Counting modulo n

Mathematical Cryptography, Lectures 1 - 2

Contents

Sets with one binary operation

Definition

A set A with a binary operation $*$ is given, i.e. $*\colon A \times A \to A$.

- $(A, *)$ is called a *semigroup* if the operation $*$ is associative, i.e. for every $x, y, z \in A$ we have $x * (y * z) = (x * y) * z$.
- $(A, *)$ is called a *monoid* if the operation $*$ is associative and has an identity element, i.e. there exists $e \in A$, such that for every $x \in A$ we have $e * x = x = x * e$.
- $(A, *)$ is called a *group* if the operation $*$ is associative, has an identity element and has all inverse elements, i.e. for every $x \in A$ there exists $y \in A$, so that $x * y = e = y * x$.
- A group $(A, *)$ is called an *Abelian group* if the operation $*$ is commutative, i.e. for every $x, y \in A$ we have $x * y = y * x$.

Sets with two binary operations

Definition

Let A be a set with two binary operations, which are denoted as addition and multiplication.

- $(A, +, \cdot)$ is called a *ring* in case
  1. $(A, +)$ is an Abelian group (identity element denoted by 0);
  2. $(A, \cdot)$ is a semigroup;
  3. both distributive laws hold, i.e., for all $x, y, z \in A$ $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$.
- If the multiplication is commutative and has an identity element (denoted by 1), than we call it a *commutative ring with unity*.

Sets with two binary operations

Definition

- $(A, +, \cdot)$ is called a *domain* in case
  1. it is a ring with unity;
  2. it is non-trivial, i.e. $0 \neq 1$ (the identity element for addition is not simultaneously the identity element for multiplication);
  3. every non-zero element $0 \neq a \in A$ can be canceled, i.e. for every $x, y \in A$ the equality $a \cdot x = a \cdot y$ implies $x = y$, as well as the equality $x \cdot a = y \cdot a$ implies $x = y$.
- Moreover, if the multiplication is commutative, we speak about an *integrity domain*.

Note

A domain can also be defined as a non-trivial ring with unity, which has no zero divisors, i.e. for every $a, b \in A$, if $a \neq 0$, $b \neq 0$, then also $a \cdot b \neq 0$.

Sets with two binary operations

Definition

- $(A, +, \cdot)$ is called a *field* in case that
  1. it is a ring with unity;
  2. it is non-trivial, i.e. $0 \neq 1$ (the identity element for addition is not simultaneously a identity element for multiplication);
  3. every non-zero element has an inverse element, thus $(A - \{0\}, \cdot)$ is a group.
- Moreover if the multiplication is commutative, we speak about a *commutative field*.

Note

Any field obviously is a domain, since the cancellation law holds for all invertible elements.

Sets with two binary operations

Example

We will mostly be interested in the set of all integers $\mathbb{Z}$ with addition and multiplication operations.

1. $(\mathbb{Z}, +)$ is an Abelian group, $(\mathbb{Z}, \cdot)$ is a commutative monoid.
2. $(\mathbb{Z}, +, \cdot)$ forms a non-trivial commutative ring with unity,
   - it has no zero divisors (any non-zero number can be cancled), so it is an integrity domain,
   - only the 1 and -1 have an inverse element, so it is not a field.

Counting with integers

Division with remainder theorem

Let $a, b \in \mathbb{Z}$, where $b > 0$. There exist unique $q, r \in \mathbb{Z}$ such that

$$a = q\,b + r \quad \text{and} \quad 0 \leq r < b.$$

Consequences of division with remainder property

1. divisibility relation, primes and composites, unique factorization into primes
2. greatest common divisor, Euclid's algorithm, Diophantes' equations
3. congruence modulo n, residue classes modulo n, field $\mathbb{Z}_p$

Divisibility relation

Definition

For every $a, b \in \mathbb{Z}$, we say that a *divides* b (or a is a divisor of b) if $b = ka$ for some $k \in \mathbb{Z}$. We denote the fact by $a \mid b$.

The divisibility relation is an ordering on N (it is reflexive, antisymmetric and transitive).

However, the divisibility relation is not antisymmetric on $\mathbb{Z}$, where $a \mid b$ and $b \mid a$ if and only if $b = \pm a$.

Primes

Definition

Len $n > 1$ be a positive integer. n is *prime*, if only 1 and n divide n among positive integers. Otherwise, n is *composite*, so it can be written as a product of two positive integers less than n.

The "brute force" primality test: a number n is prime if no prime $p \leq \sqrt{n}$ divides n.

The "brute force" primality testing (or the problem of factorizing n into a product of two smaller numbers) has exponential time complexity depending on the number of digits of n. We have to perform $\sqrt{n} = 2^{\frac{1}{2}\log_2(n)}$ divisions.

Primes

Fundamental theorem of arithmetic

Every positive integer $n \geq 2$ can be expressed as a product of powers of different primes,

$$n = p_1^{e_1} \cdot \ldots \cdot p_k^{e_k}.$$

This expression is unique, up to a reordering of the primes.

