中国剩余定理学习笔记

beck

2020 年 2 月 29 日

形式描述

中国剩余定理 [1]，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：

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

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 $m_1, m_2, \ldots, m_n$ 其中任两数互质，则对任意的整数：$a_1, a_2, \ldots, a_n$，方程组 (S) 有解，并且通解可以用如下方式构造得到：

1. 设 $M = m_1 \times m_2 \times \ldots \times m_n = \prod_{i=1}^{n} m_i$ 是整数 $m_1, m_2, \ldots, m_n$ 的乘积，并设 $M_i = M/m_i$，$\forall i \in \{1, 2, \ldots, n\}$，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：$t_i M_i \equiv 1 \pmod{m_i}$，$\forall i \in \{1, 2, \ldots, n\}$.

3. 方程组 (S) 的通解形式为：$x = a_1 t_1 M_1 + a_2 t_2 M_2 + \ldots + a_n t_n M_n + kM = kM + \sum_{i=1}^{n} a_i t_i M_i$，$k \in \mathbb{Z}$. 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 $i \in \{1, 2, \ldots, n\}$，由于 $\forall j \in \{1, 2, \ldots, n\}$，$j \neq i$，$\gcd(m_i, m_j) = 1$，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：

$$\begin{aligned} &a_i t_i M_i \equiv a_i \cdot 1 = a_i \pmod{m_i}, \\ &\forall j \in \{1, 2, \ldots, n\}, j \neq i, a_j t_j M_j \equiv 0 \pmod{m_i}. \end{aligned}$$

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

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

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：

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

而 $m_1, m_2, \ldots, m_n$ 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，$x = a_1 t_1 M_1 + a_2 t_2 M_2 + \ldots + a_n t_n M_n$ 是一个解，同时所有形式为：

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

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 [3] 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 $\bmod n$ 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 $x \mod n\ (x<n)$。

若 $g\neq 1$
则该模反元素不存在。
因为根据结果 $ax+ny\neq 1$，在 $\bmod n$ 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 $a^{\varphi(n)}\equiv 1\ (\bmod\ n)$，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 $a^{\varphi(n)}=a\times a^{\varphi(n)-1}\equiv 1\ (\bmod\ n)$，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 [5]，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 $21 = 5\times105 + (-2)\times252$。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} 小于 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 $0 \le r_k < r_{k-1}$。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_{-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：

   因为余数 r_N 是 0，r_{N-1} 能够整除 r_{N-2}：

   $$r_{N-2} = q_N r_{N-1}$$

   因为 r_{N-1} 能够整除 r_{N-2}，所以也能够整除 r_{N-3}：

   $$r_{N-3} = q_{N-1} r_{N-2} + r_{N-1}$$

   同理可证 r_{N-1} 可以整除所有之前步骤的余数，包括 a 和 b，即 r_{N-1} 是 a 和 b 的公约数，$r_{N-1} \leq g$。

2. 证明最大公约数 g 能整除 r_{N-1}：

根据定义，a 和 b 可以写成 g 的倍数：$a = mg$、$b = ng$，其中 m 和 n 是自然数。因为 $r_0 = a - q_0 b = mg - q_0 ng = (m - q_0 n)g$，所以 g 整除 r_0。同理可证 g 整除每个余数 $r_1, r2, \ldots, r_{N-1}$。因为最大公约数 g 整除 r_{N-1}，因而 $g \leq r_{N-1}$。

因为第一步的证明告诉我们 $r_{N-1} \leq g$，所以 $g = r_{N-1}$。即：

$$g = \gcd(a, b) = \gcd(b, r_0) = \gcd(r_0, r_1) = \ldots = gcd(r_{N-2}, r_{N-1}) = r_{N-1}$$

计算商和余数

在每个步骤 k 中，辗转相除法都需要计算两个数 r_{k-1} 和 r_{k-2} 的商 q_k 和余数 r_k：

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

其中 $0 \leq r_k < r_{k-1}$。除法的算法保证这样的商和余数总是存在。自然数的除法算法还指出这样的商和余数是惟一的，但这对辗转相除法而言并非必要。

