Lecture 3 : Divisors and Primes.

In the previous lecture we proved

Thm (The division algorithm)

$\forall a \in \mathbb{Z}$, $b \in \mathbb{Z}^{>0}$ $\exists!$ $q, r \in \mathbb{Z}$ s.t.

(1) $a = bq + r$,

(2) $0 \leq r < b$.

We wanted to study subgroups of $\mathbb{Z}$, i.e.

$X \subseteq \mathbb{Z}$ s.t. (1) $0 \in X$.

(2) $x \in X \Rightarrow -x \in X$.

(3) $x, y \in X \Rightarrow x + y \in X$.

Exp. For any $n \in \mathbb{Z}$,

$$n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$$

the set of multiples of n is a subgroup.

Recall. Let $a, b \in \mathbb{Z}$. If $a = bk$ for some integer k, then we say

- b divides a;
- b is a divisor of a;
- a is a multiple of b;

And we write $b \mid a$.

Basic properties

① $a \mid b \wedge b \mid c \Rightarrow a \mid c$

② $a \mid b_1 \wedge a \mid b_2 \Rightarrow a \mid b_1 x + b_2 y$ for any integers x and y.

③ $a \mid b$ and $b \neq 0 \Rightarrow |a| \leq |b|$.

④ $1 \mid a$ for any a; $a \mid 0$ for any a.

①′ $a \mid b \Leftrightarrow b\mathbb{Z} \subseteq a\mathbb{Z}$

②′ $b_1\mathbb{Z} \subseteq a\mathbb{Z} \wedge b_2\mathbb{Z} \subseteq a\mathbb{Z} \Rightarrow$

$$b_1\mathbb{Z} + b_2\mathbb{Z} \subseteq a\mathbb{Z}.$$

$$:= \{b_1 x + b_2 y \mid x, y \in \mathbb{Z}\}.$$

Thm Let X be a subgroup of $\mathbb{Z}$. Then either $X = \{0\}$ or $X = n\mathbb{Z}$ where n is the smallest positive element of X.

Pf Suppose $X \neq \{0\}$. So $\exists\, x \in X$ which is NOT zero. Hence either $x \in X \cap \mathbb{Z}^{>0}$ or $-x \in X \cap \mathbb{Z}^{>0}$. Therefore

$X \cap \mathbb{Z}^{>0} \neq \emptyset$. So by the well-ordering principle $X \cap \mathbb{Z}^{>0}$ has a smallest element $\underline{n}$.

Since $n \in X$, by a lemma we have $n\mathbb{Z} \subseteq X$.

Now for any $x \in X$, by the division algorithm

$\exists\, q, r \in \mathbb{Z}$ s.t. $x = nq + r$ and

$$0 \leq r < n.$$

Since $nq, x \in X \Rightarrow r = x - nq \in X$

$r < n$

n : smallest in $X \cap \mathbb{Z}^{>0}$

$\Rightarrow r \leq 0$

$r = 0$

$x \in n\mathbb{Z}$

$\Leftarrow \begin{cases} X \subseteq n\mathbb{Z} \\ n\mathbb{Z} \subseteq X \end{cases}$

$\therefore X = n\mathbb{Z}$ ■

Def. $\forall\, a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$, we call $\underline{d}$ the greatest common divisor of a and b if

① $d \mid a$ and $d \mid b$.

② $d' \mid a$ and $d' \mid b \Rightarrow d' \leq d$.

we denote it by $\underline{\gcd(a,b)}$.

Thm $\forall a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\}$ we have

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

In particular, $\exists\, x, y \in \mathbb{Z}$ s.t.

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

Cor. $ax + by = c$ has integer solutions $\iff \gcd(a,b) \mid c$.

Pf of thm.

$a\mathbb{Z} + b\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ which is NOT zero. Therefore

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

where n is the smallest positive element of $a\mathbb{Z} + b\mathbb{Z}$. In particular,

$$\left.\begin{array}{l} a\mathbb{Z} \subseteq n\mathbb{Z} \implies n \mid a \\ b\mathbb{Z} \subseteq n\mathbb{Z} \implies n \mid b \end{array}\right\} \implies n \leq \gcd(a,b) =: d$$

On the other hand,

$$\left.\begin{array}{l} d \mid a \implies a\mathbb{Z} \subseteq d\mathbb{Z} \\ d \mid b \implies b\mathbb{Z} \subseteq d\mathbb{Z} \end{array}\right\} \implies a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}$$

$$\implies n\mathbb{Z} \subseteq d\mathbb{Z}$$

$$\implies d \mid n$$

$\Rightarrow d = |d| \le |n| = n$

$\Rightarrow \underline{d = n}$. ∎

Corollary $a \mid bc$ and $\gcd(a,b) = 1 \Rightarrow a \mid c$.

Pf. $\gcd(a,b) = 1 \Rightarrow \exists x, y \in \mathbb{Z}$,

$$ax + by = 1$$

$$\Rightarrow \left.\begin{array}{l} acx + bcy = c \\ a \mid a \wedge a \mid bc \end{array}\right\} \Rightarrow a \mid c.$$ ∎

Def. $p > 1$ is called a prime number if its only divisors are ± 1 and $\pm p$.

Cor. Let p be a prime number. Then

$$p \mid ab \Rightarrow p \mid a \text{ or } p \mid b.$$

Pf. Suppose $p \mid ab$ and $p \nmid a$. So $\gcd(p,a) \neq p$ it is a positive divisor of p. Thus $\gcd(p,a) = 1$.

$$\left.\begin{array}{l} p \mid ab \\ \gcd(p,a) = 1 \end{array}\right\} \Rightarrow p \mid b.$$ ∎

Cor. Let p be a prime number. Then

$$p \mid a_1 \cdot \cdots \cdot a_n \Rightarrow p \mid a_1 \text{ or } p \mid a_2 \text{ or } \cdots \text{ or } p \mid a_n.$$