数学基础

胡小川

2023 年 2 月 20 日

1 最大公约数（GCD）

1.1 定义

若整数 d 满足 $\frac{a}{d}, \frac{b}{d} \in N$ ，则称 d 是整数 a, b 的**公约数**。d 有多个可能的取值，其中最大的一个被称为最大公约数 (GCD)。

1.2 求解方法

为了求得 $\gcd(a, b)$ 的值，我们可以使用如下定理进行求解：

$$\gcd(a, b) = \gcd(b, a \bmod b) \tag{1}$$

1.2.1 证明

令 $c = a \bmod b$，根据取模定义，则有 $a = kb + c\ (k \in N)$ ，设 d 为 a, b 的公约数（显然 d 一定存在），则有 $\frac{a}{d} = k\frac{b}{d} + \frac{c}{d}$ 。根据公约数定义，$\frac{a}{d}, \frac{b}{d} \in N$ ，所以 $\frac{c}{d} \in N$，即 d 是 c 的公约数。所以，d 是 $a, b, a \bmod b$ 的公约数。即 $\gcd(a, b) = \gcd(b, a \bmod b)$。

1.2.2 复杂度分析

根据（1）式可知，在每次递归之后，a 的值至多变为 $\frac{1}{2}a - 1$，所以时间复杂度为 $O(\log n)$。

2 拓展欧几里得算法（exgcd）

拓展欧几里得算法常用于求解方程 $ax + by = \gcd(a, b)$ 的一组可行解。

设

$$ax_1 + by_1 = \gcd(a, b)$$
$$bx_2 + (a \bmod b)y_2 = \gcd(b, a \bmod b)$$

根据定理 (1) $\gcd(a, b) = \gcd(b, a \bmod b)$, 可得 $ax_1 + by_1 = bx_2 + (a \bmod b)y_2$。根据取模定义，原式可化为 $ax_1 + by_1 = bx_2 + (a - (\lfloor \frac{a}{b} \rfloor \times b))y_2$。将式子展开可以得到：

$$ax_1 + by_1 = ay_2 + bx_2 - \lfloor \frac{a}{b} \rfloor \times by_2 = ay_2 + b(x_2 - \lfloor \frac{a}{b} \rfloor y_2)$$

根据待定系数法，可以得出：

$$x_1 = y_2,\ y_1 = x_2 - \lfloor \frac{a}{b} \rfloor y_2 \tag{2}$$

由此我们得到了拓展欧几里得算法的递推式。

3 乘法逆元

3.1 定义

如果一个线性同余方程 $ax \equiv 1 \pmod b$，则 x 称为 $a \bmod b$ 的逆元，记作 a^{-1}。

3.2 拓展欧几里德法求解

首先，我们可以对定义中的方程进行转化，根据取模的定义，原式可化为：

$$ax \equiv kb + 1$$

即

$$ax + bk \equiv 1$$

注意到，上式与我们刚刚在拓展欧几里德算法中求解的方程近乎一致，唯一区别在于等号右侧。事实上，若方程有解，则 $\gcd(a, b)$ 必须等于 1，否则无解。例如方程 $2x \equiv 1 \pmod 4$ 就是无解的。

因此，我们可以使用拓展欧几里德算法直接求得 x 的值。

3.3 费马小定理求解

3.3.1 定理内容

若 p 为素数，且 $\gcd(a, b) = 1$，则 $a^{p-1} \equiv 1 \pmod p$.

3.3.2 求解过程

根据逆元定义 $ax \equiv 1 \pmod b$, 使用费马小定理可得

$$ax \equiv a^{b-1} \pmod b$$

两边同时除以 a 得

$$x \equiv a^{b-2} \pmod b$$

由于 $b - 2$ 可能较大，因此我们使用快速幂方法求 a^{b-2} 的值。

3.3.3 注意事项

由于费马小定理的限制条件，本方法仅在 b 为素数时可用。

3.4 线性求解

求出 $1,2,\cdot n$ 中每个数关于 p 的逆元

上方已经给出了两种求逆元的方法，对于每个数，求出他们逆元的时间复杂度为 $O(\log n)$。因此求解本问题的时间复杂度为 $O(n\log n)$。现给出一种复杂度为 $O(n)$ 的递推解法：

首先，$1^{-1}\equiv 1 \pmod p$。接着将 p 表示为 $k*i+r(k,i,r\in N,1<r<i<p)$，可以得到：

$$k*i+r\equiv 0 \pmod p$$

两边同乘 $i^{-1}*r^{-1}$：

$$\begin{aligned}k*r^{-1}+i^{-1}&\equiv 0 \pmod p\\ i^{-1}&\equiv -k*r^{-1} \pmod p\\ i^{-1}&\equiv -\frac{p-r}{i}*(p \bmod i)^{-1} \pmod p\\ i^{-1}&\equiv -\lfloor\frac{p}{i}\rfloor*(p \bmod i)^{-1} \pmod p\end{aligned}$$

