Chapter 1 Defs & Thms

AXIOM ① Well-ordering axiom.

$\forall S \subseteq \mathbb{Z}_{\geq 0}$ contains a smallest elem

Def ① divisor (factor)

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

if $\exists q \in \mathbb{Z}$ s.t. $b = aq$.

Say: $a | b$, a is a divisor (factor) of b

Thm ① 1.1 Division Algo Thm.

Let $n, d \in \mathbb{Z}$, $d > 0$

$\Rightarrow \exists$ unique $q, r \in \mathbb{Z}$, $0 \leq r < d$ s.t. $n = qd + r$

Def ② GCD

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

if $d \in \mathbb{Z}$ s.t. $\begin{cases} d | a \\ d | b \\ \text{if } c|a, c|b \Rightarrow c \leq d \end{cases}$

Say $d = (a, b)$, the GCD of a, b

Thm ② 1.2

Let $a, b \in \mathbb{Z}$, not both 0.

$\Rightarrow \exists r, s \in \mathbb{Z}$ s.t. $ra + sb = (a, b)$

Thm ③ 1.4

If $\begin{cases} a | bc \\ (a, b) = 1 \end{cases} \Rightarrow a | c$

Thm ④ Euclidean Algorithm.

$(a, b) = (b, a \bmod b)$

Def ③ prime, composite

$p \in \mathbb{Z}$ $(p \neq 0, \pm 1)$

is $\begin{cases} \text{prime if only divisors is } \pm 1, \pm p \\ \text{composite if not prime } (\exists c | p \text{ s.t. } c \neq \pm 1, \pm p) \end{cases}$

Thm ⑤ 1.5

$a \in \mathbb{Z}$ $(\neq 0, \pm 1)$ is prime iff whenever $p | bc \Rightarrow p | b$ or $p | c$

Collary ① 1.6

if $p \in \mathbb{Z}$ is prime AND $p | (a_1 \ldots a_n)$ $(\forall a_i \in \mathbb{Z})$

$\Rightarrow$ 至少一个a_i使得 $p | a_i$

Thm ⑥ FTA

$\forall n \in \mathbb{Z}$ $(\neq 0, \pm 1)$ can be factorized into primes.

And by reordering, neglecting $\pm$, it is unique

(i.e. if $n = p_1 \ldots p_s = q_1 \ldots q_t$ $\Rightarrow s = t$, $\forall i$ $p_i = \pm q_i$)