中国剩余定理

在《孙子算经》中有这样一个问题："今有物不知其数，三三数之剩二（除以 3 余 2），五五数之剩三（除以 5 余 3），七七数之剩二（除以 7 余 2），问物几何？"这个问题称为"孙子问题"，该问题的一般解法国际上称为"中国剩余定理"。具体解法分三步：

1. 找出三个数：从 3 和 5 的公倍数中找出被 7 除余 1 的最小数 15，从 3 和 7 的公倍数中找出被 5 除余 1 的最小数 21，最后从 5 和 7 的公倍数中找出除 3 余 1 的最小数 70。

2. 用 15 乘以 2（2 为最终结果除以 7 的余数），用 21 乘以 3（3 为最终结果除以 5 的余数），同理，用 70 乘以 2（2 为最终结果除以 3 的余数），然后把三个乘积相加 15∗2+21∗3+70∗215∗2+21∗3+70∗2 得到和 233。

3. 用 233 除以 3，5，7 三个数的最小公倍数 105，得到余数 23，即 233%105=23233%105=23。这个余数 23 就是符合条件的最小数。

就这么简单。我们在感叹神奇的同时不禁想知道古人是如何想到这个方法的，有什么基本的数学依据吗？

我们将"孙子问题"拆分成几个简单的小问题，从零开始，试图揣测古人是如何推导出这个解法的。

首先，我们假设 n1n1 是满足除以 3 余 2 的一个数，比如 2，5，8 等等，也就是满足 3∗k+2（k>=0）3∗k+2（k>=0）的一个任意数。同样，我们假设 n2n2 是满足除以 5 余 3 的一个数，n3n3 是满足除以 7 余 2 的一个数。

有了前面的假设，我们先从 n1n1 这个角度出发，已知 n1n1 满足除以 3 余 2，能不能使得 n1+n2n1+n2 的和仍然满足除以 3 余 2？进而使得 n1+n2+n3n1+n2+n3 的和仍然满足除以 3 余 2？

这就牵涉到一个最基本数学定理，如果有 a%b=ca%b=c，则有(a+k∗b)%b=c(k 为非零整数)(a+k∗b)%b=c(k 为非零整数)，换句话说，如果一个除法运算的余数为 cc，那么被除数与 kk 倍的除数相加（或相减）的和（差）再与除数相除，余数不变。这个是很好证明的。

以此定理为依据，如果 n2n2 是 3 的倍数，n1+n2n1+n2 就依然满足除以 3 余 2。同理，如果 n3n3 也是 3 的倍数，那么 n1+n2+n3n1+n2+n3 的和就满足除以 3 余 2。这是从 n1n1 的角度考虑的，再从 n2n2，n3n3 的角度出发，我们可推导出以下三点：

1. 为使 n1+n2+n3n1+n2+n3 的和满足除以 3 余 2，n2n2 和 n3n3 必须是 3 的倍数。

2. 为使 n1+n2+n3n1+n2+n3 的和满足除以 5 余 3，n1n1 和 n3n3 必须是 5 的倍数。

3. 为使 n1+n2+n3n1+n2+n3 的和满足除以 7 余 2，n1n1 和 n2n2 必须是 7 的倍数。

因此，为使 n1+n2+n3n1+n2+n3 的和作为“孙子问题”的一个最终解，需满足：

1. n1n1 除以 3 余 2，且是 5 和 7 的公倍数。

2. n2n2 除以 5 余 3，且是 3 和 7 的公倍数。

3. n3n3 除以 7 余 2，且是 3 和 5 的公倍数。

所以，孙子问题解法的本质是从 5 和 7 的公倍数中找一个除以 3 余 2 的数 n1n1，从 3 和 7 的公倍数中找一个除以 5 余 3 的数 n2n2，从 3 和 5 的公倍数中找一个除以 7 余 2 的数 n3n3，再将三个数相加得到解。在求 n1n1，n2n2，n3n3 时又用了一个小技巧，以 n1n1 为例，并非从 5 和 7 的公倍数中直接找一个除以 3 余 2 的数，而是先找一个除以 3 余 1 的数，再乘以 2。也就是先求出 5 和 7 的公倍数模 3 下的逆元，再用逆元去乘余数。

这里又有一个数学公式，如果 a%b=ca%b=c，那么(a∗k)%b=a%b+a%b+…+a%b=c+c+…+c=k∗c(k>0)(a∗k)%b=a%b+a%b+…+a%b=c+c+…+c=k∗c(k>0),也就是说，如果一个除法的余数为 cc，那么被除数的 kk 倍与除数相除的余数为 k∗ck∗c。展开式中已证明。

最后，我们还要清楚一点，n1+n2+n3n1+n2+n3 只是问题的一个解，并不是最小的解。如何得到最小解？我们只需要从中最大限度的减掉掉 3，5，7 的公倍数 105 即可。道理就是前面讲过的定理“如果 a%b=ca%b=c，则有(a−k∗b)%b=c(a−k∗b)%b=c”。所以（n1+n2+n3）%105（n1+n2+n3）%105 就是最终的最小解。

这样一来就得到了中国剩余定理的公式：

设正整数 $m_1, m_2, \ldots, m_k$ 两两互素，则同余方程组

$$
\begin{aligned}
x &\equiv a_1 (mod\ m_1) \\
x &\equiv a_2 (mod\ m_2) \\
x &\equiv a_3 (mod\ m_3) \\
&\ \ \vdots \\
x &\equiv a_k (mod\ m_k)
\end{aligned}
$$

有整数解。并且在模 $M = m_1 \cdot m_2 \cdot \ldots \cdot m_k$ 下的解是唯一的，解为

$$x \equiv (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + ... + a_k M_k M_k^{-1}) mod\ M$$

其中$M_i = M/m_i$，而M_i^{-1}为M_i模m_i的逆元。

中国剩余定理扩展——求解模数不互质情况下的线性方程组：

普通的中国剩余定理要求所有的m_i互素，那么如果不互素呢，怎么求解同余方程组？

这种情况就采用两两合并的思想，假设要合并如下两个方程：

$$x = a_1 + m_1 x_1$$
$$x = a_2 + m_2 x_2$$

那么得到：

$$a_1 + m_1 x_1 = a_2 + m_2 x_2 \ \Rightarrow \ m_1 x_1 + m_2 x_2 = a_2 - a_1$$

我们需要求出一个最小的 xx 使它满足：

$$\mathrm{x} = a_1 + m_1 x_1 = a_2 + m_2 x_2$$

那么 x1x1 和 x2x2 就要尽可能的小，于是我们用扩展欧几里得算法求出 x1x1 的最小正整数解，将它代回 a1+m1x1a1+m1x1，得到 xx 的一个特解 x′x′，当然也是最小正整数解。

所以 xx 的通解一定是 x′x′加上 lcm(m1,m2)∗klcm(m1,m2)∗k，这样才能保证 xx 模 m1m1 和 m2m2 的余数是 a1a1 和 a2a2。由此，我们把这个 x′x′当做新的方程的余数，把 lcm(m1,m2)lcm(m1,m2)当做新的方程的模数。（这一段是**关键**）

合并完成：

$$\mathrm{x} \equiv x' \ (mod \ \ lcm(m1, m2))$$