zklcdc的传说题解

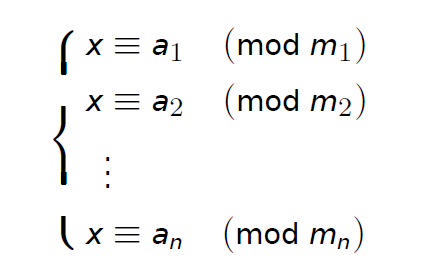
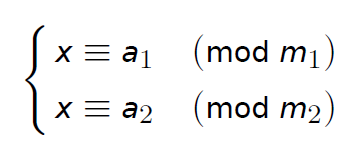
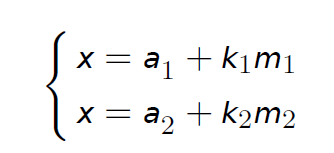
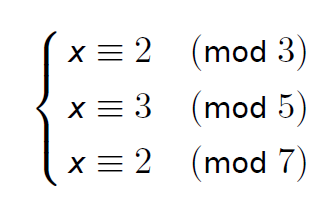
扩展欧几里得

* 现在我们要来求方程*ax* + *by* = gcd(*a, b*) 的整数解，首先根据裴蜀定理（自行百度）我们知道它肯定存在解。此外，按照先前计算最大公因数时用到的方程，*bx′*+ (*a* mod *b*)*y′*= gcd(*a, b*) 同样存在整数解。
* 同时，*a* mod *b* = *a – b\* (a/b)*，再将上面两个方程联立可以得到*ax* + *by* = *bx′*+ (*a-b\*(a/b))\*y′*
* 按照a 和b 进行合并之后

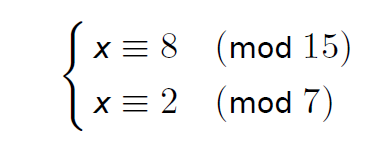
*ax* + *by* = *ay′*+ *b*(*x′- a/b\*y′)*

* 如果已经知道了(*x′, y′*)，那么在满足下式的情况下方程成立。那么
* x= *y′*
* *y=x’-a/b\*y’*
* 这样就可以利用方程*bx′*+ (*a* mod *b*)*y′*= gcd(*a, b*) 的整数解(*x′, y′*) 来计算出方程*ax* + *by* = gcd(*a, b*) 的整数解了。
* 最后只要按照前面计算最大用因数的方法，在递归的过程中加入x 和y 的计算就可以了。当递归到末尾的时候b 变为0，这是方程有整数解*x* = 1*; y* = 0。

中国剩余定理

* 中国剩余定理，又称为~~中国单身狗定理~~孙子定理，常常简写成CRT（Chinese Remainder Theorem）。
* 它给出了构造如下方程组解的方法：
* 
* 其中*m*1*, m*2,…,*m*n两两互素。
* 首先来解只有两个方程的方程组。
* 
* 我们可以把这个方程组改写成
* 
* 消去x 之后就可以得到*a*1 + *k*1*m*1 = *a*2 + *k*2*m*2，这刚好是关于*k*1*, k*2 的一个线性方程，使用刚刚的扩展欧几里得算法就可以解出。
* 此外，中国剩余定理还告诉我们一个事实，在*m*1*,m*2 互素的条件下，假设*x*0是该方程组的一个解，那么该方程组的所有解都满足如下形式：
* *x≡x*0 (mod *m*1*m*2)
* 这样我们相当于把刚刚的两个方程合并成为了一个方程。如果有多个方程，可以不断进行这样的合并，最后就可以解出结果了。
* 我们来拿刚刚开头的例子来试着算一算。那个方程组是：
* 
* 首先来合并前两个方程，联立后得到的线性方程是
* 2 + 3*k*1 = 3 + 5*k*2，
* 整理后可以得到一组解是*k*1 = 2*, k*2 = 1，这样可以得到满足前两个方程的x 都满足：

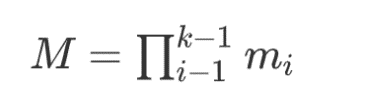
*x≡*8 (mod 15)

* 之后可以得到新的方程组：
* 
* 再合并两个方程，联立后得到的线性方程是
* 8 + 15*k*1 = 2 + 7*k*2，整理后可以得到一组解是
* *k*1 = 1*, k*2 = 3，
* 这样可以得到满足这两个方程的x 都满足：
* *x≡*23 (mod 105)

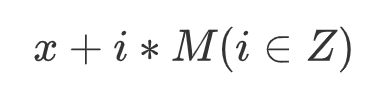
这便是最后的解了！

题目讲解

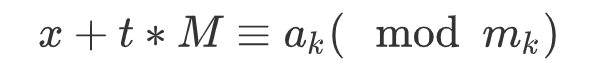
假设已经求出前k-1个方程组成的同余方程组的一个解为x

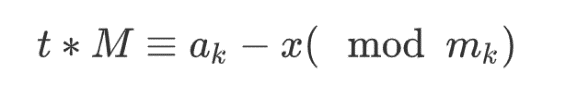
且有

（补充：代码实现中用的就是，这样是对，还更能防止溢出）

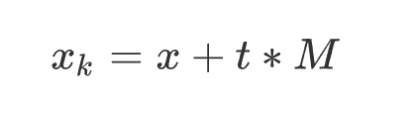
则前k-1个方程的方程组通解为

那么对于加入第k个方程后的方程组

我们就是要求一个正整数t，使得

转化一下上述式子得

对于这个式子我们已经可以通过扩展欧几里得求解t

若该同余式无解，则整个方程组无解， 若有，则前k个同余式组成的方程组的一个解解为

所以整个算法的思路就是求解**k次扩展欧几里得**

**具体可参见洛谷P4777题**