \in G$

$$\varphi_a(bc) = abca^{-1} = ab \underbrace{a^{-1}a}_{=e} ca^{-1} = \varphi_a(b)\varphi_a(c)$$

  and φ is also bijective (exercise: prove it)
- The elements b and aba^{-1} are also called *conjugates*

Kernel of a homomorphism

Definition

Let $\varphi : G \to H$ be a homomorphism between the groups $\langle G, \circ \rangle$ and $\langle H, * \rangle$. The *kernel* of φ is defined as

$$ker\varphi = \{a \in G : \varphi(a) = e'\}$$

where $e' \in H$ is the identity element of H

- In other words, the kernel contains all elements of G that are "annihilated" to the identity of H under φ
- **Example**: Consider the previous homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_m$ defined as $\varphi(a) = [a]$ for all $a \in \mathbb{Z}$
- The kernel is the set of all integers that map to the residue class $[0]$, i.e. all multiples of m

Normal subgroups

Lemma

Let $\varphi : G \to H$ be a homomorphism between $\langle G, \circ \rangle$ and $\langle H, * \rangle$. Then $ker\varphi$ is a subgroup of G

Proof: exercise

- **Remark**: Let G and H be both multiplicative groups. If $a \in G$ and $b \in ker\varphi$, then $aba^{-1} \in ker\varphi$

Definition

Let $H \leq G$ be a subgroup of a group G. Then, H is a *normal subgroup* of G if $aha^{-1} \in H$ for all $a \in G$ and $h \in H$

- **Remark**: If G is abelian, then any subgroup $H \leq G$ is normal, since $aha^{-1} = aa^{-1}h = eh = h$

Quotient Group

- Recall the definition of quotient ring R/I in lecture 5: the set of equivalence classes $a + I$ with $a \in R$ and I an ideal of R
- If we consider only the additive structure $\langle R/I, + \rangle$, then this is an abelian group, and also a *quotient group*
- More in general we define quotient groups as follows:

Definition

Let $H \leq G$ be a normal subgroup of G. Then, the set G/H of left cosets of G under H equipped with the following operation:

$$(aH)(bH) = (ab)H, \text{ for all } a, b \in G$$

is a group, and it is called the quotient group of G modulo H

Homomorphism Theorem for Groups

- If the quotient group G/H is finite, then its order is equal to the number of (left) cosets of G under H
- Hence, by Lagrange's theorem, we have that $|G/H| = \frac{|G|}{|H|}$
- Normal subgroups can be used to define a natural homomorphism between groups, as per the following result:

Theorem

Let $\varphi : G \to H$ be a homomorphism between two groups G and H. Then $ker\varphi$ is a normal subgroup of G, and the group H is isomorphic to the quotient group $G/ker\varphi$

Example: $G = \mathbb{Z}$ and $H = \mathbb{Z}_m$ with $\varphi : a \mapsto [a]$

- The kernel of φ is the set $ker\varphi = \{z \in \mathbb{Z} : z = km,\ k \in \mathbb{Z}\} = m\mathbb{Z}$
- By the homomorphism theorem, we have $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$

Direct product of groups

Definition

Let G, H be two groups. Then the *direct product* of G and H is the structure $\langle G \times H, \cdot \rangle$ with $\cdot$ defined as:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$$

for all $(g_1, h_1), (g_2, h_2) \in G \times H$

- The structure defined above is also a group (proof: exercise)
- If G and H are both abelian, then $G \times H$ is also abelian

Theorem

Let G, H be finite cyclic groups. Then $G \times H$ is cyclic if and only if $\gcd(|G|, |H|) = 1$

Direct product of groups

- **Remark:** Given n groups $G_1, G_2, \cdots, G_n$, the direct product group $G_1 \times G_2 \times \cdots \times G_n$ is defined inductively

Theorem

Let $n = m_1 m_2 \cdots m_k$. Then, the following isomorphisms hold:

- $\mathbb{Z}_n \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$
- $U_n \cong U_{m_1} \times U_{m_2} \times \cdots \times U_{m_k}$

if and only if $\gcd(m_i, m_j) = 1$ *for all* $i \neq j$

Examples:

- $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$, since $\gcd(2,3) = 1$
- $\mathbb{Z}_8$ is *not* isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, since $\gcd(2,2) = 2$
- $U_{126} \cong U_2 \times U_7 \times U_9$

Ring Homomorphisms

- Homomorphism can be naturally extended to rings as follows:

