Coding Theory

(Mathematical Background I)

Lector: Nikolai L. Manev

Institute of Mathematics and Informatics, Sofia, Bulgaria

Greatest common divisor

Euclidean Property of the integers: For any two integers a and $b,\ b \neq 0,$ there exist unique $q, r \in \mathbb{Z},$ such that

$$a = bq + r, \quad 0 \leq r < |b|.$$

The integer r is called *reminder of a modulo b.*

Greatest common divisor

Euclidean Property of the integers: For any two integers a and $b,\ b \neq 0,$ there exist unique $q, r \in \mathbb{Z},$ such that

$$a = bq + r, \quad 0 \leq r < |b|.$$

The integer r is called *reminder of a modulo b.*

The *greatest common divisor* (gcd) of $a, b \in \mathbb{Z}$ is the integer d which satisfies:

1. $d|a$ and $d|b$,
2. if $d_1|a$ and $d_1|b$, then $d_1|d$,
3. $d > 0$.

We denote it by $d = (a, b)$.

Greatest common divisor

Theorem. The greatest common divisor $d = (a, b)$ exists for any two integers a, b, not both zero, and there exist uniquely determined integers u, v such that

$$d = ua + vb.$$

Properties:

(1) $(a, ab) \sim a$ for any $a, b \in \mathbb{Z}$.

(2) $(a, -b) = (a, b)$, for any $a, b \in \mathbb{Z}$.

(3) $(a, b - qa) = (a, b)$, for any $a, b, q \in \mathbb{Z}$.

(4) $(a, (b, c)) = ((a, b), c) = (a, b, c)$, for any $a, b, c \in \mathbb{Z}$.

(5) $(ac, bc) \sim (a, b)c$, for any $a, b, c \in \mathbb{Z}$.

(6) if $(a, b) = (a, c) = 1$, then $(a, bc) = 1$, $a, b, c \in \mathbb{Z}$.

Greatest common divisor

$$
\begin{array}{rcll}
a & = & bq_1 + r_1, & 0 < r_1 < |b| \\
b & = & r_1 q_2 + r_2, & 0 < r_2 < r_1 \\
r_1 & = & r_2 q_3 + r_3, & 0 < r_3 < r_2 \\
\cdots & \cdots & \cdots\cdots\cdots\cdots & \cdots\cdots\cdots\cdots \\
r_{n-3} & = & r_{n-2} q_{n-1} + r_{n-1}, & 0 < r_{n-1} < r_{n-2} \\
r_{n-2} & = & r_{n-1} q_n, &
\end{array}
$$

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-2}, r_{n-1}) = r_{n-1}.$$

If we set

$$u_0 = 0, \quad u_1 = 1, \quad u_j \stackrel{\text{def}}{=} u_{j-2} - q_j u_{j-1}$$

$$v_0 = 1, \quad v_1 = -q_1, \quad v_j \stackrel{\text{def}}{=} v_{j-2} - q_j v_{j-1}.$$

then $r_j = a\, u_j + b\, v_j.$

Greatest common divisor

Therefore, $(a,b) = r_{n-1},\ u = u_{n-1}$ and $v = v_{n-1}$, where n is defined by $r_n = 0$.

a	1	0	$\mathbf{q}$
b	0	1	q_1
r_1	u_1	v_1	q_2
r_2	u_2	v_2	q_3
$\vdots$	$\vdots$	$\vdots$	$\vdots$
r_{n-1}	u_{n-1}	v_{n-1}	q_n
0			

Algorithm 1. *Data:* a, b *integers*

($a > b > 0$)

Output: $d = (a,b),\ u,\ v$ integers

Variables:

$A = (a_1, a_2, a_3),\ B = (b_1, b_2, b_3),$

$C = (c_1, c_2, c_3);\quad q$ integer.

$A := (a, 1, 0),\ B := (b, 0, 1),$

$C := (1, 0, 0).$

while $c_1 \neq 0$ do $\quad q := \lfloor \frac{a_1}{b_1} \rfloor,$

$C := A - qB, \quad A := B, \quad B := C$

else

$d := a_1,\ u := a_2,\ v := a_3.$

Greatest common divisor - an example

29	1	0	q
25	0	1	1
4	1	-1	6
1	-6	7	4
0			

The required values of u and v are in the forth row, 2nd and 3rd column - the row before 0 in the first row. Hence $(29, 25) = 1$, and $u = -6$, $v = 7$. Therefore

$$29 \cdot (-6) + 25 \cdot 7 = 1.$$

Congruences

For a, b, m, integers, we say that a *is congruent to* b *modulo* m, and write

$$a \equiv b \pmod{m},$$

if m divides $a - b$.

Congruences

For a, b, m, integers, we say that a *is congruent to* b *modulo* m, and write

$$a \equiv b \pmod{m},$$

if m divides $a - b$.

