

中国剩余定理学习笔记

beck

2020 年 2 月 27 日

形式描述

中国剩余定理，又称中国余数定理，是数论中的一个关于一元线性同余方程组的定理，说明了一元线性同余方程组有解的准则以及求解方法。也称为孙子定理，古有“韩信点兵”、“孙子定理”、“求一术”（宋沈括）、“鬼谷算”（宋周密）、“隔墙算”（宋周密）、“剪管术”（宋杨辉）、“秦王暗点兵”、“物不知数”之名。用现代数学的语言来说明的话，中国剩余定理给出了以下的一元线性同余方程组：

$$(S): \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

有解的判定条件，并用构造法给出了在有解情况下解的具体形式。中国剩余定理说明：假设整数 m_1, m_2, \dots, m_n 其中任两数互质，则对任意的整数： a_1, a_2, \dots, a_n ，方程组 (S) 有解，并且通解可以用如下方式构造得到：

1. 设 $M = m_1 \times m_2 \times \dots \times m_n = \prod_{i=1}^n m_i$ 是整数 m_1, m_2, \dots, m_n 的乘积，并设 $M_i = M/m_i, \forall i \in \{1, 2, \dots, n\}$ ，即 M_i 是除了 m_i 以外的 $n-1$ 个整数的乘积。
2. 设 $t_i = M_i^{-1}$ 为 M_i 模 m_i 的数论倒数： $t_i M_i \equiv 1 \pmod{m_i}, \forall i \in \{1, 2, \dots, n\}$ 。

3. 方程组 (S) 的通解形式为: $x = a_1 t_1 M_1 + a_2 t_2 M_2 + \dots + a_n t_n M_n + kM = kM + \sum_{i=1}^n a_i t_i M_i$, $k \in \mathbb{Z}$. 在模 M 的意义下, 方程组 (S) 只有一个解: $x = \sum_{i=1}^n a_i t_i M_i$.

证明

从假设可知, 对任何 $i \in \{1, 2, \dots, n\}$, 由于 $\forall j \in \{1, 2, \dots, n\}, j \neq i$, $\gcd(m_i, m_j) = 1$, 所以 $\gcd(m_i, M_i) = 1$. 这说明存在整数 t_i 使得 $t_i M_i \equiv 1 \pmod{m_i}$. 这样的 t_i 叫做 M_i 模 m_i 的数论倒数。考察乘积 $a_i t_i M_i$ 可知:

$$a_i t_i M_i \equiv a_i \cdot 1 = a_i \pmod{m_i},$$

$$\forall j \in \{1, 2, \dots, n\}, j \neq i, a_j t_j M_j \equiv 0 \pmod{m_i}.$$

所以 $x = a_1 t_1 M_1 + a_2 t_2 M_2 + \dots + a_n t_n M_n$ 满足:

$$\forall i \in \{1, 2, \dots, n\}, x = a_i t_i M_i + \sum_{j \neq i} a_j t_j M_j \equiv a_i + \sum_{j \neq i} 0 = a_i \pmod{m_i}.$$

这说明 x 就是方程组 (S) 的一个解。另外, 假设 x_1 和 x_2 都是方程组 (S) 的解, 那么:

$$\forall i \in \{1, 2, \dots, n\}, x_1 - x_2 \equiv 0 \pmod{m_i}.$$

而 m_1, m_2, \dots, m_n 两两互质, 这说明 $M = \prod_{i=1}^n m_i$ 整除 $x_1 - x_2$. 所以方程组 (S) 的任何两个解之间必然相差 M 的整数倍。而另一方面, $x = a_1 t_1 M_1 + a_2 t_2 M_2 + \dots + a_n t_n M_n$ 是一个解, 同时所有形式为:

$$a_1 t_1 M_1 + a_2 t_2 M_2 + \dots + a_n t_n M_n + kM = kM + \sum_{i=1}^n a_i t_i M_i, \quad k \in \mathbb{Z}$$

的整数也是方程组 (S) 的解。所以方程组 (S) 所有的解的集合就是:

$$\left\{ kM + \sum_{i=1}^n a_i t_i M_i; \quad k \in \mathbb{Z} \right\}$$

模反元素

模反元素也称为模倒数, 或者模逆元。一整数 a 对同余之模反元素是指满足以下公式的整数 b

$$a^{-1} \equiv b \pmod{n}.$$

也可以写成以下的式子

$$ab \equiv 1 \pmod{n}.$$

整数 a 对模数 n 之模反元素存在的充分必要条件是 a 和 n 互质，若此模反元素存在，在模数 n 下的除法可以用和对应模反元素的乘法来达成，此概念和实数除法的概念相同。

求模反元素

用扩展欧几里得算法

设 $\text{exgcd}(a, n)$ 为扩展欧几里得算法的函数，则可得到 $ax + ny = g$ ， g 是 a, n 的最大公因数。

若 $g = 1$

则该模反元素存在，根据结果 $ax + ny = 1$

在 $\text{mod } n$ 之下， $ax + ny \equiv ax \equiv 1$ ，根据模反元素的定义 $a \times a^{-1} \equiv 1$ ，此时 x 即为 a 关于模 n 的其中一个模反元素。

