DIVISIBILITY THEORY

$\mathbb{Z} = \mathbb{N} \cup -\mathbb{N}$

$+, \cdot$

$(\mathbb{Z}, +, \cdot)$ commutative ring with unity

integral domain $ab = 0 \Rightarrow a = 0$ or $b = 0$

Divisibility relation:

$a | b$ if $\exists c \quad b = a \cdot c$

Properties of divisibility

a) $a | 0, \quad 1 | a, \quad a | a$

b) $a | 1 \iff a = \pm 1$

c) $a | b$ and $b | a \iff a = \pm b$

d) $a | b$ and $b | c \Rightarrow a | c$

e) $a | b$ and $b \neq 0$ then $|a| \leq |b|$

f) $a | b$ and $a | c$ then $a | \underbrace{bx + cy}$ $\forall x, y \in \mathbb{Z}$

$\mathbb{Z}$ is a PID (principal ideal domain)

I ideal of $\mathbb{Z}$ $\qquad I = (a)$

$a | b \qquad b \in (a)$

Given $a, b \in \mathbb{Z}$ $\longrightarrow$ not both 0

consider

$I = (a, b) = \{ax + by \mid x, y \in \mathbb{Z}\}$

$I = (d)$ for a unique $d \in \mathbb{Z}$ $d > 0$

d = greatest common divisor of a, b

$\gcd(a,b)$

in fact: $d \mid a$, $d \mid b$

and if $d' \mid a$ and $d' \mid b$ then $d' \mid d$

$d \in (d')$

In particular $d = ax_0 + by_0$ $\quad x_0, y_0 \in \mathbb{Z}$

BÉZOUT IDENTITY

If $d = 1$ a, b are said relatively prime

$1 = ax_0 + by_0$

Property

1) a, b relatively prime $\Leftrightarrow$ $1 = ax + by$ for some x, y.

2) if $\gcd(a,b) = 1$ and $a \mid bc$ then $a \mid c$

$ax + by = 1$

$\underbrace{acx}_{} + \underbrace{bcy}_{} = c$.

Algorithm of division

Given $a, b \in \mathbb{Z}$ $b \neq 0$ then $\exists!\, q, r$

quotient remainder

$$a = qb + r \qquad 0 \leq r < b$$

Example

$a = 37 \quad b = 7 \qquad 37 = 5 \cdot 7 + 2 \qquad q = 5 \quad r = 2$

$a = -37 \quad b = 7 \qquad -37 = -5 \cdot 7 - 2$

$= -5 \cdot 7 - 2 + 7 - 7$

$= -6 \cdot 7 + 5$

$\underset{a}{5} = \underset{q}{0} \cdot \underset{b}{37} + \underset{r}{5} \qquad q = 0 \quad r = 5$

Euclidean algorithm for GCD

$a, b \qquad b \neq 0$

$a = q_1 b + r_1 \qquad 0 \leq r_1 < b$

if $r_1 = 0 \Rightarrow b = \gcd(a, b)$

$b = q_2 r_1 + r_2 \qquad 0 \leq r_2 < r_1$

$\vdots$

$r_{n-2} = q_n r_{n-1} + r_n \qquad 0 \leq r_n < r_{n-1} \dots < b$

$r_{n-1} = q_{n+1} r_n + \cancel{0}$ $\qquad \downarrow$ must stop

$r_n =$ last non zero remaind.

$= \gcd(a, b)$

Indeed

1. By going across the chain of equalities from the bottom to the top we see that $r_n | r_{n-1} \dots$

$\rightsquigarrow \quad r_n \mid b$ and $r_n \mid a$

② Assume that $d' \mid a$ and $d' \mid b$

Then $d' \mid r_1 \; r_2 \ldots\ldots r_n$

$\rightsquigarrow \quad r_n = \gcd(a, b)$.