(1) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $(a \pm c) \equiv (b \pm d) \pmod{n}$;

(2) If $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$;

(3) If $f(x) \in \mathbb{Z}[x]$, $a \equiv b \pmod{n}$, then $f(a) \equiv f(b) \pmod{n}$;

(4) If $ma \equiv mb \pmod{n}$, $d = (m, n)$), then $a \equiv b \pmod{\frac{n}{d}}$;

(5) If $a \equiv b \pmod{n}$ and d is a common divisor of a and n (in partial $d = (a, n)$), then $d \mid b$.

Ring and fields

Let R be a set with two binary operations: $a+b$ and ab.
R is a *field* if:

1. $a+b=b+a$,
2. $(a+b)+c=a+(b+c)$,
3. $\exists\, 0$: $a+0=a$,
4. $\forall a, \exists -a$: $a+(-a)=0$,
5. $ab=ba$,
6. $(ab)c=a(bc)$,
7. $a(b+c)=ab+ac$,
8. $1\cdot a=a$,
9. For any $a\neq 0$ $\exists\, a^{-1}$: $aa^{-1}=1$.

The first 8 axioms define a *commutative ring with identity*.
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields; $\mathbb{Z}$ is a ring, but not a field.
In a field both equations $ax=b$ and $ya=b$ has unique solution for $a\neq 0$.

The ring $\mathbb{Z}_n$

Let n be a positive integer. Consider the set of all nonnegative reminders modulo n:

$$\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n-1\}.$$

Define addition $a \oplus b$ and multiplication $a \circ b$ in $\mathbb{Z}_n$ by:

$$a \oplus b \stackrel{\text{def}}{=} a + b \pmod{n}$$

$$a \circ b \stackrel{\text{def}}{=} ab \pmod{n}$$

A nonzero element a of $\mathbb{Z}_n$ is invertible if and only if $(a, n) = 1$. $\mathbb{Z}_n$ is a field if and only if n is a prime.

$\mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_{11}$ are fields; $\mathbb{Z}_6, \mathbb{Z}_9$ are only commutative rings.
For $a \neq 0$ find a^{-1}: there exist u, v such that $au + vn = 1$.
Then $au \equiv 1 \pmod{n}$, that is $aa^{-1} = 1$ in $\mathbb{Z}_n$.

The Fermat Little Theorem: If p is prime, then $a^{p-1} \equiv 1 \pmod{p}$ for any $a \not\equiv 0 \pmod{p}$.

Theorem. For any prime p there exist such an integer a with $(a, p) = 1$ that all powers $1, a, a^2, a^3, \ldots, a^{p-2}$ are non-congruent one another, that is,

$$\mathbb{Z}_p = \{0, 1, a, a^2, a^3, \ldots, a^{p-2}\}.$$

Any element of $\mathbb{Z}_p$ with the above property is called *primitive element* of the field $\mathbb{Z}_p$.

Theorem (Euler). Let $n > 0$ be an integer. For any $(a, n) = 1$, we have $a^{\varphi(n)} \equiv 1 \pmod{n}$, where $\varphi(n)$ is the number integers $< n$ and co-prime with n (*Euler function*).

If $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, then $\varphi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k})$.

Characteristic of a field

Definition. The *characteristic* of a field (ring) $\mathbb{F}$ is the smallest positive integer m (written $\mathrm{char}\mathbb{F} = m$) such that $m \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{m} = 0$. If such a integer does not exist we say that the characteristic is zero.

$\mathrm{char}\mathbb{Q} = \mathrm{char}\mathbb{R} = \mathrm{char}\mathbb{C} = 0$, but $\mathrm{char}\mathbb{Z}_5 = 5$.

If $\mathrm{char}\mathbb{F} = m$, then $m \cdot a = \underbrace{a + a + \cdots + a}_{m} = 0$ for any $a \in \mathbb{F}$.

Characteristic of a field

Definition. The *characteristic* of a field (ring) $\mathbb{F}$ is the smallest positive integer m (written $\mathrm{char}\mathbb{F} = m$) such that $m \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{m} = 0$. If such a integer does not exist we say that the characteristic is zero.

$\mathrm{char}\mathbb{Q} = \mathrm{char}\mathbb{R} = \mathrm{char}\mathbb{C} = 0$, but $\mathrm{char}\mathbb{Z}_5 = 5$.

If $\mathrm{char}\mathbb{F} = m$, then $m \cdot a = \underbrace{a + a + \cdots + a}_{m} = 0$ for any $a \in \mathbb{F}$.

Theorem. The characteristic of a finite field is always a prime integer.

Theorem. If $\mathrm{char}\mathbb{F} = p$, then for any $a, b \in \mathbb{F}$

$$(a + b)^p = a^p + b^p.$$

Cosets in a linear space

Let L be a linear space over the field $\mathbb{F}$ and $U \subset L$ be its subspace, that is, for any $u, v \in U$ and $\lambda \in \mathbb{F}$:

$$u \pm v \in U \quad \text{and} \quad \lambda u \in U.$$

Definition. For a fixed vector $a \in L$, the subset

$$a + U \stackrel{\text{def}}{=} \{a + u \mid u \in U\}$$

is called *coset, or affine subspace, of U in L*. Any vector of $a + U$ is referred to as a *representative* of the coset. The set of all cosets of U in L is called *quotient space L/U*.

