Worksheet 3

Pf of Thm ①

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

Pf Step (1) Show: p is prime $\Rightarrow$ $(p|bc \Rightarrow p|b$ or $p|c)$

Let $bc = kp$, $k \in \mathbb{Z}$

Consider (p, b)

Since p is prime, (p, b) can only be 1 or $\pm p$ ($\pm p$ 中 positive 的那一个)

Case ①: $(p,b) = 1 \Rightarrow p|c$ by (MLS 3 Thm ③)

Case ②: $(p,b) = p \Rightarrow p|b$ by def

□

Step (2) Show: $(p|bc \Rightarrow p|b$ or $p|c) \Rightarrow p$ is prime

Prove it by contrapositive:

if p is not a prime, then $\exists\, b, c \in \mathbb{Z}$ s.t. $p|bc$ 但 $p \nmid b$ and $p \nmid c$.

Assume p is not a prime.

$\Rightarrow$ By def, $k|p$ for some $k \in \mathbb{Z}$ with $k \neq \pm 1, \pm p$.

这一段实际很好想: p is composite, 要找一个数 bc 使 $p|bc$ 但 $p \nmid b$, $p \nmid c$, 可以想到它自身数一个这样的数, 因为 $p|p$, 而它不可能整除自己的 factor.

$\Rightarrow$ Say $p = kd$, $d \in \mathbb{Z}$

$\Rightarrow p|kd$

but since we know $p = kd$, $|p| > |k|$, $|p| > |d|$

therefor $p \nmid k$ and $p \nmid d$.

□

E. Pf of Corollary ①

if $p \in \mathbb{Z}$ is prime and $p|(a_1 \cdots a_n)$, $a_i \in \mathbb{Z}$ $\Rightarrow p|a_i$ for some i

Pf (思路实际很简单: 把 $(a_1 \cdots a_{n-1})$ 和 a_n 看作 b, c 用 Thm ① 可得 p_i 或 a_n divide 其中一个; 而后递归可得. 证明过简单略.)

C. Pf of Thm ② (FTA)

Part I. Existence.

Consider the set $S = \{s > 1 \mid s \in \mathbb{Z}, s$ is not product of primes$\}$

Show that S is empty.

(4) **Step 1: Every elem of S is composite**

Pf. 一个数: either prime or composite

$\forall$ prime p cannot be in S, since $p = p$ (单因子 trivial factorization)

$\Rightarrow$ (if $S \neq \emptyset$,) every elem of S is composite

(5) **Step 2: let $a, b > 1 \in \mathbb{Z}$ if $ab \in S \Rightarrow a$ or $b \in S$**

Pf. We prove the contrapositive:

if $a \notin S$ and $b \notin S \Rightarrow ab \notin S$

Let $a, b > 1 \in \mathbb{Z}$ with $a, b \notin S$

$\Rightarrow a, b$ admit prime factorization

$\Rightarrow a = p_1 \cdots p_s$ and $b = q_1 \cdots q_t$ for some primes $p_1 \cdots p_s, q_1 \cdots q_t$

$\Rightarrow ab = p_1 \cdots p_s q_1 \cdots q_t$

$\Rightarrow ab \notin S$

(6) **Step 3: S is empty**

Pf We proceed by contradiction.

If S is nonempty $\Rightarrow S$ has a minimal elem s by well-ordering axiom.

By (4) $\Rightarrow S$ is composite

$\Rightarrow$ can write $s = ab$ for some $a, b > 1$

$\Rightarrow$ By (5), either a or $b \in S$ and since $s = ab$ ($a, b > 1$) $\Rightarrow a, b < s$

$\Rightarrow$ then the elem a or b in S is smaller than $s \Rightarrow$ contradicts.

□ $\Rightarrow S$ is empty.

D. Pf of Thm ② FTA

Part II. Uniqueness

(1) Suppose $p_1 \cdots p_s$ and $q_1 \cdots q_t$ are two different factorizations of an int. n into primes. Show: p_1 must divide one of q_i

Pf $n = p_1 \cdots p_s = q_1 \cdots q_t$

So $p_1 \mid n$, IOW, $p_1 \mid (q_1 \cdots q_t)$

By Corollary ①, p_1 must divide one of q_i, $1 \le i \le t$

Since q_i is prime, by def, the only factor of q_i is $\pm 1, \pm q_i$

Hence $p_1 = \pm 1$ or $\pm q_i$

Since p_1 is prime $\Rightarrow p_1 \neq \pm 1 \Rightarrow p_1 = \pm q_i$

(2) Eliminate p_i, q_i from both sides

$\Rightarrow p_2 \cdots p_s = q_1 \cdots q_{i-1} \cdot q_{i+1} \cdots q_t$

Assume for sake of contradiction: $s \neq t$

WLOG suppose $s \le t$

Perform the same same elimination to $p_2 \cdots p_s \Rightarrow 1 = q_{s+1} \cdots q_t$

Since $\forall q_i$ is prime, this is impossible

$\Rightarrow$ contradicts, $s = t$

And by elimination we have associated all s pairs of p_i, q_i, which means that by reordering we can get $\forall i\ p_i = q_i$

□

F. GCD Exercise

(1) The common divisors of a, b

$$S = \{\pm p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n} \mid 0 \le c_i \le \min\{a_i, b_i\}, 1 \le i \le n\}$$

$\Rightarrow$ all elements of S

(2) write (a,b) in terms of $p_1, \cdots, p_n$, $a_1, \cdots, a_n$, $b_1, \cdots, b_n$.

$$(a,b) = p_1^{\min\{a_1,b_1\}} p_2^{\min\{a_2,b_2\}} \cdots p_n^{\min\{a_n,b_n\}}$$

$$= \prod_{i=1}^{n} p_i^{\min\{a_i,b_i\}}$$

(3) Let d be a common divisor of a, b

By (1), $d = \pm p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n}$, where $\forall c_i$, $0 \le c_i \le \min\{a_i, b_i\}$

Since $\forall\ c_i$, $p_i^{c_i} \mid p_i^{\min\{a_i,b_i\}}$

$\Rightarrow d = \pm p_1^{c_1} \cdots p_n^{c_n} \mid p_1^{\min\{a_1,b_1\}} \cdots p_n^{\min\{a_n,b_n\}}$