

自学部分

Pf of Thm ②

Pf Let $S = \{am + bn \mid m, n \in \mathbb{Z}\}$
(i.e. S is a, b 的所有 linear combination)

W.T.S. (want to show):

$t = (a, b)$ $\begin{cases} \textcircled{1} \exists t \in S \text{ s.t. } t \mid a, t \mid b \\ \textcircled{2} \forall c \text{ s.t. } c \mid a, c \mid b, \\ \Rightarrow c \leq t \end{cases}$

Step (1) : Show $\textcircled{1}$

(1.1) Let t be the smallest positive elem of S . (神奇, 这里直接过一个灵感来想到 (a, b) 是 S 的 smallest positive elem, 这怎么想得到)

By well-ordering axiom, $t \exists$.

那么 $t = ua + vb$ for some $u, v \in \mathbb{Z}$.

(1.2) (又一个想不到的, 但是仔细想, 在现有工具上
这样做合理)
By division algo,

$$\underline{a = tq + r \text{ for some } q, r \in \mathbb{Z}} \\ \text{and } \underline{0 \leq r < t}$$

$$\Rightarrow r = a - tq = a - (ua - vb)q \\ = a(1 - uq) + b(vq) \\ \text{is also a linear comb of } a, b$$

$$\Rightarrow r \in S$$

Since $0 \leq r < t$ but t is the
smallest positive elem in S

$$\Rightarrow \boxed{r \text{ can only be } 0}$$

$$\Rightarrow a = tq \Rightarrow \boxed{t|a} \\ \text{Similarly } \boxed{t|b}$$

Step(2): show (2)

$$\text{let } c|a, c|b \Rightarrow a = ck, b = cs \\ \text{for some } k, s \in \mathbb{Z}$$

$$\Rightarrow t = ua + vb = uck + vcs = c(uk + vs)$$

$$\Rightarrow c \mid t$$

$$\Rightarrow c \leq |t| \Rightarrow c \leq t$$

pf of Thm ③

pf Since $(a, b) = 1$,

By Thm ②, $\exists u, v \in \mathbb{Z}$ s.t.
 $au + bv = 1$

$$\Rightarrow auc + bvc = c$$

Since $a \mid bc \Rightarrow bc = ka$ for
some $k \in \mathbb{Z}$

$$\Rightarrow auc + akv = c$$

$$a(cu + kv) = c$$

$$\Rightarrow a \mid c$$

这个东西的意思是：

如果 a 是 bc 的因子，但 a 和 b 互质，那 a
肯定就是 c 的因子（直观可见）

Pf of Collary 1-3

Pf Step 1

Pf: If $d = (a, b) \Rightarrow$

- (i) $d|a, d|b$
- (ii) if $c|a, c|b \Rightarrow c|d$

(i) by def 可证

(ii) Let $a = cr, b = cs$ for some $r, s \in \mathbb{Z}$

By Thm (2) $\Rightarrow d = ua + vb$
for some $u, v \in \mathbb{R}$

$$\Rightarrow d = ucr + vcs = c(ur + vs)$$

$$\Rightarrow c|d$$

Step 2

Pf: If $\begin{cases} (i) d|a, d|b \\ (ii) \text{ if } c|a, c|b \Rightarrow c|d \end{cases}$
 $\Rightarrow d = (a, b)$

($c|d \Rightarrow c \leq |d| \Rightarrow c \leq d$, 易证, 用 gcd 定义)

Worksheet 部分

B: Pf of Thm ⑤: Euclidean Algorithm
 $(a, b) = (b, a \bmod b)$

这部分为 Worksheet 多出的 Euclidean Algorithm 部分：
书上只证明了 (a, b) 是能写成 a 和 b 的 linear combination 的，但没有说具体的找出这个 linear comb 的具体方法，不是很直观

Worksheet 则介绍了 Euclidean Algorithm (辗转相除)