Definition

Let $\langle R, +, \cdot \rangle$ and $\langle S, \circ, * \rangle$ be two rings. The mapping $\varphi : R \to S$ is a *ring homomorphism* if:

- φ is a group homomorphism between $\langle R, + \rangle$ and $\langle S, \circ \rangle$, i.e. $\varphi(a + b) = \varphi(a) \circ \varphi(b)$ for all $a, b \in R$
- $\varphi(a \cdot b) = \varphi(a) * \varphi(b)$ for all $a, b \in R$

- epi-, iso-, endo- and auto- morphisms are defined analogously
- The kernel of a ring homomorphism is defined in the same way as for group homomorphisms:

$$ker\varphi = \{a \in R : \varphi(a) = 0\}$$

where $0 \in S$ is the additive identity of S

Homomorphism Theorem for Rings

- A result similar to the homomorphism theorem for groups holds for rings, with normal subgroups replaced by ideals:

Theorem

Let $\varphi : R \to S$ be a homomorphism between a ring R and a ring S. Then, $\ker\varphi$ is an ideal of R and $S \cong R/\ker\varphi$

- Bijective mappings can be used to transfer the structure of a ring R to a set without operations S
- In particular, one can define the operations on S in terms of the bijective mapping, obtaining the ring *induced* by R

Induced Rings

- Let $\langle R, +, \cdot \rangle$ be a ring and S a set, and let $\varphi : R \to S$ be a bijective mapping from R to S
- Given $s_1, s_2 \in S$, let $r_1, r_2 \in R$ be the unique elements s.t. $s_1 = \varphi(r_1)$ and $s_2 = \varphi(r_2)$
- Define now sum and multiplication on S as

$$s_1 + s_2 = \varphi(r_1 + r_2),$$
$$s_1 s_2 = \varphi(r_1 r_2)$$

  for all elements $s_1, s_2 \in S$
- $\langle S, +, \cdot \rangle$ is a ring, and φ is an isomorphism between R and S

Ring Homomorphisms - Examples

Example 1: Let $p \in \mathbb{N}$ be prime, and define $\mathbb{F}_p = \{0, 1 \cdots, p-1\}$

- We already know that the quotient ring $\mathbb{Z}/(p)$ of $\mathbb{Z}$ by the ideal (p) is a finite field
- Let $\varphi : \mathbb{Z}/(p) \to \mathbb{F}_p$ be defined as $\varphi(a+(p)) = a$ for all $0 \leq a \leq p-1$. The mapping is clearly bijective
- Define now sum and multiplication on $\mathbb{F}_p$ as:

$$a + b = \varphi(a+(p)) + \varphi(b+(p))$$
$$ab = \varphi(a+(p)) \cdot \varphi(b+(p))$$

- Then, the set $\mathbb{F}_p$ endowed with the operations inherited from $\mathbb{Z}/(p)$ is a field, and it is called the *Galois field of order p*
- φ becomes a ring isomorphism

Ring Homomorphisms - Examples

Example 1: Concrete example: $p = 3$, $\mathbb{F}_3 = \{0,1,2\}$

- $\mathbb{Z}/(3) = \{0+(3), 1+(3), 2+(3)\}$ is isomorphic to $\mathbb{F}_3$
- φ is defined as $\varphi(0+(3)) = 0$, $\varphi(1+(3)) = 1$,$\varphi(2+(3)) = 2$
- The operations $+$ and $\cdot$ induced on $\mathbb{F}_3$ are the following:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

- Hence, computing in $\mathbb{F}_3$ amounts to ordinary arithmetic on $\mathbb{Z}$ with reduction modulo 3
- Analogously, arithmetic in the Galois field $\mathbb{F}_p$ is arithmetic on $\mathbb{Z}$ with reduction modulo p

Ring Homomorphisms - Examples

Example 2: The ring of integers modulo m

- The same mapping φ used for $\mathbb{F}_p$ can be also used to map any quotient ring $\mathbb{Z}/(m)$ to $\{0,1,\cdots,m-1\}$, for $m \in \mathbb{Z}$
- Similarly, one can define an isomorphism between the ring $\mathbb{Z}_m$ and the set $\{0,1,\cdots,m-1\}$ by $\gamma([a]) = a$ for $a = 0,1,\cdots,m-1$
- Therefore, $\mathbb{Z}/(m)$ is isomorphic to $\mathbb{Z}_m$, since it suffices to compose the two isomorphisms φ and γ
- **Concrete example:** $\mathbb{Z}/(6) \cong \mathbb{Z}_6 \cong \{0,1,2,3,4,5\}$
- The only difference with the case of $\mathbb{F}_p$ is that we do not obtain a field structure for a non prime m, but only a ring
- Again, in practice arithmetic in the ring $\mathbb{Z}/(m) \cong \mathbb{Z}_m$ is arithmetic on $\mathbb{Z}$ with reduction modulo m

