

## 1.3.7 gcd的线性组合

---

□ 如何找出两个整数的线性组合以使之等于其最大公约数呢？

➤ **方法1**: 使用欧几里得算法做反向处理, 获得线性组合的 $s$ 和 $t$ 值. 该方法因此需要将欧几里得算法的步骤正反各走一遍.

## 1.3.7 gcd的线性组合

□例: 把 $\gcd(252, 198) = 18$ 表示为252, 198的线性组合

□解: 首先用欧几里得算法可得 $\gcd(252, 198) = 18$

➤  $252 = 1 \cdot 198 + 54$

➤  $198 = 3 \cdot 54 + 36$

➤  $54 = 1 \cdot 36 + 18$

➤  $36 = 2 \cdot 18$

根据倒数第二行, 可以得到 $18 = 54 - 1 \cdot 36$ , 这其中36又可以由倒数第三行得到 $36 = 198 - 3 \cdot 54$ . 代入就可以得到 $18 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$ , 这其中54又可以由第一行得到 $54 = 252 - 1 \cdot 198$ . 代入就可以得到 $18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198$ , 从而得解.

## 1.3.7 gcd的线性组合

□ 如何找出两个整数的线性组合以使之等于其最大公约数呢？

➤ 方法1: 使用欧几里得算法做反向处理, 获得线性组合的s和t值. 该方法因此需要将欧几里得算法的步骤正反各走一遍.

➤ 方法2(扩展欧几里得算法): 设置 $s_0=1, s_1=0, t_0=0, t_1=1$ . 然后令

$$s_j = s_{j-2} - q_{j-1}s_{j-1}$$

$$t_j = t_{j-2} - q_{j-1}t_{j-1}$$

其中 $j = 2, 3, \dots, n$ .  $q_j$ 表示欧几里得算法中做除法时的商. 最终求得 $s_n$ 和 $t_n$ . 因此 $\gcd(a, b) = s_na + t_nb$ . 该方法只需要经历一遍欧几里得算法的步骤.

除数	被除数	商	余数	
$r_0$	$= r_1$	$q_1$	$+ r_2$	$0 \leq r_2 < r_1,$
$r_1$	$= r_2$	$q_2$	$+ r_3$	$0 \leq r_3 < r_2,$
$\vdots$				
$r_{n-2}$	$= r_{n-1}$	$q_{n-1}$	$+ r_n$	$0 \leq r_n < r_{n-1},$
$r_{n-1}$	$= r_n$	$q_n$		

## 1.3.7 gcd的线性组合

□例: 使用扩展欧几里得算法, 把 $\gcd(252, 198) = 18$ 表示为252, 198的线性组合

□解: 首先用欧几里得算法可得 $\gcd(252, 198) = 18$

➤  $252 = 1 \cdot 198 + 54$

➤  $198 = 3 \cdot 54 + 36$

➤  $54 = 1 \cdot 36 + 18$

➤  $36 = 2 \cdot 18$

其中 $q_1=1, q_2=3, q_3=1, q_4=2$ .  $s_0=1, s_1=0, t_0=0, t_1=1$ . 那么根据 $s_j = s_{j-2} - q_{j-1}s_{j-1}$ 和 $t_j = t_{j-2} - q_{j-1}t_{j-1}$ 分别计算

$$s_2 = 1 - 1 \cdot 0 = 1,$$

$$t_2 = 0 - 1 \cdot 1 = -1$$

$$s_3 = 0 - 3 \cdot 1 = -3,$$

$$t_3 = 1 - 3 \cdot (-1) = 4$$

$$s_4 = 1 - 1 \cdot (-3) = 4,$$

$$t_4 = -1 - 1 \cdot 4 = -5$$

因此 $\gcd(252, 198) = 4 \cdot 252 - 5 \cdot 198$

## 1.3.7 gcd的线性组合

□引理2: 如果 $a, b, c$ 为正整数, 使得 $\gcd(a, b) = 1$ , 且 $a|bc$ , 则有 $a|c$ .

