Lecture 3

Integer linear combinations

Let $a, b \in \mathbb{Z}$ are two integers.

Def. All linear combinations

$$a\mathbb{Z} + b\mathbb{Z}$$

define a set of integer linear combin.

T. The set of integer linear combinations of a and b is the set of all integer multiples of $\gcd(a,b)$, i.e

$$a\mathbb{Z} + b\mathbb{Z} = \gcd(a,b)\,\mathbb{Z}.$$

Proof. 1. For $\boxed{a = b = 0}$ is obviously correct.

2. a or b (or both) are nonzero.

Ex. $a = 3,\ b = 8 \Longrightarrow \gcd(3,8) = 1.$

$$3 \cdot (+3) + 8 \cdot (-1) = 1.$$

Set the set

$$I = a\mathbb{Z} + b\mathbb{Z}$$

Let g be the smallest positive integer in I (such number always exist).

We claim that $I = g\mathbb{Z}$.

Let choose a nonzero element $c \in I$.

We must show that $\boxed{c = gq}$ for some q.

There are q and r with

$$c = qg + r, \quad 0 \le r < g.$$

Therefore $r = c - qg$ belongs to I.

$(c, g \in I)$

g is the smallest positive integer in I and $r < g$, $\Rightarrow$ $r = 0$ and $\boxed{c = qg.}$

It remains ~~to~~ to show that

$$g = \gcd(a, b).$$

First, $a, b \in I$, then it follows from $I = g\mathbb{Z}$ that g is a common divisor of a and b.

Second, $g \in I$ there are $x, y \in \mathbb{Z}$ with:

$$g = xa + yb.$$

Thus if d is a common divisor of a and b, then d is also a divisor of $g \Rightarrow |d| \leq g$.

This shows that $g = \gcd(a, b)$.

T. For all $a, b, n \in \mathbb{Z}$ the equation

$$ax + by = n$$

is solvable in integers x and y iff $\gcd(a, b)$ divides n (i.e., $n = \gcd(a, b)\mathbb{Z}$).

Proof 1) If there are x and y with $n = ax + by$, then $n \in a\mathbb{Z} + b\mathbb{Z}$ and by T1 $n \in \gcd(a, b)\mathbb{Z}$.

Therefore $n = c \gcd(a, b) \Rightarrow n$ is a multiple of $\gcd(a, b)$.

2) If n is a multiple of $\gcd(a, b)$, then ~~$n \in \gcd\ n \in a$~~ n is an element of $\gcd(a, b)\mathbb{Z}$. By T1 we also have $n \in a\mathbb{Z} + b\mathbb{Z}$, therefore there are integers x and y such that

$$n = ax + by.$$

How to compute integers x and y with

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

We have an euclidean algorithm to compute $\gcd(a,b)$. In many cryptographic systems it is very important to compute $\gcd(a, b)$ and x, y solutions of $(*)$.

Extended Euclidean Algorithm

We solve equation

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

Two sequences are constructed

$$\{x_k\} \text{ and } \{y_k\}.$$

We had the sequences of remainders $\{r_1, r_2, \dots, r_{n+1}\}$ and of quotients $\{q_1, q_2, \dots, q_n\}$,

with $$\boxed{\gcd(a,b) = r_n, \quad r_{n+1} = 0.}$$

The required coefficients will be

$$x = (-1)^n x_n, \quad y = (-1)^{n+1} y_n.$$

We set

$$x_0 = 1, \quad x_1 = 0$$

$$y_0 = 0, \quad y_1 = 1$$

Then for $k \geq 1$:

$$x_{k+1} = q_k x_k + x_{k-1}$$

$$y_{k+1} = q_k y_k + y_{k-1}.$$

$$r_0 = a, \quad r_1 = b$$

$$r_{k-1} = q_k r_k + r_{k+1}$$

Euclidean algorithm. $k \geq 1$.

Example $a = 100$, $b = 35$

k	0	1	2	3	4
r_k	100	35	30	5	0
q_k		2	1	6	
x_k	1	0	1	1	7
y_k	0	1	2	3	20

$n = 3$

$x = (-1)^3 \cdot 1 = -1$

$y = (-1)^4 \cdot 3 = 3$

$5 = -1 \cdot 100 + 3 \cdot 35$

T. We have

$$r_k = (-1)^k x_k\, a + (-1)^{k+1} y_k\, b\,,$$

$$0 \le k \le n+1.$$

in particular

$$\underset{\gcd(a,b)}{\underset{\parallel}{r_n}} = \underbrace{(-1)^n x_n}_{x}\, a + \underbrace{(-1)^{n+1} y_{n+1}}_{y}\, b.$$

Proof. We use the method of mathemat induction.

We note first that

$$r_0 = a = 1\cdot a + 0\cdot b = a$$

$$r_1 = b = (-1)\cdot 0\cdot a + 1\cdot b = b.$$

Now let $k \ge 2$ and suppose that the assertion is true for all $k' < k$.

$$\left(\frac{r_{k-1} = q_k r_k + r_{k+1}}{\text{Euclid. algorithm}} \right)$$

$$r_k \overset{\text{def}}{=} r_{k-2} - q_{k-1} r_{k-1}$$

$$= (-1)^{k-2} x_{k-2} a + (-1)^{k-1} y_{k-2} b$$

$$- q_{k-1} \left((-1)^{k-1} x_{k-1} a + (-1)^{k} y_{k-1} b \right)$$

$$= (-1)^{k} a \left(x_{k-2} + q_{k-1} x_{k-1} \right) + (-1)^{k+1} b$$

$$\times \left(y_{k-2} + q_{k-1} y_{k-1} \right)$$

$$= (-1)^{k} x_k a + (-1)^{k+1} y_k b .$$