Direct products of rings and CRT

- Direct products for rings are defined analogously to groups:

Definition

Given two rings $\langle R, +, \cdot \rangle$ and $\langle S, \circ, * \rangle$, define the following two operations $\oplus, \otimes$ on the Cartesian product $R \times S$:

- $(a_1, b_1) \oplus (a_2, b_2) = (a_1 + a_2, b_1 \circ b_2)$
- $(a_1, b_1) \otimes (a_2, b_2) = (a_1 \cdot a_2, b_1 * b_2)$

Then the structure $\langle R \times S, \oplus, \otimes \rangle$ is a ring and it is called the *direct product* of R and S

- If R and S are commutative rings, then $R \times S$ is commutative
- If R and S have a unity, then so does $R \times S$

Chinese Remainder Theorem and direct products

- The CRT can be generalized in terms of direct products:

Theorem

Let $M = m_1 m_2 \cdots m_k$ *with* $\gcd(m_i, m_j) = 1$ *for all* $i \neq j$. *Then the map* φ *defined for all* $a \in \mathbb{Z}_M$ *as*

$$\varphi(a) = (a \bmod m_1, a \bmod m_2, \cdots, a \bmod m_k)$$

is an isomorphism between the ring $\mathbb{Z}_M$ *and the direct product ring* $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$.

- **Example:** $M = 7 \cdot 11 \cdot 13$. Then $\mathbb{Z}_{1001} \cong \mathbb{Z}_7 \times \mathbb{Z}_{11} \times \mathbb{Z}_{13}$
- As a corollary, any system $x \equiv a_1 \mod m_1, \cdots, x \equiv a_k \mod m_k$ with $m_1, \cdots, m_k$ pairwise relatively prime admits a unique solution modulo M (the original CRT theorem)

Order and characteristic of a ring

- Similarly to groups, the *order* of a ring R is simply the number of elements of R

Definition

The *characteristic* of a ring $\langle R, +, \cdot \rangle$ is the smallest $n \in \mathbb{N}$ such that $nr = 0$ for all $r \in R$. If no such n exists, then the characteristic is 0

Examples:

- $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are all rings of characteristic 0
- For any $m \in \mathbb{Z}$, the characteristic of $\mathbb{Z}_m$ is m
- Any finite field has characteristic p, with p prime
- For any ring of characteristic 2, we have that $2a = a + a = 0$, $\Rightarrow a = -a$, and thus sum and subtraction coincide

Primitive element of a field

Theorem

Let F be a finite field. Then F has $q = p^n$ elements, where p is the characteristic of F.

Theorem

Given a finite field $\langle F, +, \cdot \rangle$, the multiplicative group $\langle F^*, \cdot \rangle$ of all nonzero elements of F is cyclic

- Any generator of the cyclic group F^* is called a *primitive element* of F
- The number ρ_q of primitive elements in the multiplicative group of the finite field $F = \mathbb{F}_q$ is $\phi(q-1)$
- **Examples:** $F = \mathbb{F}_7$, $\rho_7 = \phi(6) = 2$; $F = \mathbb{F}_{2^4}$, $\rho_{16} = \phi(15) = 8$

Primitive polynomial

Recall:

- Given an extension E of a field F, $\alpha \in E$ is called algebraic over F if it is a root of a polynomial in $F[x]$
- The set $J = \{f \in F[x] : f(\alpha) = 0\}$ of polynomials that have α as a root is a principal ideal of $F[x]$
- The unique irreducible polynomial $m_\alpha(x)$ that generates J is the *minimal polynomial* of α

Definition

A polynomial $f \in F[x]$ over a finite field $F = \mathbb{F}_q$ of degree $m \geq 1$ is called a *primitive* polynomial if it is the minimal polynomial of a primitive element α of $\mathbb{F}_{q^m}$

- A primitive polynomial is thus irreducible over $\mathbb{F}_q$ with a root $\alpha \in \mathbb{F}_{q^m}$ that generates the multiplicative group $\mathbb{F}^*_{q^m}$