The existence of a factorization can be proved by induction on n. However, the Bezout theorem is needed to prove uniqueness. So let us first introduce one more chapter.

Greatest common divisor

Definition

The greatest common divisor of two numbers $a, b \in \mathbb{Z}$ is a number $d \in \mathbb{Z}$ that satisfies:

1. d divides both of them, a and b
2. d is divisible by all common divisors of both numbers
3. $d \geq 0$

We denote $d = \gcd(a, b)$.

By analogy, we can define *the least common multiple* $\mathrm{lcm}(a, b)$.

Greatest common divisor

Definition

If $gcd(a, b) = 1$, then we say that a, b are *relatively prime*.

Finding $\gcd(a, b)$

If the prime factorisations of a and b are known, then $\gcd(a, b)$ contains just all common primes in common powers.
But of course, finding the factorization of a or b is an exponential problem.

Euclidean algorithm

Euclidean algorithm

We are looking for $\gcd(a, b)$. Suppose that $a \geq b > 0$.

1. Divide with a remainder: $a = q\,b + r$ and $0 \leq r < b$
2. If the remainder $r = 0$, then $\gcd(a, b) = b$.
3. If the remainder $r > 0$, then look for $\gcd(b, r)$.

This is a recursive algorithm based on division with remainder.

- If the remainder $r > 0$, the pair a, b has the same common divisors as the pair b, r. So also $\gcd(a, b) = \gcd(b, r)$.
- Since remainders are getting smaller non-negative integers, the algorithm will stop in a finate number of steps.
- Time complexity - the number of divisions with remainder is linear according to a number of digits of b.

Euclidean algorithm

Euclidean algorithm

Input: integers $a \geq b \geq 0$
Output: $d = \gcd(a, b)$
Algorithm:

- $r \leftarrow a$, $r' \leftarrow b$
- while $r' \neq 0$ do
  - find $q, r'' \in \mathbb{N}$ such that $r = qr' + r''$ and $0 \leq r'' < r'$
  - $r \leftarrow r'$, $r' \leftarrow r''$
  - enddo
- $d \leftarrow r$
- output d

Extended Euclidean algorithm

Bezout's Theorem

The greatest common divisor of numbers $a, b \in \mathbb{Z}$ is their integer combination, or

$$\gcd(a, b) \;=\; s\,a \;+\; t\,b \quad \text{for some} \quad s, t \in \mathbb{Z}.$$

To find the integer coefficients $s, t \in \mathbb{Z}$ from Bezout's theorem, we can use an *extended Euclidean algorithm*:

- In each step of Euclidean algorithm we express a current remainder as an integer combination of a, b.
- $\gcd(a, b)$ is the last non-zero reminder, so finally we combine by a, b their greatest common divisor.

Extended Euclidean Algorithm

Extended Euclidean Algorithm

Input: integers $a \geq b \geq 0$
Output: natural numbers d, s, t where $d = \gcd(a, b) = sa + tb$

- $r \leftarrow a$, $r' \leftarrow b$
- $s \leftarrow 1$, $t \leftarrow 0$
- $s' \leftarrow 0$, $t' \leftarrow 1$
- while $r' \neq 0$ do
  - find $q, r'' \in \mathbb{N}$ such that $r = qr' + r''$ and $0 \leq r'' < r'$
  - $s'' \leftarrow s - qs'$, $t'' \leftarrow t - qt'$
  - $r \leftarrow r'$, $r' \leftarrow r''$, $s \leftarrow s'$, $s' \leftarrow s''$, $t \leftarrow t'$, $t' \leftarrow t''$
  - enddo
- $d \leftarrow r$
- output d, s, t

Diophantine equations

Theorem

The equation $ax + by = c$, where $a, b, c \in \mathbb{Z}$, has a solution in $\mathbb{Z}$ only if $\gcd(a, b) \mid c$.

If there exists any integer solution of the Diophantine equation, then there are infinitely many of them and they are in a form

$$(x, y) = (x_p, y_p) + k\,(x_0, y_0) \quad \text{for any} \quad k \in \mathbb{Z},$$

where (x_p, y_p) is a partial solution (found by extended Euclidean algorithm) and (x_0, y_0) is a "relatively prime" solution of a homogeneous equation $ax + by = 0$,
so $(x_0, y_0) = (\frac{b}{d}, -\frac{a}{d})$, where $d = \gcd(a, b)$.

Diophantine equations

Example

Solve the equation $105x + 39y = 6$ in Z.

Extended Euclidean algorithm for $a = 105$, $b = 39$:

$$\begin{array}{rcl@{\qquad}rcl}
105 &=& 2 \cdot 39 + 27 & 27 &=& a - 2b \\
39 &=& 1 \cdot 27 + 12 & 12 &=& -a + 3b \\
27 &=& 2 \cdot 12 + 3 & 3 &=& 3a - 8b \\
12 &=& 4 \cdot 3 + 0 & 0 &=& -13a + 35b
\end{array}$$

$\gcd(105, 39) = 3 \mid 6$, so the solution in $\mathbb{Z}$ exists.

