



算法笔记

algorithm note

作者: LHesperus

组织: UESTC

时间: 2019.09.29-September 30, 2019

版本: 1.00



目 录

1 数论算法	1
1.1 最大公约数	1
1.2 扩展欧几里得算法	1
1.3 求解模线性方程	2
1.4 快速幂	3

第 1 章 数论算法

1.1 最大公约数

两个不同时为 0 的数 a 与 b 的最大公因数是同时整除它们的两个最大的数，记为 $\gcd(a, b)$ ，同时，如果 $\gcd(a, b) = 1$ ，我们称它们互素。

$O(\log(N))$ 欧几里得算法/辗转相除法： $\gcd(m, n) = \gcd(n, m \bmod n)$

递归不会栈溢出： \gcd 函数的递归层数不会超过 $4.785 \lg N + 1.6723$, $N = \max(a, b)$ ，让 \gcd 递归最多层的是 $\gcd(F_n, F_{n-1})$, F_n 是 Fibonacci 数。

1.2 扩展欧几里得算法

应用：

- 求解不定方程 (如 $99x + 78b = 6$ 的整数解);
- 求解模线性方程 (线性同余方程);
- 求解模的逆元;

1.2.1 裴蜀定理

若 a 和 b 是整数，方程 $ax+by=d$ 有整数解当且当 $\gcd(a, b) \mid d$ 。例如，方程 $3x+6y=2$ 就不存在整数解，方程 $3x+6y=3$ 存在（无数多个）整数解，其中一个是 $x=1, y=0$ 。

这个定理给我们了一个判定形如 $ax+by=d$ 的方程是否有整数解的方法，但是它并没有告诉我们如何求解。求解这样的方程是扩展欧几里得算法的内容。

1.2.2 同余

$a \equiv b \pmod{p}$: a, b 模 p 后的余数相同。

若

$$\begin{cases} a1 \equiv b1 \pmod{p} \\ a2 \equiv b2 \pmod{p} \end{cases}$$

则：

$$\begin{cases} a1 \pm a2 \equiv b1 \pm b2 \pmod{p} \\ a1 \cdot a2 \equiv b1 \cdot b2 \pmod{p} \end{cases}$$

例 1.1 求关于 x 的同余方程 $ax \equiv 1 \pmod{b}$ 的最小正整数解。其中 $0 \leq a, b \leq 2 < 10^9$ ，并且保证该方程有解。

如果上述同余方程被满足的话,一定存在整数 y 使得 $ax = 1 + by$, 这样我们可以直接利用扩展欧几里得算法得出一个解。至于最小正整数解也是可以很容易就计算得出, 因为在 $1 \leq x \leq b$ 中这个方程有唯一解。

1.2.3 乘法逆元

如果 $ax = 1 \pmod{p}$, 且 $\gcd(a, p) = 1$ (a 与 p 互质), 则称 a 关于模 p 的乘法逆元为 x 。

在同余意义下, 加减法和乘法都和普通的运算没什么区别, 但是唯独“除法”有一些区别: 当没有逆元时无法进行“除法”!

如 $15 \times 2 = 20 \times 2 \pmod{10}$

但 $15 \neq 20 \pmod{10}$ 因为在模 10 意义下, 2 是没有乘法逆元的。

1.3 求解模线性方程

参考文献

1.4 快速幂

github:LHesperus