中国剩余定理

主讲人：邓哲也

线性同余方程组

从现在开始我们将会讨论线性同余方程组。

第一种：有两个以上的不同模的一元线性同余方程；

第二种：变元数大于 1，方程数大于 1，但是方程的模相同。

中国剩余定理的引入

下面取自成书于公元 3 世纪晚期的《孙子算经》的问题。

求一个数，它被 3 除余 1，被 5 除余 2，被 7 除余 3。

这也就等价于如下方程组：

$$x \equiv 1 \pmod 3$$

$$x \equiv 2 \pmod 5$$

$$x \equiv 3 \pmod 7$$

中国剩余定理

设 m_1，m_2，…，m_r 是两两互素的正整数，则同余方程组

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\cdots$$
$$x \equiv a_r \pmod{m_r}$$

有模 $M = m_1 m_2 \cdots m_r$ 的唯一解。

中国剩余定理

首先我们构造同余方程组的一个联立解。

令 $M_k = M / m_k = m_1 m_2 \cdots m_{k-1} m_{k+1} \cdots m_r$

由于 $(M_k, m_k) = 1$，因此可以求得 M_k 模 m_k 的一个逆 y_k。

所以 $M_k y_k \equiv 1 \pmod{m_k}$

现在构造一个

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_r M_r y_r$$

x 就是这 r 个同余方程的联立解。

中国剩余定理

$$x = a_1M_1y_1 + a_2M_2y_2 + \cdots + a_rM_ry_r$$

正确性显然。

还需要证明唯一性。

如果 x_0 和 x_1 都是解。

那么 $x_0 \equiv x_1 \equiv a_k \pmod{m_k}$，所以 $m_k \mid (x_0 - x_1)$

因此 $M \mid (x_0 - x_1)$

故 $x_0 \equiv x_1 \pmod{M}$

中国剩余定理

$$x \equiv 1 \pmod 3$$

$$x \equiv 2 \pmod 5$$

$$x \equiv 3 \pmod 7$$

现在回到开头的那个方程组，首先有 $M = 105$

$M_1 = 35$，$M_2 = 21$，$M_3 = 15$

$y_1 = 2$，$y_2 = 1$，$y_3 = 1$

因此 $x \equiv 1 * 35 * 2 + 2 * 21 * 1 + 3 * 15 * 1$

$\equiv 157$

$\equiv 52 \pmod{105}$

迭代法

$$x \equiv 1 \pmod 5$$

$$x \equiv 2 \pmod 6$$

$$x \equiv 3 \pmod 7$$

由第一个等式得到 $x = 5t + 1$，其中 t 是整数

把这个表达式带入第二个同余方程，得到

$$5t + 1 \equiv 2 \pmod 6$$

解出 $t \equiv 5 \pmod 6$

因此有 $t = 6u + 5$

所以 $x = 5(6u+5)+1 = 30u + 26$

迭代法

$$x \equiv 1 \pmod 5$$

$$x \equiv 2 \pmod 6$$

$$x \equiv 3 \pmod 7$$

把 $x = 30u + 26$ 带入第三个方程，得到

$$30u + 26 \equiv 3 \pmod 7$$

解得 $u \equiv 6 \pmod 7$

说明 $u = 7v + 6$

那么 $x = 30u + 26 = 30(7v + 6) = 210v + 206$

也即 $x \equiv 206 \pmod{210}$

下节课再见