A partial solution is $(x_p, y_p) = 2 \cdot (3, -8) = (6, -16)$,
a solution of the homogeneous equation is $(x_0, y_0) = (-13, 35)$,
where its parts are relatively prime.
All solutions in $\mathbb{Z}$ are $(x, y) = (6, -16) + k(-13, 35)$ for any $k \in \mathbb{Z}$.

Factorization into primes

Proposition

- If $a \mid bc$ and $\gcd(a, c) = 1$, then $a \mid b$.
- If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Fundamental theorem of arithmetic

Every positive integer $n \geq 2$ can be expressed as a product of primes:

$$n = p_1^{e_1} \cdot \ldots \cdot p_k^{e_k} = \prod_{i=1}^{k} p_i^{e_i},$$

where $p_1 < \ldots < p_k$ are primes, $e_i \geq 1$ for $1 \leq i \leq k$, $k \geq 1$.
This expression is unique, up to a reordering of the primes.
We are talking about a unique *prime factorization* of n.

Congruence modulo n

Definition

Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Number a is *congruent* to b *modulo n*, if $n \mid (b - a)$. We denote it by $a \equiv b \pmod{n}$.

Proposition

The following statements are equivalent:

- $a \equiv b \pmod{n}$
- a, b both have the same remainder when divided by n
- $b = a + kn$ for some $k \in \mathbb{Z}$

Congruence modulo n

Theorem

A congruence relation modulo n is an equivalence relation on the set of integers (it is reflexive, symmetric and transitive).

Consequence

A congruence relation modulo n decomposes the set of integers into classes of mutually equivalent elements, called *residue classes modulo n*, the set of all residue classes modulo n is denoted by $\mathbb{Z}_n$.

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}, \text{ where } [a]_n = \{a + kn | k \in \mathbb{Z}\}$$

Congruence modulo n

Theorem

Congruence relation modulo n is respected by integer addition and multiplication:
If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$,
then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$.

Consequence

We can correctly define addition and multiplication on the set $\mathbb{Z}_n$ of residue classes, working with representatives of classes:

$$[a]_n \oplus [b]_n = [a+b]_n, \quad [a]_n \odot [b]_n = [a \cdot b]_n$$

Residual classes modulo n

Thanks to the definition through representatives, operations $\oplus$ and $\odot$ inherit most of the properties, which integer addition and multiplication have.

Proposition

The triple $(\mathbb{Z}_n, \oplus, \odot)$ forms a commutative ring with a unit, which is called a *factor ring of residue classes modulo n*.

In the following we simplify the notation:

$$(\mathbb{Z}_n = \{0, 1, \ldots, n-1\}, +, \cdot)$$

Linear equations in $\mathbb{Z}_n$

The linear equation $ax = b$ in $\mathbb{Z}_n$ can be converted to the Diophantine equation by the following modifications:

- $ax = b$ in $\mathbb{Z}_n$
- $ax \equiv b \pmod{n}$ in $\mathbb{Z}$
- $ax + ny = b$ in $\mathbb{Z}$

Theorem

The linear equation $ax = b$ has a solution in $\mathbb{Z}_n$ if and only if $\gcd(a, n) \mid b$.

If x_p is one solution, then each solution has the form $x = x_p + kx_0$, where $x_0 = \frac{n}{\gcd(a,n)}$, $k \in \mathbb{Z}$.
This gives $d = \gcd(a, n)$ different solutions in the ring $\mathbb{Z}_n$.

Finding inverse elements in $\mathbb{Z}_n$

Consequence

The equation $ax = 1$ has a solution in $\mathbb{Z}_n$ only if $\gcd(a, n) = 1$ and the solution is unique. It is an inverse element of a in $\mathbb{Z}_n$ and it can be found by the Extended Euclidean algorithm.

Propositoin

The element $a \in \mathbb{Z}_n$ is invertible in $\mathbb{Z}_n$ if and only if a and n are relatively prime numbers.

Only ± 1 were invertible in the ring $\mathbb{Z}$.
Now we can have more invertible elements in the ring $\mathbb{Z}_n$, specially for $n = p$ prime all non-zero elements are invertible.

Residue classes modulo prime p

Theorem

The ring $(\mathbb{Z}_n, +, \cdot)$ is a field if and only if $n = p$ is prime.

Example

In Z_5, $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$.

Note

If n is a composite number, then the ring $(\mathbb{Z}_n, +, \cdot)$ is not even an integrity domain, since every number not relatively prime to n is a zero divisor.

For example, the equation $2x = 4$ has two solutions in $\mathbb{Z}_6$, $x_1 = 2$, $x_2 = 5$, thus the non-invertible element $a = 2$ cannot be cancelled.

Counting modulo n

Literature

- Velebil: Discrete mathematics. Chapters 2.1-3, 3.1 and 3.4. ftp://math.feld.cvut.cz/pub/velebil/y01dma/dma-notes.pdf
- Shoup: A Computational Introduction to Number Theory and Algebra. Chapters 1.1-3, 2.1-3, 2.5, 4.1-2. http://shoup.net/ntb/