NIS2312-1 2022-2023 Fall

信息安全的数学基础 (1)

Assignment 1

2022 年 9 月 14 日

Problem 1

证明: 设 a, b 是两个不全为零的整数, 令 $S = \{xa + yb > 0 \mid x, y \in \mathbb{Z}\}$, 则 $(a, b) = \min S$.

解：设 $d = \min S$, 则 $d \mid a, d \mid b$: 假设 $d \nmid a$, 则 $a = qd + r$, 其中 $q \geq 0, 0 < r < d$. 因此有 $qd = q(ax + by) = a - r$, 即 $r = (1 - qx)a - qyb$. 注意到 $1 - qx, -qy$ 均为整数, 因此确定 $r \in S$, 但 $r < d$, 与 $d = \min S$ 矛盾, 所以 $d \mid a$. 同样的方法可以证明 $d \mid b$. 因此 $d = \min S$ 是 a, b 的公因子.

下证 a, b 的任意公因子均整除 d: 假设 $a = cu, b = cv$, 那么 $d = ax + by = c(au + bv)$, 即 $c \mid d$. Q.E.D.

Problem 2

证明: 若 a, b, c 是三个整数, 则:

(1) 若 $(a, c) = 1$ 且 $(b, c) = 1$, 则 $(ab, c) = 1$;

(2) 若 $(a, c) = 1$ 且 $c \mid ab$, 则 $c \mid b$;

(3) 若 c 为素数且 $c \mid ab$, 则 $c \mid a$ 或者 $c \mid b$.

解:

(1) $(a, c) = 1 \Rightarrow \exists m, n \in \mathbb{Z}$, s.t. $ma + nc = 1$, 同理得到 $m'b + n'c = 1$. 因此 $(ma + nc)(m'b + n'c) = 1$, 整理得到 $mm'ab + (man' + m'bn + ncn')c = 1$, 再根据第一题, 可确定 $(ab, c) = 1$.

(2) 因为 $c \mid ab$, 故 $ab = xc$, 那么由 $(a, c) = 1$ 可知 $\exists m, n \in \mathbb{Z}$ s.t. $ma + nc = 1 \Rightarrow mab + ncb = b \Rightarrow mxc + ncb = b$, 即 $c(mx + nb) = b$, Q.E.D.

(3) 反证: 假设 c 为素数且 $c \mid ab$, 则 $c \nmid a$ 且 $c \nmid b$, 因此 $(a, c) = 1, (b, c) = 1$, 同时根据第二题第一小题, 可知 $(ab, c) = 1$, 与 $c \mid ab$ 矛盾. Q.E.D.

Problem 3

设 a, b 是任意两个正整数, 证明:

(1) a, b 的所有公倍数就是 $[a, b]$ 的所有倍数;

(2) $[a, b] = \frac{ab}{(a,b)}$.

解:

(1) 设 m 为 a, b 的公倍数, 则 $a \mid m, b \mid m$. 反证: 假设 m 不是 $[a, b]$ 的公倍数, 则有 $m = q[a, b] + r$, 其中 $q \geq 0, 0 < r < [a, b]$, 注意到 $a \mid m, a \mid [a, b]$, 则 $a \mid r$, 同理 $b \mid r$, 故 r 也是 a, b 的公倍数, 与 $[a, b]$ 是最小公倍数矛盾. Q.E.D.

(2) 设 $d = (a, b)$, 则 $a = md, b = nd$ 且 $(n, m) = 1$. 显然 mnd 是 a, b 的公倍数, 下面证明 $mnd = [a, b]$: 设 c 是 a, b 的公倍数, 则有 $c = ka = kmd$, 同时 $b = nd \mid c = kmd$, 得到 $n \mid km$, 利用第二题第二小问可确定 $n \mid k$, 因此 $mnd \mid c$, 故 $[a, b](a, b) = ab$. Q.E.D.