Collections Of Math

数学 收集箱

If people do not believe that mathematics is simple,
it is only because they do not realize how complicated life is.

整理：Huyi Chen
整理时间：November 3, 2016
Email: hooyuser@outlook.com

Version: 1.00

目　录

第 1 章　数论

1.1　中国剩余定理

1.1.1　历史

《孙子算经》是中国南北朝时期（公元 5 世纪）的数学著作 [1]. 其卷下第二十六题，叫做“物不知数”问题，原文如下:

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？

翻译成白话文，即一个整数除以三余二，除以五余三，除以七余二，求这个整数. 《孙子算经》中首次提到了同余方程组问题，并给出了以上具体问题的解法，因此在一些中文数学文献中，中国剩余定理也会被称为孙子定理.

宋朝数学家秦九韶于 1247 年《数书九章》卷一、二《大衍类》对“物不知数”问题做出了完整系统的解答。明朝数学家程大位将解法编成易于上口的《孙子歌诀》[2]:

三人同行七十希，五树梅花廿一支，七子团圆正半月，除百零五使得知.

这个歌诀给出了模数为 3、5、7 时候的同余方程的秦九韶解法。意思是：将除以 3 得到的余数乘以 70，将除以 5 得到的余数乘以 21，将除以 7 得到的余数乘以 15，全部加起来后除以 105，得到的余数就是答案。比如说在以上的物不知数问题里面，使用以上的方法计算就得到

$$70 \times 2 + 21 \times 3 + 15 \times 2 = 233 = 2 \times 105 + 23.$$

因此按歌诀求出的结果就是 23.

1.1.2　定理陈述

中国剩余定理有三种常见的表述方式，将在下面一一给出. 第一种是以余数的形式. 我们首先引入带余除法的概念.

Proposition 1.1 带余除法

设 $a \in \mathbb{Z}$，$b \in \mathbb{N}^+$. 一定存在唯一的整数对 (q,r)，使 $a = bq + r$，且 $0 \le r < b$. 其中 $b = \left[\frac{a}{b}\right]$ 称作 a 除以 b 的不完全商，$r = a - b\left[\frac{a}{b}\right]$ 称作 a 除以 b 的余数，r 也常常被记作 $a \bmod b$.

命题的证明是平凡的,这里略去. 在下面定理的叙述中,我们总是假定 $n_1, n_2, \cdots, n_k$ 是大于 1 的整数，而 n_i 常常称作模. 同时，我们记 $N = n_1 n_2 \cdots n_k$ 为所有模的积. 现在给出中国剩余定理的第一种表述.

Theorem 1.1 中国剩余定理 I

如果 n_i 两两互素, 且整数 r_i 满足 $0 \le r < n_i$, 则存在唯一满足 $0 \le x < N$ 的整数 x，使得对每一个 $i(1 \le i \le k)$, 都有 $x \bmod n_i = r_i$.

上述表述是《孙子算经》中具体问题的一般化描述，但直接处理余数往往并不方便. 若引入同余记号，这个问题实际上就变成如何去求解一个一元一次同余方程组，这也是中国剩余定理的第二种表述，而它与第一种描述是完全等价的.

Theorem 1.2 中国剩余定理 II

如果 $n_1, n_2, \cdots, n_k$ 两两互素，且 $r_1, r_2, \cdots, r_k \in \mathbb{Z}$，则同余方程组

$$\begin{cases} x \equiv r_1 \pmod{n_1} \\ x \equiv r_2 \pmod{n_2} \\ \qquad \vdots \\ x \equiv r_k \pmod{n_k} \end{cases}$$

有无穷多解，且任意两个解模 N 同余.

☞ **Proof:** 先证存在性. 记除了 N_i 外所有模的乘积为 $N_i = \dfrac{N}{n_i}$. 因为 n_i 两两互素, 故 N_i 也与 n_i 互素. 由 Bézout 等式，存在整数 M_i, m_i，使得

$$M_i N_i + m_i n_i = 1.$$

因此

$$N_i M_i \equiv 1 \pmod{n_i}.$$

记 $M_i = N_i^{-1}$ 为 N_i 的数论倒数，则 x 可以构造为 $\sum_{i=1}^{k} r_i N_i N_i^{-1}$. 事实上，只要注意到 $j \ne i$ 时

$n_j|N_i$，于是有

$$x \equiv \sum_{i=1}^{k} r_i N_i N_i^{-1} \equiv r_i N_i N_i^{-1} \equiv r_i \pmod{n_i}.$$

再证唯一性. 若 y 也是一个解，则 $x \equiv y \equiv r_i \pmod{n_i}$. 又因为 n_i 两两互素，由算术基本定理知 $x \equiv y \pmod{N}$. 综上可得，同余方程组的通解是

$$x = \sum_{i=1}^{k} r_i N_i N_i^{-1} + N.$$

□

因为模 n_i 的剩余类构成一个环 $\mathbb{Z}_{n_i} = \mathbb{Z}/n_i\mathbb{Z}$，运用抽象代数的语言，中国剩余定理可以描述成一个环同构. 在此之前，我们有必要先明确环的直积的定义.

