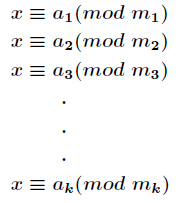
**中国剩余定理（CRT）**的表述如下

设正整数http://img.blog.csdn.net/20140618184134796两两互素，则同余方程组



有整数解。并且在模http://img.blog.csdn.net/20140618184354156下的解是唯一的，解为

http://img.blog.csdn.net/20140618184502609

其中http://img.blog.csdn.net/20140618184601062，而http://img.blog.csdn.net/20140618184638140为http://img.blog.csdn.net/20140618184737359模http://img.blog.csdn.net/20140904164235549的逆元。

如果只有一个方程：x mod a0 = r0。那么，显然x的最小正值为a0+r0。

根据模的性质，我们容易得知，x+a0\*k均为该方程的解。(k为正整数)

如果多了一个方程：x mod a1 = r1。那么，我们为了使之间求得的解x0=a0+r0能够同时满足这两个方程，只好令x0=x0+a0\*k，显然这样做x0仍然满足第一个方程。这时候我们相当于要求解这样一个模方程：(x0+a0\*k) mod a1 = r1。这个方程我们可以用拓展欧几里得算法求得k的值。这样，只要令x0变成x0+a0\*k，就能同时满足这两个方程了。

推而广之，对于方程x mod ai = ri，假如我们之前求得的解为X，那么我们要令X变成X+k\*LCM(a0,a1,a2...ai-1)，使得它满足这个方程。k我们可以用拓展欧几里得 算法求解，LCM可以在每一次更新，这样就能在接近O(klogk)的时间复杂度内解决这个问题了。