欧几里得算法与裴蜀等式

Euclidean Algorithm and Bezout's Equation

刘铎

liuduo@bjtu.edu.cn

欧几里得算法与裴蜀等式

- 当不知道整数 a 和 b 的因子分解时，也可以计算 a 和 b 的最大公因子
- 欧几里得（Euclid）在《几何原本》中提出了计算最大公因子的算法，这被公认是最早的算法，也是人类历史上最美丽的算法之一。

欧几里得算法与裴蜀等式

- 在表述该算法之前，先给出下述定理，奠定算法的理论基础：
- 定理

  设 $a=qb+r$，其中 a, b, q, r 都是整数，则

  $$\mathrm{GCD}(a, b) = \mathrm{GCD}(b, r)$$

- 证明
  - 若 $d \mid a$ 且 $d \mid b$，则有 $d \mid b$ 且 $d \mid r = (a-qb)$
  - 若 $d \mid b$ 且 $d \mid r$，则有 $d \mid (qb+r)$，即 $d \mid a$
  - 于是，a 与 b 的公因子集合和 b 与 r 的公因子集合相同。继而，最大公因子相同

欧几里得算法与裴蜀等式

- 欧几里得算法（辗转相除法） GCD (a, b)
- 输入：整数 a, b，满足 $a \geq b \geq 0$，且 a, b 不全为0
- 输出：GCD(a, b)

Step1　If $b = 0$ then return a

Step2　Else return GCD(b, a mod b)

其中，若 $a=q \cdot b + r$ 且 $0 \leq r < b$

则定义 $a \bmod b = r$

欧几里得算法与裴蜀等式

- 例
  - 计算 **GCD(210, 715)**

	210	715	715=3×210+85
210=2×85+40	210	85	
	40	85	85=2×40+5
40=8×5+0	40	5	
	0	5	

GCD(715, 210)=5

欧几里得算法与裴蜀等式

	210	715	$715=3\times210+85$
$210=2\times85+40$	210	85	
	40	85	$85=2\times40+5$
$40=8\times5+0$	40	5	
	0	5	

$$5 = 85-2\times40 \qquad = 85-2\times(210-2\times85)$$

$$= 5\times85-2\times210 \qquad = 5\times(715-3\times210)-2\times210$$

$$= 5\times715-17\times210$$

欧几里得算法与裴蜀等式

- 对于不全为0的整数 a, b 和 d，方程 $sa+tb=d$ 存在整数解 s 和 t 当且仅当 $\mathrm{GCD}(a, b)|d$ 。
- 方程 $sa+tb=d$ 称作**裴蜀（Bezout）等式**或**贝祖等式**。
- 证明.
  - （充分性）通过回代法，可知 $sa+tb=\mathrm{GCD}(a, b)$ 存在整数解，设其为 s_0、t_0
  - 若 $d=k\cdot\mathrm{GCD}(a, b)$，则$k\cdot s_0$，$k\cdot t_0$是方程的一个解。
  - （必要性）若方程 $sa+tb=d$ 存在整数解 s 和 t 则 $\mathrm{GCD}(a, b) \mid (sa+tb)=d$

欧几里得算法与裴蜀等式

- 例
  - $15s+21t = 3$
    - $15\cdot(-4)+21\cdot 3 = 3$
  - $22s+34t = 9$
    - 无整数解
  - $21s+28t = 14$
    - $21\cdot(-2)+28\cdot 2 = 14$

欧几里得算法与裴蜀等式

- 练习
  - 使用欧几里得算法计算 GCD(2009, 1394)
  - 计算 s, t 使得 $2009s+1394t$ = GCD(2009, 1394) 成立
  - 计算LCM(2009, 1394)

End