中国剩余定理及其拓展

Ⅰ. 中国剩余定理：

一. 定理内容：

对于线性同余方程组 $(S):\begin{cases} x \equiv a_1 (Mod\ m_1) \\ x \equiv a_2 (Mod\ m_2) \\ \cdots \\ x \equiv a_n (Mod\ m_n) \end{cases}$，其最小整数解 $x = \sum_{i=1}^{n} a_i \cdot t_i \cdot M_i$。

其中，$M_i = \frac{\prod_{j=1}^{n} m_j}{m_i}$，$t_i \cdot M_i \equiv 1 (Mod\ m_i)$，且 m_i 两两互质

二. 定理证明：

我们不妨将 x 拆开，对于第 i 号方程有：

$$x = \sum_{i=1}^{n} a_i \cdot t_i \cdot M_i = a_1 \cdot t_1 \cdot M_1 + a_2 \cdot t_2 \cdot M_2 + \cdots + a_n \cdot t_n \cdot M_n = a_i \cdot t_i \cdot M_i = a_i (Mod\ m_i)$$

得证。

三. 代码参考：http://paste.ubuntu.com/23048720/[1]

四. 该算法的局限性：

a) 如果不考虑使用高精度/JAVA 的话，该算法中的 M_i 会受到 long long 的数据范围的限制，所以方程组数不能太多

b) m_i 两两互质。如果 m_i 与 m_j 不互质的话，则 a_i 与 a_j 便会相互影响

Ⅱ. 求解一般线性同余方程：

一. 算法中心思想：

a) 将 $\begin{cases} x \equiv a_1 (Mod\ m_1) \\ x \equiv a_2 (Mod\ m_2) \end{cases}$ 合并为 $x \equiv a_1 + k_1 \cdot m_1 (Mod\ \frac{m_1 \cdot m_2}{GCD(m_1, m_2)})$，其中

[1] 配套例题：http://poj.org/problem?id=1006

$$k_1 \cdot m_1 - k_2 \cdot m_2 = a_2 - a_1$$

b) 不断合并方程，至只剩下一个方程时，直接得出答案

二. 算法证明：

a) $\begin{cases} x \equiv a_1 (Mod\ m_1) \\ x \equiv a_2 (Mod\ m_2) \end{cases} \rightarrow x = a_1 + k_1 \cdot m_1 = a_2 + k_2 \cdot m_2 \rightarrow k_1 \cdot m_1 - k_2 \cdot m_2 = a_2 - a_1$

b) 使用拓展欧几里得算法，不难求出 k_1 的一个可行解，也可以得到 k_1 的通解为

$$k_1 + \frac{m_2}{GCD(m_1, m_2)} \cdot h \quad (h \in Z^*)$$ [2]

c) 带回 $x = a_1 + k_1 \cdot m_1$ 得•

三. 代码参考[3]：http://paste.ubuntu.com/23048785/[4]

四. 该算法的局限性

a) 不难发现，m_i 将会以指数级别增大，所以其也会受到 long long 在数据范围上的限制

Ⅲ. Reference：

一. Wikipedia：https://en.wikipedia.org/wiki/Chinese_remainder_theorem

二.《算法竞赛入门经典•第二版》

[2] 参见《算法竞赛入门经典 第二版》第 313 页

[3] 代码实现上，这里给出的是 O(sqrt(n)*log(n))的代码，可以做到 O(sqrt(n))但因为不是很直观，所以这里不提供代码

[4] 配套例题：http://poj.org/problem?id=2891