得出递推公式为：

$$i^{-1}\equiv\begin{cases}1 & i=1\\ -\lfloor\frac{p}{i}\rfloor*(p \bmod i)^{-1} \pmod p & else\end{cases}$$

3.5 用处

1. 求解线性同余方程
2. 处理组合数取模问题
3. 在有取模要求的题目中进行除法运算

3.6 例题

洛谷 P3811

4 中国剩余定理（CRT）

中国剩余定理被用来求解如下的线性同余方程组：

$$\begin{cases}x &\equiv a_1 \pmod{n_1}\\ x &\equiv a_2 \pmod{n_2}\\ &\vdots\\ x &\equiv a_k \pmod{n_k}\end{cases}$$

其中 $n_1,n_2\cdot n_k$ 两两互素

4.1 求解过程

1. 首先，令 $n = \prod_{n=1}^{k}$
2. 接着，对于方程 i:
   (a) 令 $m_i = n/n_i$
   (b) 计算 m_i 关于 n_i 的逆元 m^{-1}
   (c) 令 $c_i = m_i * m^{-1}$
3. 方程的解 $x = \sum_{i=1}^{k} a_i c_i \pmod n$

4.2 证明

111

4.3 例题

有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二。问物几何?

——《孙子算经》

求整数 x 使得 $x \bmod 3 = 2, x \bmod 5 = 3, x \bmod 7 = 2$
解:
$n = 3 * 5 * 7 = 105, n_1 = 3, n_2 = 5, n_3 = 7$
$m_1 = 35, m_2 = 21, m_3 = 15$
$m_1^{-1} = 2, m_2^{-1} = 1, m_3^{-1} = 1$
$c_1 = 35 * 2 = 70, c_1 = 21 * 1 = 21, c_3 = 15 * 1 = 15$
$x = 70 * 2 + 21 * 3 + 15 * 2 = 233 \equiv 23 \pmod{105}$

4.4 洛谷例题

洛谷 P1495

- 题目大意

  自从曹冲搞定了大象以后，曹操就开始捉摸让儿子干些事业，于是派他到中原养猪场养猪，可是曹冲满不高兴，于是在工作中马马虎虎，有一次曹操想知道母猪的数量，于是曹冲想狠狠耍曹操一把。举个例子，假如有 16 头母猪，如果建了 3 个猪圈，剩下 1 头猪就没有地方安家了。如果建造了 5 个猪圈，但是仍然有 1 头猪没有地方去，然后如果建造了 7 个猪圈，还有 2 头没有地方去。你作为曹总的私人秘书理所当然要将准确的猪数报给曹总，你该怎么办?

- 输入描述

  第一行包含一个整数 n ——建立猪圈的次数，接下来 n 行，每行两个整数 a_i, b_i，表示建立了 a_i 个猪圈，有 b_i 头猪没有去处。你可以假定 $a_1 \sim a_n$ 互质。

- 输出格式

  输出包含一个正整数，即为曹冲至少养母猪的数目。

- 样例

  输入

  3

  3 1

  5 1

  7 2

  输出

  16

5 拓展中国剩余定理 (exCRT)

拓展中国剩余定理被用来求解如下的线性同余方程组：

$$\begin{cases} x & \equiv a_1 \pmod{n_1} \\ x & \equiv a_2 \pmod{n_2} \\ & \vdots \\ x & \equiv a_k \pmod{n_k} \end{cases}$$

其中 $n_1, n_2 \cdot n_k$ 不一定互质。
针对此类问题，我们采用讲 k 个方程组两两合并的方法。为了方便演示，设待求解方程组为：

$$\begin{cases} x & \equiv a_1 \pmod{n_1} \\ x & \equiv a_2 \pmod{n_2} \end{cases}$$

根据取模定义，原方程组可化为：

$$\begin{cases} x & \equiv k_1 n_1 + a_1 \\ x & \equiv k_2 n_2 + a_2 \end{cases}$$

将两式合并得：

$$k_1 n_1 + a_1 = k_2 n_2 + a_2$$

即

$$k_1 n_1 - k_2 n_2 = a_2 - a_1$$

根据裴蜀定理，若 $\gcd(n_1, n_2)$ 不能被 $a_2 - a_1$ 整除，则方程组无解。因此，在方程组有解的情况下，设 $t = \frac{a_2 - a_1}{\gcd(n_1, n_2)}, t \in N$。接着，我们使用拓展欧几里德算法求出 $k_1 n_1 - k_2 n_2 = a_2 - a_1$ 的解。设解为 (λ_1, λ_2)，那么方程 $k_1 n_1 - k_2 n_2 = a_2 - a_1$ 的解为 $(t\lambda_1, t\lambda_2)$。即 $k_1 = t\lambda_1, k_2 = t\lambda_2$. 于是 $x = a_1 + t\lambda_1 n_1$. 基础解系为：

$$x \equiv a_1 + t\lambda_1 m_1 \pmod{lcm(n_1, n_2)}$$

5.1 例题

洛谷 P4777

(板子题)