中国剩余定理

《数论概论》的描述

定理 11.2（中国剩余定理） 设 m 与 n 是整数，$\gcd(m, n)=1$，b 与 c 是任意整数．则同余式组

$$x \equiv b(\bmod m) \quad 与 \quad x \equiv c(\bmod n)$$

恰有一个解 $0 \leqslant x \leqslant mn$.

证明 像通常一样，我们由例子开始．假设要解

$$x \equiv 8(\bmod 11) \quad 与 \quad x \equiv 3(\bmod 19).$$

第一个同余式的解由形如 $x=11y+8$ 的所有整数组成．将它代入第二个同余式，化简并求解．因此，

$$11y+8 \equiv 3(\bmod 19)$$
$$11y \equiv 14(\bmod 19).$$

我们知道怎样解这种类型的线性同余式组（见第 8 章线性同余式定理）．解是 $y_1 \equiv 3(\bmod 19)$，然后可用 $x_1=11y_1+8=11 \cdot 3+8=41$ 求得原来同余式的解．最后验证答案：$(41-8)/11=3$ 与 $(41-3)/9=2$ 是正确的．

对一般情况，由解第一个同余式 $x \equiv b(\bmod m)$ 开始．其解由形如 $x=my+b$ 的所有数组成．将此代入第二个同余式得

$$my \equiv c-b(\bmod n).$$

已知 $\gcd(m, n)=1$，第 8 章线性同余式定理告诉我们恰有一个解 y_1，$0 \leqslant y_1<n$．则

$$x_1=my_1+b$$

给出了原来同余式组的解，这是唯一解 x_1，$0 \leqslant x_1<mn$，因为在 0 与 n 之间有唯一解 y_1，且用 m 乘 y_1 得 x_1．这就完成了中国剩余定理的证明及公式 $\phi(mn)=\phi(m)\phi(n)$ 的证明． □

历史插曲 中国剩余定理的第一个有记载的实例出现在 3 世纪末 4 世纪初的中国数学著作中．令人惊讶的是，它涉及解由三个同余式构成的同余式组这样的难题．

“今有物不知其数．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》(孙子的数学著作)，大约公元 300 年，第 3 卷问题 26

《数学一本通》的描述

【例 1.5－1】 孙子算经

【问题描述】

今有物不知其数，三三数之余二；五五数之余三；七七数之余二。问物几何？

【问题分析】

答曰：二十三。

古人的口诀：三人同行七十稀，五树梅花廿一枝，七子团圆月正半，除百零五便得知。

现代同余理论：$23\equiv2\times70+3\times21+2\times15 \pmod{105}$，问，70，21，15 如何得到的？

其实，原问题为求解以下的同余方程组：$\begin{cases}x\equiv2 \pmod 3\\x\equiv3 \pmod 5\\x\equiv2 \pmod 7\end{cases}$

首先，若 X_0 为上述同余方程组的解，则 $X_0+105\times k$（k 为整数）也为上述同余方程组的解。

其次，古人的口诀已经提示我们先解下面三个特殊的同余方程组：

(1) $\begin{cases}x\equiv1 \pmod 3\\x\equiv0 \pmod 5\\x\equiv0 \pmod 7\end{cases}$ (2) $\begin{cases}x\equiv0 \pmod 3\\x\equiv1 \pmod 5\\x\equiv0 \pmod 7\end{cases}$ (3) $\begin{cases}x\equiv0 \pmod 3\\x\equiv0 \pmod 5\\x\equiv1 \pmod 7\end{cases}$

的特殊解：

$\begin{bmatrix}1\\0\\0\end{bmatrix}=?$ $\begin{bmatrix}0\\1\\0\end{bmatrix}=?$ $\begin{bmatrix}0\\0\\1\end{bmatrix}=?$

以方程(1)为对象，相当于解一个这样的同余方程：$35y\equiv1 \pmod 3$，为什么呢？原因是从(1)的模数及条件知，x 应是 35 的倍数，于是可以假设 $x=35y$，有：$35y\equiv1 \pmod 3$，相当于 $2y\equiv1 \pmod 3$，解出 $y=2 \pmod 3$，于是 $x\equiv35\times2\equiv70 \pmod{105}$。类似地，得到(2)、(3)方程的模 105 的解 21、15。于是有：

$\begin{bmatrix}1\\0\\0\end{bmatrix}=70$ $\begin{bmatrix}0\\1\\0\end{bmatrix}=21$ $\begin{bmatrix}0\\0\\1\end{bmatrix}=15$

得出：$\begin{bmatrix}2\\3\\2\end{bmatrix}=2\begin{bmatrix}1\\0\\0\end{bmatrix}+3\begin{bmatrix}0\\1\\0\end{bmatrix}+2\begin{bmatrix}0\\0\\1\end{bmatrix}=2\times70+3\times21+2\times15\equiv23 \pmod{105}$

上面的解法分三步：

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，$15*2+21*3+70*2$ 15*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 $233\%105=23$ 233%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 ***n*1** 是满足除以3余2的一个数，比如2，5，8等等，也就是满足$3*k+2$（$k>=0$）的一个任意数。同样，我们假设 ***n*2** 是满足除以5余3的一个数，***n*3** 是满足除以7余2的一个数。