事实上， $x + kn (k \in \mathbb{Z})$ 都是 a 关于模 n 的模反元素，这里我们取最小的正整数解 $x \bmod n (x < n)$ 。

若 $g \neq 1$

则该模反元素不存在。

因为根据结果 $ax + ny \neq 1$ ，在 $\text{mod } n$ 之下， $ax \equiv g (g < n)$ 不会同余于 1，因此满足 $a \times a^{-1} \equiv 1$ 的 a^{-1} 不存在。

用欧拉定理

欧拉定理证明当 a, n 为两个互质的正整数时，则有 $a^{\varphi(n)} \equiv 1 \pmod{n}$ ，其中 $\varphi(n)$ 为欧拉函数（小于等于 n 且与 n 互质的正整数个数）。

上述结果可分解为 $a^{\varphi(n)} = a \times a^{\varphi(n)-1} \equiv 1 \pmod{n}$ ，其中 $a^{\varphi(n)-1}$ 即为 a 关于模 n 之模反元素。

辗转相除法

在数学中,辗转相除法,又称欧几里得算法(英语:Euclidean algorithm),是求最大公约数的算法。辗转相除法首次出现于欧几里得的《几何原本》(第VII卷,命题i和ii)中,而在中国则可以追溯至东汉出现的《九章算术》。两个整数的最大公约数是能够同时整除它们的最大的正整数。辗转相除法基于如下原理:两个整数的最大公约数等于其中较小的数和两数相除余数的最大公约数。例如,252和105的最大公约数是21($252 = 21 \times 12$; $105 = 21 \times 5$);因为 $252 - 105 = 21 \times (12 - 5) = 147$,所以147和105的最大公约数也是21。在这个过程中,较大的数缩小了,所以继续进行同样的计算可以不断缩小这两个数直至其中一个变成零。这时,所剩下的还没有变成零的数就是两数的最大公约数。由辗转相除法也可以推出,两数的最大公约数可以用两数的整数倍相加来表示,如 $21 = 5 \times 105 + (-2) \times 252$ 。这个重要的结论叫做贝祖定理。

算法描述

计算过程

辗转相除法是一种递归算法,每一步计算的输出值就是下一步计算时的输入值。设 k 表示步骤数(从0开始计数),算法的计算过程如下。每一步的输入是都是前两次计算的非负余数 r_{k-1} 和 r_{k-2} 。因为每一步计算出的余数都在不断减小,所以, $r_{k-1} < r_{k-2}$ 。在第 k 步中,算法计算出满足以下等式的商 q_k 和余数 r_k :

$$r_{k-2} = q_k r_{k-1} + r_k$$

其中 $0 \leq r_k < r_{k-1}$ 。也就是 r_{k-2} 要不断减去 r_{k-1} 直到比 r_{k-1} 小。为求简明,以下只说明如何求两个非负整数 a 和 b 的最大公约数(负数的情况是简单的)。在第一步计算时($k=0$),设 r_{-2} 和 r_{-1} 分别等于 a 和 b ,第二步(此时 $k=1$)时计算 r_{k-1} (即 b)和 r_0 (第一步计算产生的余数)

相除产生的商和余数，以此类推。整个算法可以用如下等式表示：

$$\begin{aligned}a &= q_0 b + r_0 \\b &= q_1 r_0 + r_1 \\r_0 &= q_2 r_1 + r_2 \\r_1 &= q_3 r_2 + r_3 \\&\dots\end{aligned}$$

如果有 $a < b$ ，算法的第一步实际上会把两个数字交换，因为这时 a 除以 b 所得的商 q_0 会等于 0，余数 r_0 则等于 a 。然后，算法的第二步便是把 b 除以 a ，再计算所得之商和余数。所以，对于 $k \geq 0$ 总有 $r_k < r_{k-1}$ ，即运算的每一步中得出的余数一定小于上一步计算的余数。

由于每一步的余数都在减小并且不为负数，必然存在第 N 步时 r_N 等于 0，使算法终止， r_{N-1} 就是 a 和 b 的最大公约数。其中 N 不可能无穷大，因为在 r_0 和 0 之间只有有限个自然数。

正确性的证明

辗转相除法的正确性可以分成两步来证明。在第一步，我们会证明算法的最终结果 r_{N-1} 同时整除 a 和 b 。因为它是一个公约数，所以必然小于或者等于最大公约数 g 。在第二步，我们证明 g 能整除 r_{N-1} 。所以 g 一定小于或等于 r_{N-1} 。两个不等式只在 $r_{N-1} = g$ 时同时成立。具体证明如下：

1. 证明 r_{N-1} 同时整除 a 和 b ：

因为

2.