在欧几里得最初的描述中，商和余数是通过连续的减法来计算的，即从 r_{k-2} 中不断减去 r_{k-1} 直到小于 r_{k-1}。一个更高效的做法是使用整数除法和模除来计算商和余数：

$$r_k \equiv r_{k-2} \bmod r_{k-1}$$

扩展欧几里得算法

扩展欧几里得算法 [2]（英语：Extended Euclidean algorithm）是欧几里得算法（又叫辗转相除法）的扩展。已知整数 a、b，扩展欧几里得算法可以在求得 a、b 的最大公约数的同时，能找到整数 x、y（其中一个很可能是负数），使它们满足贝祖等式

$$ax + by = \gcd(a, b)$$

如果 a 是负数，可以把问题转化成

$$|a|(-x) + by = \gcd(|a|, b)$$

（$|a|$ 为 a 的绝对值），然后令 $x' = (-x)$。
通常谈到最大公约数时，我们都会提到一个非常基本的事实（由裴蜀定理给出）：给定二个整数 a、b，必存在整数 x、y 使得 $ax + by = \gcd(a, b)$。
众所周知，已知两个数 a 和 b，对它们进行辗转相除（欧几里得算法），可得它们的最大公约数。不过，在欧几里得算法中，我们仅仅利用了每步带余除法所得的余数。扩展欧几里得算法还利用了带余除法所得的商，在辗转相除的同时也能得到裴蜀等式（裴蜀定理中描述的等式，裴蜀定理也翻译成贝祖定理）中的 x、y 两个系数。以扩展欧几里得算法求得的系数是满足裴蜀等式的最简系数。
另外，扩展欧几里得算法是一种自验证算法，最后一步得到的 s_{i+1} 和 t_{i+1}（s_{i+1} 和 t_{i+1} 的含义见下文）乘以 $\gcd(a, b)$ 后恰为 a 和 b，可以用来验证计算结果是否正确。
扩展欧几里得算法可以用来计算模反元素 (也叫模逆元)，求出模反元素是 RSA 加密算法中获得所需公钥、私钥的必要步骤。

算法和举例

在标准的欧几里得算法中，我们记欲求最大公约数的两个数为 a, b，第 i 步带余除法得到的商为 q_i，余数为 r_{i+1}，则欧几里得算法可以写成如下形

式:

$$
\begin{aligned}
r_0 &= a \\
r_1 &= b \\
&\cdots \\
r_{i+1} &= r_{i-1} - q_i r_i \quad and \quad 0 \le r_{i+1} < |r_i| \\
&\cdots
\end{aligned}
$$

当某步得到的 $r_{i+1} = 0$ 时，计算结束。上一步得到的 r_i 即为 a, b 的最大公约数。

扩展欧几里得算法在 q_i, r_i 的基础上增加了两组序列，记作 s_i 和 t_i，并令 $s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1$，在欧几里得算法每步计算 $r_{i+1} = r_{i-1} - q_i r_i$ 之外额外计算 $s_{i+1} = s_{i-1} - q_i s_i$ 和 $t_{i+1} = t_{i-1} - q_i t_i$，亦即:

$$
\begin{aligned}
r_0 &= a & r_1 &= b \\
s_0 &= 1 & s_1 &= 0 \\
t_0 &= 0 & t_1 &= 1 \\
&\vdots & &\vdots \\
r_{i+1} &= r_{i-1} - q_i r_i \quad and \quad 0 \le r_{i+1} < |r_i| \\
s_{i+1} &= s_{i-1} - q_i s_i \\
t_{i+1} &= t_{i-1} - q_i t_i \\
&\vdots
\end{aligned}
$$

算法结束条件与欧几里得算法一致，也是 $r_{i+1} = 0$，此时所得的 s_i 和 t_i 即满足等式 $\gcd(a, b) = r_i = as_i + bt_i$。

证明

由于 $0 \le r_{i+1} < |r_i|$，r_i 序列是一个递减序列，所以本算法可以在有限步内终止。又因为 $r_{i+1} = r_{i-1} - r_i q_i$，$(r_{i-1}, r_i)$ 和 (r_i, r_{i+1}) 的最大公约数是一样的，所以最终得到的 r_k 是 a, b 的最大公约数。

在欧几里得算法正确性的基础上，又对于 $a = r_0$ 和 $b = r_1$ 有等式 $as_i + bt_i =$

r_i 成立（$i = 0$ 或 1）。这一关系由下列递推式对所有 $i > 1$ 成立：

$$\begin{aligned} r_{i+1} = r_{i-1} - r_i q_i &= (as_{i-1} + bt_{i-1}) - (as_i + bt_i)q_i \\ &= (as_{i-1} - as_i q_i) + (bt_{i-1} - bt_i q_i) \\ &= as_{i+1} + bt_{i+1} \end{aligned}$$

因此 s_i 和 t_i 满足裴蜀等式，这就证明了扩展欧几里得算法的正确性。

裴蜀定理

在数论中，裴蜀等式（英语：Bézout's identity）或裴蜀定理 [4]（Bézout's lemma）是一个关于最大公约数（或最大公约式）的定理。裴蜀定理得名于法国数学家艾蒂安·裴蜀，说明了对任何整数 a、b 和 m，关于未知数 x 和 y 的线性丢番图方程（称为裴蜀等式）：

$$ax + by = m$$

有整数解时当且仅当 m 是 a 及 b 的最大公约数 d 的倍数。裴蜀等式有解时必然有无穷多个整数解，每组解 x、y 都称为裴蜀数，可用扩展欧几里得算法求得。

例如，12 和 42 的最大公约数是 6，则方程 $12x + 42y = 6$ 有解。事实上有 $(-3) \times 12 + 1 \times 42 = 6$ 及 $4 \times 12 + (-1) \times 42 = 6$。