这种方法则证明，当我们知道 $(a, b) = (b, a \bmod b)$ 时，最后会到某对 u, v 使 $u \bmod v = 0$

那么下一步 $v \bmod 0 = v$, $(v, 0) = v$, 这个 v 就是一路下来的 (a, b) 了, (其实半路就可以看出来)

而 u, v 上面每一个 $c = dq + r$ 中 c, q, r 都可以

最终向前递归表示为 a, b , 最后就会得出 linear comb

因为 Euclidean Algo \Rightarrow Thm ②
(Thm ⑤)

现有 $a, b \in \mathbb{Z}$ 以及 let $d = (a, b)$

By division algo, $a = bq + r$ for some $q, r \in \mathbb{Z}$

(1) Show: if $d|b$ AND $d|r$ (这个很直观)
 $\Rightarrow d|a$ (即 d 为 a, b 的 common divider)

Let d be a common divider of b, r

$$\Rightarrow \exists k_1, k_2 \in \mathbb{Z} \text{ s.t. } b = dk_1, r = dk_2$$

$$\Rightarrow a = bq + r = d(k_1q + k_2) \Rightarrow d|a$$

而我们可以 conclude: $(b, r) \leq (a, b)$

因为 (b, r) 一定也是 a 和 b 的 common factor

(2) Show: if $d|a, d|b$

$\Rightarrow d|r$ (即 d 如果是 a, b 的 common divider, 那么也是 r 的 common divider)

(和 (1) similar:)

Let d be a common divider of a, b

$$\Rightarrow \exists k_1, k_2 \in \mathbb{Z} \text{ s.t. } b = dk_1, a = dk_2 \dots$$

易证 \Rightarrow 和 (1) 一样, 得出 $(b, r) \geq (a, b)$

(3) Show: $(b, r) = (a, b)$

Let $d = (a, b) \Rightarrow d|a, d|b \Rightarrow$ By (2), $d|r$

$$\Rightarrow (b, r) \geq (a, b)$$

$$\text{又 } d|r, d|b \Rightarrow (b, r) \leq (a, b) \text{ by (1)}$$

$$\Rightarrow (b, r) = (a, b)$$

$C, D : \text{ex } 1$

$$(524, 148) = 4$$

$$524 = 148 \times 3 + 80$$

$$148 = 80 \times 1 + 68$$

$$80 = 68 \times 1 + 12$$

$$68 = 12 \times 5 + 8$$

$$\underline{12 = 8 \times 1 + 4} \rightarrow \text{result}$$

$$8 = 4 \times 2 + 0$$

$$\Rightarrow 4 = 12 - 8 \times 1$$

$$= 12 - (68 - 12 \times 5) \times 1 = -68 + 6 \times 12$$

$$= -(148 - 80 \times 1) + 6 \times (80 - 68 \times 1) = -148 + 7 \times 80 - 6 \times 68$$

$$= -148 + 7 \times (524 - 3 \times 148) - 6 \times (148 - 80)$$

$$= -28 \cdot 148 + 7 \cdot 524 + 6 \cdot (524 - 3 \cdot 148) = -28 \cdot 148 + 7 \cdot 524 + 6 \cdot 80$$

$$= 13 \cdot 524 - 46 \cdot 148$$

E: Ex2

$$\underline{(1003, 456) = 1}$$

$$1003 = 456 \times 2 + 91 \quad (\Rightarrow (1003, 456) = (456, 91))$$

recursion

$$456 = 91 \times 5 + \boxed{1} \quad (\Rightarrow (456, 91) = (91, 1))$$
$$91 = \boxed{1} \times 91 + 0 \quad (\Rightarrow (91, 1) = (1, 0) = 1)$$

~ 最后结果 (mod 为 0 时的 b)

整个过程:

$$1 = 456 - 91 \times 5$$

$$= 456 - (1003 - 2 \times 456) \times 5$$

$$\Rightarrow = \underline{-5 \times 1003 + 11 \times 456}$$