□证明:

- 由于 $\gcd(a, b) = 1$ , 根据贝祖定理知有整数 $s$ 和 $t$ , 使得 $sa + tb = 1$ .
- 在等式两边乘以 $c$ , 可得 $sac + tbc = c$ .
- 根据定理1(如果 $a|b$ , 则对所有的整数 $c$ 有 $a|bc$ ), 已有 $a|bc$ , 则 $a|tbc$ 成立.
- 因为 $a|sac$ (这是 $sac$ 除以 $a$ 一定没有余数),  $a|tbc$ , 由定理1[如果 $a|b, a|c$ , 则有 $a|(b + c)$ ], 则有 $a|(sac + tbc)$ .
- 因为 $sac + tbc = c$ , 所以可得 $a|c$ , 得证.

## 1.3.7 gcd的线性组合

□引理3: 如果 $p$ 是素数, 且 $p|a_1a_2\cdots a_n$ , 那么对于某个 $i$ ,  $p|a_i$ 成立.

□备注: 证明此处省略, 提示可以数学归纳法.

□定理 7: 令 $m$ 为正整数,  $a, b, c$ 为整数. 如果 $ac \equiv bc \pmod{m}$ ,  $\gcd(c, m) = 1$ , 则 $a \equiv b \pmod{m}$ .

□证明:

➤ 因为 $ac \equiv bc \pmod{m}$ , 则有 $m|ac - bc$  整理为 $m|c(a - b)$ .

➤ 根据引理2( $\gcd(a, b) = 1$ , 且 $a|bc$ , 则有 $a|c$ ), 因为 $\gcd(c, m) = 1$ , 所以  $m|a - b$ .

➤ 从而,  $a \equiv b \pmod{m}$ .

## 1.3.7 gcd的线性组合

---

□定理:整数 $a$ 和 $b$ 互素的充分必要条件是存在整数 $x$ 和 $y$ 使得 $xa + yb = 1$

□证明略.

【基础知识:如果 $a|b$ ,且 $b$ 不为0, 那么 $|a| \leq |b|$ 】

## 1.3.7 gcd的线性组合

---

□例: 如果 $a|c$ ,  $b|c$ , 且 $a$ 和 $b$ 互素, 那么证明 $ab|c$

□证:

- 根据上一个定理,  $a$ 和 $b$ 互素, 那么存在整数 $x$ 和 $y$ 使得 $xa + yb = 1$ .
- 在等式两边同乘以 $c$ , 得到 $cxa + cyb = c$ .
- 又由 $a|xa$ (根据整除的定义可得该结果),  $b|c$ , 那么 $ab|cxa$ .
  - 这是因为 $a|xa$ , 那么 $xa=xa$ .  $b|c$ , 那么 $c = bt$ , 其中 $t$ 为整数. 因此 $cxa = xt * ab$ . 即 $ab|cxa$ .
- 类似地,  $a|c$ ,  $b|yb$ , 那么 $ab|cyb$ .
- 于是 $ab|cxa + cyb$ .
- 由于 $xa + yb = 1$ , 所以 $ab|c$ , 得证.



## 第1.3节 素数和最大公约数小结

---

- 素数, 大于1且恰只有1和它自身两个正因子的整数
- 合数, 大于1又不是素数的整数
- 最大公约数 $\gcd(a,b)$ , 能整除 $a$ 和 $b$ 的最大整数
- 互素, 满足 $\gcd(a,b) = 1$ 的整数 $a$ 和 $b$
- 最小公倍数 $\text{lcm}(a,b)$ , 能被 $a$ 和 $b$ 整除的最小正整数
- 欧几里得算法求最大公约数
- 贝祖系数,  $sa + tb = \gcd(a,b)$ 成立的整数 $s$ 和 $t$ , 欧几里得算法反向处理获得, 或者扩展欧几里得算法.