CHINESE REMAINDER THEOREM

余晨宁 151242062

问题描述

- 向小伙伴们介绍中国剩余定理

中国剩余定理

- 令 $n = n_1 n_2 n_3 \cdots n_k$，其中因子 n_i 两两互质。
- 则存在映射关系：$a \leftrightarrow (a_1, a_2, \cdots, a_k)$
- 其中 $a \in Z_n$，$a_i \in Z_{n_i}$，而且对于 $i = 1, 2, \cdots, k$
- 有 $a_i = a \bmod n_i$

举例

- 对于n=6;n1=2,n2=3:
- 0对应(0,0)
- 1对应(1,1)
- 2对应(0,2)
- 3对应(1,0)
- 4对应(0,1)
- 5对应(1,2)

PROOF

- 证明这是一个双射的映射的思路：
- 1　先证明 $a \to (a_1, a_2, \cdots, a_k)$
- 2　再证明 $a \leftarrow (a_1, a_2, \cdots, a_k)$

$a \to (a_1, a_2, \cdots, a_k)$

- 执行k次模运算即可

$a \leftarrow (a_1, a_2, \cdots, a_k)$

- 定义 $m_i = n/n_i$ ，即 $m_i = n_1 n_2 \cdots n_{i-1} n_{i+1} \cdots n_k$
- 由于 $n_1, n_2, \cdots, n_{i-1}, n_{i+1}, \cdots, n_k$ 均与 n_i 互质，
- 则 $gcd(m_i, n_i) = 1$，即存在 ${m_i}^{-1} \bmod n_i$
- 定义 $c_i = m_i({m_i}^{-1} \bmod n_i)$
- 则计算 a 的方式如下：

$$a \equiv (a_1 c_1 + a_2 c_2 + \cdots + a_k c_k)(mod\ n)$$

$a \equiv (a_1c_1 + a_2c_2 + \cdots + a_kc_k)(mod\ n)$

现在证明对 $i = 1, 2, \cdots, k$ **，**

上面的等式能保证 $a \equiv a_i(mod\ n_i)$

- 由于 $m_i = n/n_i$ ，则对于 $\forall j \neq i, m_j = 0(mod\ n_i)$
- 又 $c_i = m_i(m_i{}^{-1} \bmod n_i)$
- 则 $$\begin{aligned} a &\equiv (a_1c_1 + \cdots + a_kc_k) && (mod\ n_i) \\ &\equiv c_ia_i && (mod\ n_i) \\ &\equiv a_im_i(m_i^{-1} \bmod n_i) && (mod\ n_i) \\ &\equiv a_im_im_i^{-1} && (mod\ n_i) \\ &\equiv a_i && (mod\ n_i) \end{aligned}$$

- 则对 $i = 1, 2, \cdots, k$ ，用从 a_i 计算 a 的方法，
- 得到了满足 $a \equiv a_i \pmod{n_i}$ 约束条件的结果 a .
- 由于此变换是双向的，因此，这种映射关系是一一对应的，即为双射。

中国剩余定理的一些应用

- 题目1:如果 $n_1, n_2, \cdots, n_k$两两互质，且 $n = n_1 n_2 n_3 \cdots n_k$，证明对所有整数 x 和 a，

$$x_i \equiv a(mod\ n_i)$$

当且仅当

$$x \equiv a(mod\ n)$$

- 解答:
- from $x \equiv a(mod\ n)$ to $x_i \equiv a(mod\ n_i)$:

$$x_i \equiv x \equiv (a\ mod\ n) \equiv a - kn \equiv a(mod\ n_i)$$

- from $\forall i, x_i \equiv a(mod\ n_i)$ to $x \equiv a(mod\ n)$:

根据剩余定理立刻可知。

- 题目2:一个数被3除余2，被7除余4，被8除余5，这个数最小是几?
- 解答：

$$
\begin{aligned}
c_1 &= 56 * 2 = 112, \\
c_2 &= 24 * 5 = 120, \\
c_3 &= 21 * 5 = 105. \\
x &\equiv 2 * 112 + 4 * 120 + 5 * 105 \equiv 53 (mod\ 168)
\end{aligned}
$$

没了，谢谢