有了前面的假设，我们先从***n*1** 这个角度出发，已知***n*1** 满足除以3余2，能不能使得 ***n*1 +*n*2** 的和仍然满足除以3余2？进而使得 ***n*1+*n*2+*n*3** 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$a\%b=c$，则有 $(a+k*b)\%b=c$ (k为非零整数)，换句话说，如果一个除法运算的余数为c，那么被除数与 k 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 ***n*2** 是3的倍数，***n*1 +*n*2** 就依然满足除以3余2。同理，如果 ***n*3** 也是3的倍数，那么***n*1 +*n*2 +*n*3** 的和就满足除以3余2。这是从***n*1** 的角度考虑的，再从***n*2**，***n*3** 的角度出发，我们可推导出以下三点：

1. 为使 ***n*1+*n*2+*n*3** 的和满足除以3余2，***n*2** 和 ***n*3** 必须是3的倍数。
2. 为使 ***n*1+*n*2+*n*3** 的和满足除以5余3，***n*1** 和 ***n*3** 必须是5的倍数。
3. 为使 ***n*1+*n*2+*n*3** 的和满足除以7余2，***n*1** 和 ***n*2** 必须是7的倍数。

因此，为使 ***n*1 +*n*2 +*n*3** 的和作为“孙子问题”的一个最终解，需满足：

1. ***n*1**除以3余2，且是5和7的公倍数。
2. ***n*2**除以5余3，且是3和7的公倍数。
3. ***n*3**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 ***n*1**，从3和7的公倍数中找一个除以5余3的数 ***n*2**，从3和5的公倍数中找一个除以7余2的数 ***n*3** ，再将三个数相加得到解。在求***n*1** ，***n*2**，***n*3** 时又用了一个小技巧，以 ***n*1** 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$a\%b=c$ 那么$(a*k)\%b=a\%b+a\%b+\ldots+a\%b=c+c+\ldots+c=k*c$($k$>0) ,也就是说，如果一个除法的余数为$c$，那么被除数的 k 倍与除数相除的余数为$k*c$ 。展开式中已证明。

最后，我们还要清楚一点，***n* 1 +*n* 2 +*n* 3** 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$a\%b=c$，则有$(a-k*b)\%b=c$ ”。所以 **(*n*1 +*n*2 +*n*3) %105** 就是最终的最小解。

下面，我们就来介绍“中国剩余定理”。

设自然数 $m_1, m_2, \cdots m_r$ 两两互素，并记 $N=m_1 * m_2 * \cdots * m_r$，则同余方程组：

$$\begin{cases} x\equiv b_1 \pmod{m_1} \\ x\equiv b_2 \pmod{m_2} \\ \cdots \\ \cdots \\ x\equiv b_r \pmod{m_r} \end{cases}$$

在模 N 同余的意义下有唯一解。

证明：考虑方程组($1\leqslant i\leqslant r$)：

$$\begin{cases} x\equiv 0 \pmod{m_1} \\ \cdots \\ x\equiv 0 \pmod{m_{i-1}} \\ x\equiv 1 \pmod{m_i} \\ x\equiv 0 \pmod{m_{i+1}} \\ \cdots \\ \cdots \\ x\equiv 0 \pmod{m_r} \end{cases}$$

除m_i外其它位置要求整除

由于诸 m_i($1\leqslant i\leqslant r$)两两互素，这个方程组作变量替换，令 $x=(N/m_i)*y$，方程组等价于解同余方程：$(N/m_i)y\equiv 1 \pmod{m_i}$，若要得到特解 y_i，只要令：$x_i=(N/m_i)*y_i$，则方程组的解为：$x_0=b_1x_1+b_2x_2+\cdots+b_rx_r \pmod N$，在模 N 意义下唯一。

中国剩余定理就是用来求解“模线性方程组”的解，即：

$a\equiv B[1] \pmod{W[1]}$

$a\equiv B[2] \pmod{W[2]}$

…

$a \equiv B[n] (\bmod W[n])$

其中：W, B 已知，$W[i]>0$ 且 $W[i]$ 与 $W[j]$ 互质，求 a。

【参考程序】

中国剩余定理：

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

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

其中 $M_i = M/m_i$，而 M_i^{-1} 为 M_i 模 m_i 的逆元。

参考代码

```
// 中国剩余定理模板
int China(int W[],int B[],int k)// W[]为按多少排列，B[]为剩余个数，W>B,k为组数
{
    int x,y,a=0,m,n=1;
    for(int i=0;i<k;i++)// 算出它们累乘的结果
        n*=W[i];
    for(int i=0;i<k;i++)
    {
        m=n/W[i];
        exgcd(W[i],m,x,y);// 计算逆元
        a=(a+y*m*B[i]%n;
    }
    if (a>0)
       return a;
    else
       return a+n;
 }
```

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 *x* 使它满足：

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

那么 ***x*1** 和 ***x*2** 就要尽可能的小，于是我们用扩展欧几里得算法求出 ***x*1** 的最小正整数解，将它代回 ***a*1 +*m*1∗ *x*1** ，得到 ***x*** 的一个特解 ***x*'**，当然也是最小正整数解。

所以 ***x*** 的通解一定是 ***x*'** 加上***lcm*(*m*1,*m*2)∗*k*** ，这样才能保证 ***x*** 模 ***m*1** 和 ***m*2** 的余数是 ***a*1** 和 ***a*2** 。由此，我们把这个 ***x*'** 当做新的方程的余数，把 ***lcm*(*m*1,*m*2)** 当做新的方程的模数。（这一段是关键。）

合并完成：

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

参考资料

《数论概论》第11章《欧拉φ函数与中国剩余定理》

《数学一本通》第1.5节《中国剩余定理》

中国剩余定理学习笔记

http://www.cnblogs.com/walker01/archive/2010/01/23/1654880.html

http://blog.csdn.net/acdreamers/article/details/8050018