Definition 1.1 环的直积

给定两个环 $(G,+,*)$ 和 $(H,\oplus,\odot)$，它们的直积仍是一个环 $(G\times H,+,\cdot)$，其中集合 $G\times H = \{(g,h)|g\in G, h\in H\}$ 是 G 与 H 的笛卡儿积；环上的运算 $+,\cdot$ 定义为

- $(g_1,h_1)+(g_2,h_2) = (g_1+g_2, h_1\oplus h_2)$
- $(g_1,h_1)\cdot(g_2,h_2) = (g_1 * g_2, h_1\odot h_2)$

在不会引起误解的情形下，环 $(G\times H,+,*)$ 可简记 $G\times H$, 其乘法单位元为 $(1_G,1_H)$. 类似地，对于可数个环，我们也可通过这种分量加法和分量乘法的方式，定义 $\{R_i\}_{i\in I}$ 的直积 $\prod\limits_{i\in I} R_i$.

♡

有了环的直积这一个概念后，就可以正式介绍定理的第三种表述了. 这将为我们提供一个更加清晰的视角.

Theorem 1.3 中国剩余定理 III

若 $n_1 n_2 \cdots n_k$ 两两互素，则映射

$$\varphi : (x \bmod n_1, x \bmod n_2, \cdots, x \bmod n_k) \mapsto x \bmod N$$

确定一个环同构

$$\varphi : \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}.$$

♣

☞ **Proof:** 在下面的证明中为了书写简便，对于模 m 剩余类 $\bar{x} = x + m\mathbb{Z} = \{x + km|k\in\mathbb{Z}\} \in \mathbb{Z}/m\mathbb{Z}$，我们将它与剩余类的代表元 x 不做区分. 首先证明 φ 是一个双射. 事实上，如果

$$\varphi(r_1, r_2, \cdots, r_k) = \varphi(r_1', r_2', \cdots, r_k') = R,$$

则有 $r_i \equiv r_i' \equiv R \pmod{n_i}$，或 $(r_1, r_2, \cdots, r_k) = (r_1', r_2', \cdots, r_k')$. 这说明 φ 是单射. 又注意到基数 $|\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}| = |\mathbb{Z}/N\mathbb{Z}| = N$, 所以 φ 一定是双射. 此外，我们还需验证双射 φ 保持运算。根据环的直积的定义，我们有

$$\begin{aligned}\varphi(a_1, a_2, \cdots, a_k) + \varphi(b_1, b_2, \cdots, b_k) &= \sum_{i=1}^{k} a_i N_i N_i^{-1} + \sum_{i=1}^{k} b_i N_i N_i^{-1} = \sum_{i=1}^{k} (a_i + b_i) N_i N_i^{-1} \\ &= \varphi(a_1 + b_1, a_2 + b_2, \cdots, a_k + b_k) \\ &= \varphi[(a_1, a_2, \cdots, a_k) + (b_1, b_2, \cdots, b_k)].\end{aligned}$$

$$\begin{aligned}\varphi(a_1, a_2, \cdots, a_k) \cdot \varphi(b_1, b_2, \cdots, b_k) &= \left(\sum_{i=1}^{k} a_i N_i N_i^{-1}\right) \cdot \left(\sum_{i=1}^{k} b_i N_i N_i^{-1}\right) \\ &= \sum_{i=1}^{k} a_i b_i (N_i N_i^{-1})^2 + \sum_{i \neq j} a_i N_i N_i^{-1} b_j N_j N_j^{-1} \\ &= \sum_{i=1}^{k} a_i b_i N_i N_i^{-1} \\ &= \varphi(a_1 \cdot b_1, a_2 \cdot b_2, \cdots, a_k \cdot b_k) \\ &= \varphi[(a_1, a_2, \cdots, a_k) \cdot (b_1, b_2, \cdots, b_k)].\end{aligned}$$

这就证明了 φ 是 $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$ 到 $\mathbb{Z}/N\mathbb{Z}$ 上的环同构.

□

在环同构的看法下，我们可以将定理自然地推广到一般的 PID（主理想整环）上. 这是因为证明中用到的 Bézout 等式有对应的推广，而算术基本定理（唯一分解定理）在更一般的 UFD（唯一分解整环）上也成立. 如果用互素理想代替

参考文献

[1] J. W. Dauben, “The mathematics of egypt, mesopotamia, china, india and islam：A sourcebook,” 2007.

[2] 李俨, “大衍求一术的过去和未来,” 1998.