Bézout identity

$$r_n = r_{n-2} - q_n r_{n-1}$$
$$= (1 + q_n q_{n-1}) r_{n-2} + (-q_n) r_{n-1}$$
$$\vdots$$
$$r_n = A a + B b$$

Example $\gcd(12378, 3054)$

$$12378 = 4 \cdot 3054 + 162$$
$$3054 = 18 \cdot 162 + 138 \leftarrow$$
$$162 = 1 \cdot 138 + 24 \leftarrow$$
$$138 = 5 \cdot 24 + 18 \leftarrow$$
$$24 = 18 + 6 \leftarrow$$
$$18 = 3 \cdot 6$$

$6 = \gcd(12378, 3054)$

$$6 = 24 - 18 = 24 - (138 - 5 \cdot 24) = 6 \cdot 24 - 138$$
$$= 6 \cdot (162 - 138) - 138 = 6 \cdot 162 - 7 \cdot 138$$
$$= 6 \cdot 162 - 7 \left(3054 - 18 \cdot 162\right) = -7 \cdot 3054 + 132 \cdot 168$$

$$= \boxed{132 \cdot 12378 - 535 \cdot 3054}$$

There are many possibilities for writing
$d = ax + by$

$$6 = 132 \cdot 12378 - 535 \cdot 3054 +$$
$$12378 \cdot 3054 - 12378 \cdot 3054$$
$$= 12378 \underbrace{(132 + 3054)}_{A'} - 3054 \underbrace{(535 + 12378)}_{B'}$$

LEAST COMMON MULTIPLE of $a, b \in \mathbb{Z}$ $\quad a, b$ not both 0

$m = \mathrm{lcm}(a, b)$ it is the unique $m > 0$
such that $a \mid m$, $b \mid m$
and if $a \mid m'$, $b \mid m' \Rightarrow m \mid m'$.

Exercise : prove that
$$\gcd(a,b)\, \mathrm{lcm}(a,b) = ab$$
($\Rightarrow$ if a, b rel. prime then $\mathrm{lcm}(a,b) = ab$).

Rem gcd and lcm can be defined for more than two numbers in the obvious way.

Exercises

A) Find $\gcd(272, 1479)$, $\mathrm{lcm}(272, 1479)$

and write the Bézout identity.

3) Assume that $\gcd(a,b)=1$

prove that

$\gcd(a+b, a-b) = 1$ or 2

$\gcd(2a+b, a+2b) = 1$ or 3

$\gcd(a+b, a^2+b^2) = 1$ or 2

Bézout identity provides a solution to the equation $ax+by=d$ $\quad d=\gcd(a,b)$

DIOPHANTINE EQUATION

$ax+by=c$ $\quad a,b,c\in\mathbb{Z}$

linear diophantine equation in two variable

→ A solution is a pair x_0, y_0 of integers s.t $ax_0+by_0=c$.

Solutions do not always exist. Ex

$3x+21y=5$

does not admit solutions because

$3 \mid 3x+21y \quad \forall x,y$ but $3 \nmid 5$.

Theorem $a, b \in \mathbb{Z}$ not both zero

A) The linear diophantine equation

$$ax + by = c$$

admits a solution $\Leftrightarrow$ $\gcd(a,b) \mid c$

B) If x_0, y_0 is a particular solution then

$$\boxed{\begin{cases} x = x_0 + \frac{b}{d} k \\ y = y_0 - \frac{a}{d} k \end{cases}}$$

where $d = \gcd(a,b)$ and $k \in \mathbb{Z}$.

Exercise

Write 100 as a sum of two positive integers which are multiple of 7 and 11 respectively.

$$100 = 7 \cdot x + 11 \cdot y$$

$$1 = 7 x_0 + 11 \cdot y_0$$

$$100 = 7 \cdot X_0 + 11 \cdot Y_0$$

CONGRUENCES

MODULO

In $\mathbb{Z}$ we define $a, b, m \in \mathbb{Z}$

$$\boxed{a \equiv b \mod m \quad \text{if} \quad m \mid a - b}$$

Congruence relation mod m is an eq.ce relation

A) $a \equiv a \mod m \quad \forall a \in \mathbb{Z}$

b) $a \equiv b \mod m \Rightarrow b \equiv a \mod m$

c) $a \equiv b \mod m,\ b \equiv c \mod m \Rightarrow a \equiv c \mod m$

Equivalence classes

$$[a]_m = \{ b \in \mathbb{Z} \mid a \equiv b \mod m \} = \bar{a}$$

RESIDUAL CLASSES MOD m.