Obviously, two vectors of $a, b \in L$ belong to one and the same coset if and only if $a - b \in U$.

There is one-to-one correspondence between U and $a + U$, that is $|U| = |a + U|$.

Polynomials

Let $a(x)$ and $b(x)$ be two polynomials in x over the field $\mathbb{F}$:

$$\begin{aligned} a(x) = &\quad a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \neq 0, \\ b(x) = &\quad b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0, \quad b_m \neq 0. \end{aligned}$$

Euclidean Property: Given two polynomials $a(x)$ and $b(x)$, $b(x)$ not identically 0, there exist $q(x), r(x) \in \mathbb{F}[x]$, such that

$$a(x) = b(x)q(x) + r(x),$$

and either $r(x) \equiv 0$, or $\deg r(x) < \deg b(x)$.

Polynomials 2

The *greatest common divisor* (gcd) of $a(x)$ and $b(x)$ is the polynomial $d(x)$ which satisfies:

1. $d(x)|(x)$ and $d(x)|b(x)$,
2. if $d_1(x)|a(x)$ and $d_1(x)|b(x)$, then $d_1(x)|d(x)$,
3. $d(x)$ is a monic polynomial, i.e., the coefficient of the highest power of x is equal to 1.

The *greatest common divisor* (gcd) of $a(x)$ and $b(x)$ is the polynomial $d(x)$ which satisfies:

1. $d(x)|(x)$ and $d(x)|b(x)$,
2. if $d_1(x)|a(x)$ and $d_1(x)|b(x)$, then $d_1(x)|d(x)$,
3. $d(x)$ is a monic polynomial, i.e., the coefficient of the highest power of x is equal to 1.

In the ring of polynomials over a field the greatest common divisor $d(x) = (a(x), b(x))$ exists for any two polynomials, and there exist polynomials $u(x), v(x)$ such that

$$d(x) = u(x)a(x) + v(x)b(x).$$

Definition. Let $a(x)$, $b(x)$ and $m(x)$ be polynomials in x over a field (or a ring) $\mathbb{F}$. We say that $a(x)$ *is congruent to* $b(x)$ *modulo* $m(x)$, written

$$a(x) \equiv b(x) \pmod{m(x)},$$

if $m(x)$ divides $a(x) - b(x)$.

The congruences in a ring of polynomials posses the same properties as the congruences in $\mathbb{Z}$.

Example: In the ring $\mathbb{Z}_2[x]$:
$x^3 + 1 \equiv 0 \pmod{x^2 + x + 1}$ and $x^2 \equiv x + 1 \pmod{x^2 + x + 1}$.

In $\mathbb{Z}_3[x]$: $x^3 - 1 \equiv 2x + 2 \pmod{x^2 + 1}$.

Definition. Let $\mathbb{F}$ and $\mathbb{K}$ be fields such that $\mathbb{F} \subseteq \mathbb{K}$.
A polynomial $f(x) \in \mathbb{F}[x]$ is called *irreducible over* $\mathbb{K}$, if it cannot be represented as a product of two polynomials over $\mathbb{K}$ with degree at least one, that is, in the form

$$f(x) = a(x)b(x),\ a(x), b(x) \in \mathbb{K}[x].$$

Example: $x^2 - 2 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$, but reducible over $\mathbb{R}$: $x^2 - 2 = (x - \sqrt{2})(x - \sqrt{2})$.
The polynomial $x^2 + 1 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$ and $\mathbb{R}$, but reducible over $\mathbb{C}$.
Polynomials $x^2 + x + 1$ and $x^3 + x + 1$ are irreducible over $\mathbb{Z}_2$, but $x^2 + 1 = (x + 1)^2$ is reducible over $\mathbb{Z}_2$.

Theorem. Let $\mathbb{F}$ and $\mathbb{K}$ be fields such that $\mathbb{F} \subseteq \mathbb{K}$.
A polynomial $f(x) \in \mathbb{F}[x]$ is divisible by $x - \alpha,\ \alpha \in \mathbb{K}$ if and only if $f(\alpha) = 0$. If $\deg f(x) = n$, then $f(x)$ has at most n roots.

Theorem. For any field $\mathbb{F}$ there exists an extension $\mathbb{K} \supseteq \mathbb{F}$, where any polynomial $f(x) \in \mathbb{F}[x]$ can be decomposed in a product of polynomials of degree one:

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

where $n = \deg f(x)$.

The minimal such extension for a given polynomial $f(x)$ is called the *splitting field of* $f(x)$.

For example, any polynomial over $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ can be factorized into a product of linear polynomials. Examples of splitting fields we will give later.

The end of the part

Thank You for Attention!