# 中国剩余定理

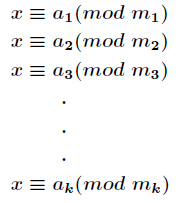
中国剩余定理解决了什么问题：

有个数未知X，它除3余2，除5余3，除7余2。求这个数

其实可以知道 X%3=2 X%5=3 X%7=2

那么X=T1\*3+2=T2\*5+3=T3\*7+2

中国剩余定理适用，条件要求整数http://img.blog.csdn.net/20140618184134796两两互素



上述同余方程等价于：

X%m1=a1%m1

X%m2=a2%m1

X%m3=a3%m1

…………………………

X%mk=ak%m1

已知余数ai和除数mi，求X

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(这里注意，是对mi取逆元)。

解步骤是：

设http://img.blog.csdn.net/20140618184354156 Mi=M/mi;

分别求出逆元=inv(Mi,mi) 时间复杂度n\*logP P是pi平均值

# 解模数不互质情况下的线性方程组：

上面提到mi必须两两互质，那不互质呢？也是能求，下面是所有同余方程任意的两个

http://img.blog.csdn.net/20140618185529953

http://img.blog.csdn.net/20140618185628671

https://images2015.cnblogs.com/blog/994344/201609/994344-20160928225142250-925008424.png

需要求最小的x1和x2 使X尽可能小, 由于x1x1可以取负无穷到正无穷，所以符号不能约束它们, 能得到的m1\*x1+m2\*x2=a2-a1

我们已知a1 a2 m1 m2 扩展欧几里得解这个方程求得x1和x2特解，然后再写出x1或x2的通解表达式。

比如说x1=x0+m2/g\*t t∈ Z g代表gcd(m1,m2);

带回http://img.blog.csdn.net/20140618185529953

x=a1+m1\*x0+m1\*m2\*t/g这个式子里只有x和t是未知数

现在令m=m1\*m2/g 上述式子两边对m取模，变换成

x%m=( a1+m1\*x0)%m 设a=a1+m1\*x0 得到x%m=a%m

注意到这式子个又是同余方程，一番扩展欧几里得之后，相当于把2个同余方程和为一个，这样就有了思路：按顺序计算前2个方程，合并成1个，再用合并的方程与第三个合并，如此循环直到合并了所有的方程，最后一次合并后，

x=a1+m1\*x0+m1\*m2\*t/g这个式子里，取适当的t，就能得到最小正整数解

时间复杂度是n\*logn logn是扩展欧几里得的时间复杂度