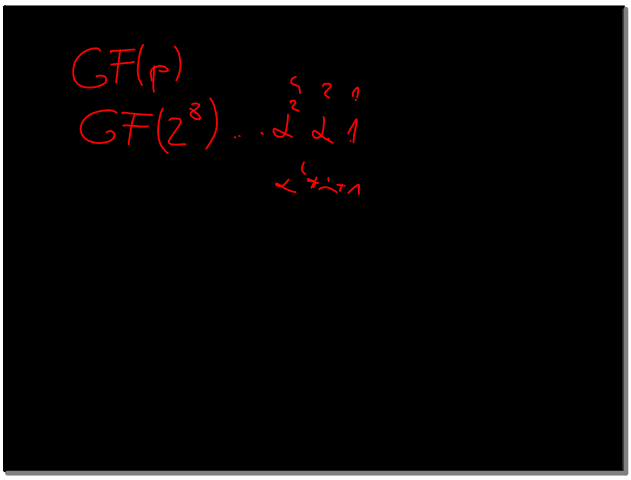
Representations of Finite Fields

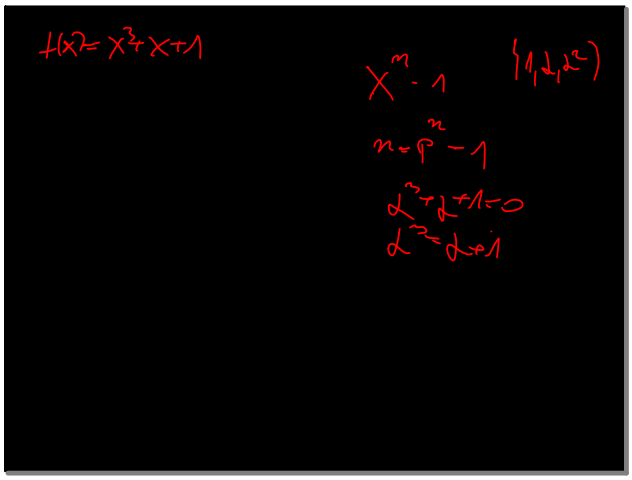
- Recall that up to now we saw only one method to represent the elements of a finite field, i.e. the *additive notation*
- Such method starts from a root α of a polynomial that is irreducible over the ground field F
- The elements of the extension are then represented as linear combinations of the basis $\{1, \alpha, \cdots, \alpha^{q^m-1}\}$
- Primitive polynomials can be used for an alternative representation of finite fields: the *multiplicative notation*
- A root of a primitive polynomial of degree m generates the multiplicative group of the extension of degree m

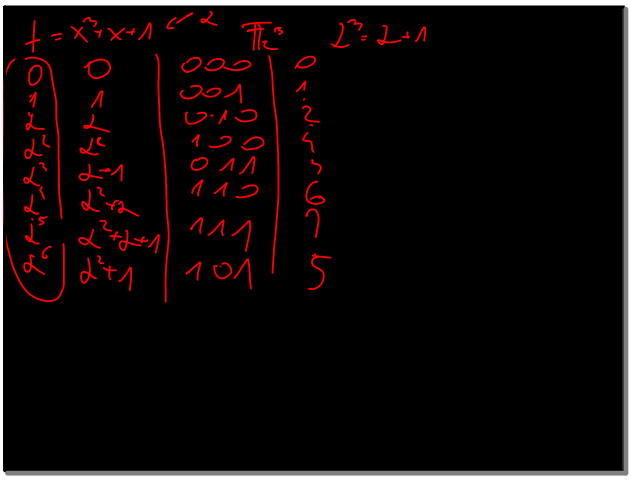
Representations of Finite Fields

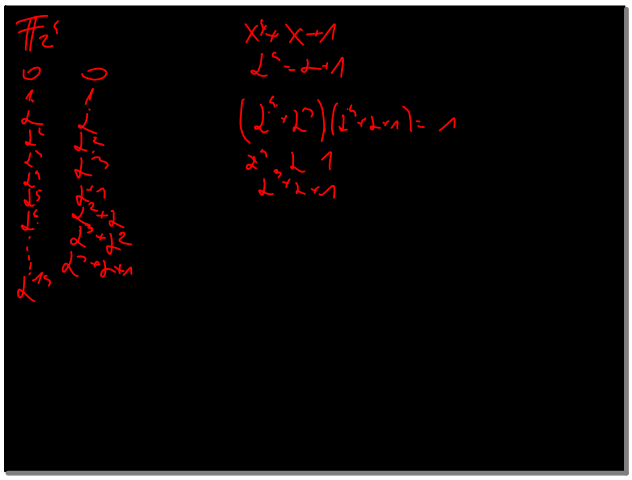
- **Example**: Let $F = \mathbb{F}_2$ (hence, $q = 2$) and consider the irreducible polynomial $f(x) = 1 + x + x^3 \in \mathbb{F}_2[x]$ of degree 3
- f is primitive (details omitted). Then, given a root α of f, we can represent the extension field $\mathbb{F}_{2^3}$ in two ways:
- **Additive**: since $\alpha^3 + \alpha + 1 = 0$ we have $\alpha^3 = \alpha + 1$, and the basis of the vector space is $\{1, \alpha, \alpha^2\}$
- **Multiplicative**: since α is a root of a primitive polynomial, we can map all 7 nonzero elements of $\mathbb{F}_{2^3}$ to powers of α
- The table below summarises the two different representations and the corresponding mapping to the vector space $\mathbb{F}_2^3$:

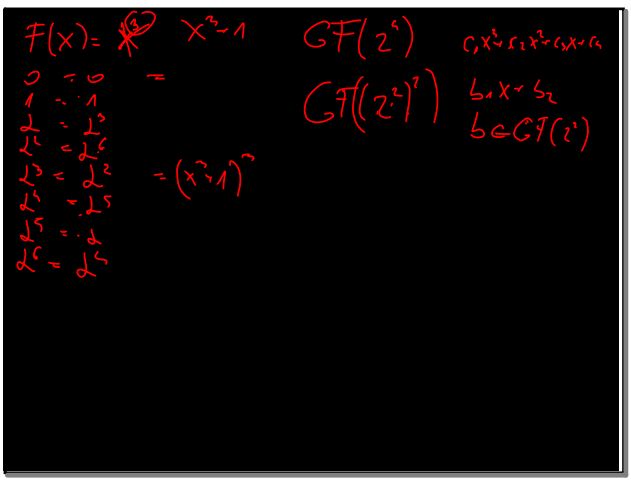
mult.	0	1	α	α^2	α^3	α^4	α^5	α^6
add.	0	1	α	α^2	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2+1
vect.	000	001	010	100	011	110	111	101

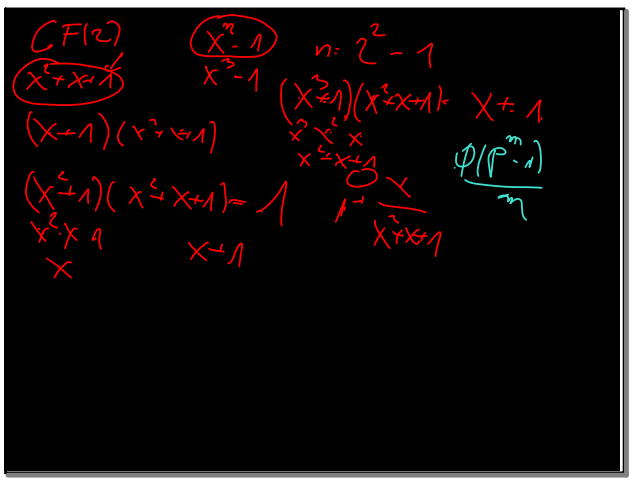

GF(p)
GF(2^8)

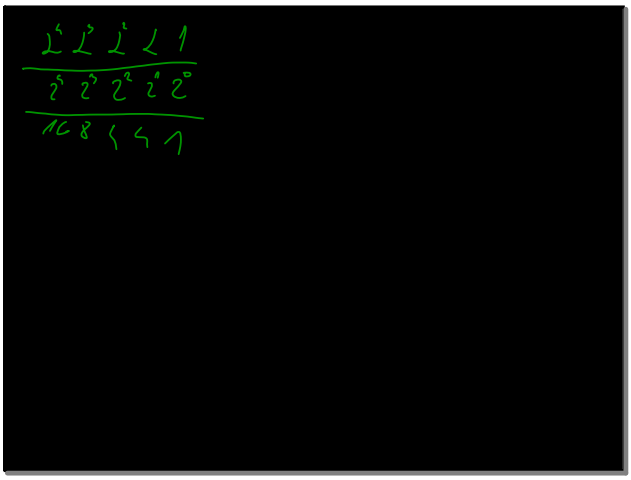

h(x) = x^3 + x + 1
x^n - 1
n = p^n - 1


h = x^3 + x + 1
F_2^3


F_2^4
x^4 + x + 1


F(x) =
x^3 - 1
GF(2^3)
GF((2^3)^2)


GF(2)
x^3 - 1
n = 2^2 - 1


2⁵ 2⁴ 2³ 2² 2¹ 2⁰
1 1 0 0 0 1