特别来说，方程 $ax + by = 1$ 有整数解当且仅当整数 a 和 b 互素。

裴蜀等式也可以用来给最大公约数定义：d 其实就是最小的可以写成 $ax+by$ 形式的正整数。这个定义的本质是整环中“理想”的概念。因此对于多项式整环也有相应的裴蜀定理。

整数中的裴蜀定理

对任意两个整数 a、b，设 d 是它们的最大公约数。那么关于未知数 x 和 y 的线性丢番图方程（称为裴蜀等式）：

$$ax + by = m$$

有整数解 (x, y) 当且仅当 m 是 d 的整数倍。裴蜀等式有解时必然有无穷多个解。

证明:

如果 a 和 b 中有一个是 0，比如 $a=0$，那么它们两个的最大公约数是 b。这时裴蜀等式变成 $by=m$，它有整数解 (x,y) 当且仅当 m 是 b 的倍数，而且有解时必然有无穷多个解，因为 x 可以是任何整数。定理成立。
以下设 a 和 b 都不为 0。
设 $A=\{xa+yb;(x;y)\ \in \mathbb{Z}^2\}$，下面证明 A 中的最小正元素是 a 与 b 的最大公约数。
首先，$A\bigcap \mathbb{N}^*$ 不是空集（至少包含 $|a|$ 和 $|b|$），因此由于自然数集合是良序的，A 中存在最小正元素 $d_0=x_0a+y_0b$。考虑 A 中任意一个正元素 $p\ (=x_1a+y_1b)$ 对 d_0 的带余除法：
设 $p=qd_0+r$，其中 q 为正整数，$0\leq r<d_0$。但是

$$r=p-qd_0=x_1a+y_1b-q(x_0a+y_0b)\in A$$

因此 $r=0$, $d_0|p$。也就是说，A 中任意一个正元素 p 都是 d_0 的倍数，特别地：$d_0|a$、$d_0|b$。因此 d_0 是 a 和 b 的公约数。
另一方面，对 a 和 b 的任意正公约数 d，设 $a=kd$、$b=ld$，那么

$$d_0=x_0a+y_0b=(x_0k+y_0l)d$$

因此 $d|d_0$。所以 d_0 是 a 和 b 的最大公约数。
在方程 $ax+by=m$ 中，如果 $m=m_0d_0$，那么方程显然有无穷多个解：

$$\left\{(m_0x_0+\frac{kb}{d},m_0y_0-\frac{ka}{d})\mid k\in\mathbb{Z}\right\}$$

$m=1$ 时，方程有解当且仅当 a、b 互质。方程有解时，解的集合是

$$\left\{(\frac{m}{d}x_0+\frac{kb}{d},\frac{m}{d}y_0-\frac{ka}{d})\mid k\in\mathbb{Z}\right\}$$

其中 (x_0,y_0) 是方程 $ax+by=d$ 的一个解，可由辗转相除法得到。
所有解中，恰有二解 (x,y) 满足 $|x|\leq|b/d|$ 及 $|y|\leq|a/d|$，等号只会在 a 及 b 其中一个是另一个的倍数时成立。辗转相除法给出的解会是这两解中的一个。

References

[1] wikipedia. 中国剩余定理. URL: https://zh.wikipedia.org/wiki/%E4%B8%AD%E5%9B%BD%E5%89%A9%E4%BD%99%E5%AE%9A%E7%90%86.

[2] wikipedia. 扩展欧几里得算法. URL: https://zh.wikipedia.org/wiki/%E6%89%A9%E5%B1%95%E6%AC%A7%E5%87%A0%E9%87%8C%E5%BE%97%E7%AE%97%E6%B3%95.

[3] wikipedia. 模逆元. URL: https://zh.wikipedia.org/wiki/%E6%A8%A1%E5%8F%8D%E5%85%83%E7%B4%A0.

[4] wikipedia. 裴蜀定理. URL: https://zh.wikipedia.org/wiki/%E8%A3%B4%E8%9C%80%E5%AE%9A%E7%90%86.

[5] wikipedia. 辗转相除法. URL: https://zh.wikipedia.org/wiki/%E8%BE%97%E8%BD%AC%E7%9B%B8%E9%99%A4%E6%B3%95.