$\bar{a} = \{ a + km \mid k \in \mathbb{Z} \}$

- it contains a unique r s.t. $0 \leq r < m$ (r is the remainder of the division of a by m)

r = CANONICAL REPRESENTATIVE of $\bar{a}$

$\mathbb{Z}_m = \{ \bar{a} \mid \bar{a} \text{ congruence class. mod } m \}$

$|\mathbb{Z}_m| = m$

$\mathbb{Z}_m = \{ \bar{0}, \bar{1}, \dots, \overline{m-1} \}$

Addition

$\bar{a} + \bar{b} = \overline{a+b}$

$\bar{a}\,\bar{b} = \overline{ab}$

$(\mathbb{Z}_m, +, \cdot)$ is a commutative ring with unity.

$$\theta : \mathbb{Z} \longrightarrow \mathbb{Z}_m$$
$$a \longmapsto \bar{a}$$ is a ring homomorphism surjective

$$\ker(\theta) = \{ a \mid m \mid a \} = (m)$$

When $m \mid n$ there is a well defined map

$$F : \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$$
$$[a]_n \longmapsto [a]_m$$

well defined because

if $a \equiv a' \mod n$ then $a \equiv a' \mod m$.

is a ring homomorphism, surjective.

and $n = m m'$

$$\ker F = \{ [a]_n \mid m \mid a \}$$
$$= ([m]_n) \leftarrow \text{ideal in } \mathbb{Z}_n.$$

$\mathbb{Z}_m$ finite ring with unity $\bar{1}$

We can consider

$$\mathbb{Z}_m^{\times} = \{ \bar{a} \in \mathbb{Z}_m \mid \bar{a} \text{ invertible} \}$$
$$= \{ \bar{a} \in \mathbb{Z}_m \mid \exists \bar{b} \in \mathbb{Z}_m \ \ \bar{a}\bar{b} = \bar{1} \}$$

$$\bar{a}\bar{b} = \bar{1} \iff ab - 1 \in m\mathbb{Z}$$
$$\iff \exists c \in \mathbb{Z} \quad ab - 1 = mc$$

$$\iff \quad ab - mc = 1$$

$\bar{a} \in \mathbb{Z}_m^\times \iff$ the equation

$$ax + my = 1$$ admits a solution.

$$\iff \gcd(a, m) = 1$$

If $\gcd(a,m) = 1$ then Bézout allows to compute

$$a x_0 + m y_0 = 1$$

that is

$$a x_0 - 1 \in m\mathbb{Z}$$ that is

$$a x_0 \equiv 1 \mod m$$

$$\bar{a}\, \bar{x}_0 = \bar{1} \quad \text{in } \mathbb{Z}_m$$

<u>Exercise</u> $m = 841$

Find $\overline{160}^{-1}$ in $\mathbb{Z}_m$.

<u>Hint</u>:

160 is r.p. to 841

$$1 = 160\, x_0 + 841\, y_0$$

<u>Consequence</u>: if $m = p$ prime

then $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$

$\gcd(a, p) = 1 \iff p \nmid a$

$\mathbb{Z}_p^\times = \{\bar{1}, \dots, \overline{p-1}\}$

All nonzero elements in $\mathbb{Z}_p$ is invertible

$\rightsquigarrow$ $\mathbb{Z}_p$ is a field.

$\mathbb{F}_p$

$\rightsquigarrow$ finite fields of order p for each prime p.

Notice that if n is not prime then $\mathbb{Z}_n$ is not an integral domain ($\Rightarrow$ not a field) because $n = n_1 n_2$ $\quad 1 < n_1, n_2 < n$

then $[n_1]_n [n_2]_n = [0]$ $\qquad n \nmid n_1$, $n \nmid n_2$

but $[n_1]_n \neq [0]_n$

$[n_2]_n \neq [0]_n$.

If p prime then $|\mathbb{F}_p^\times| = p-1$

$\forall \bar{x} \in \mathbb{F}_p^\times \quad \bar{x}^{p-1} = \bar{1}$

$$x^{p-1} \equiv 1 \mod p \qquad \forall x \text{ s.t. } p \nmid x$$

$\hookrightarrow$ $\boxed{\text{FERMAT LITTLE THEOREM}}$