中国剩余定理

CRT：Chinese Remainder Theorem

引例

今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？

解： 问题归结为求解下列方程组

$$\begin{cases} X \equiv 2 \bmod 3 \\ X \equiv 3 \bmod 5 \\ X \equiv 2 \bmod 7 \end{cases}$$

中国剩余定理

中国剩余定理

设$W_1,W_2,\ldots$，W_k是**两两互质**的**正整数**，
即$gcd(W_i,W_j)=1$， $i\neq j$，$1<=i, j=k$，则下面方程组有**惟一**解：

$$\begin{cases} X\equiv b_1 \bmod W_1 & //表示X\ \%\ W_1==b_1 \\ X\equiv b_2 \bmod W_2 & //表示X\ \%\ W_2==b_2 \\ \ldots\ldots & \\ X\equiv b_k \bmod W_k & //表示X\ \%\ W_K==b_K \end{cases}$$

上面方程组的解为：

$$X=(M_1*M_1^{-1}*b_1 + M_2*M_2^{-1}*b_2 +\ldots+ M_k*M_k^{-1}*b_k\ ) \bmod P$$

其中：$P = W_1*W_2*\ldots*W_k$

$M_i = P / W_i$

M_i^{-1}是M_i模W_i的乘法逆元　　即$M_i*M_i^{-1} \equiv 1 \bmod W_i$

例1

今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？

解： 问题归结为求解下列方程组

$$\begin{cases} X \equiv 2 \bmod 3 \\ X \equiv 3 \bmod 5 \\ X \equiv 2 \bmod 7 \end{cases}$$

b_i W_i

$$\begin{cases} X \equiv 2 \bmod 3 \\ X \equiv 3 \bmod 5 \\ X \equiv 2 \bmod 7 \end{cases}$$

$$X=(M_1*M_1^{-1}*b_1 + M_2*M_2^{-1}*b_2 +\ldots+ M_k*M_k^{-1}*b_k\ ) \% P$$

$P = W_1*W_2*\ldots*W_k$

$M_i = P / W_i$

$M_i*M_i^{-1} \% W_i==1$

$P = w_1*w_2*w_3 =3*5*7=105$

$M_1= P / w_1 =105/3=35$

$M_2= P / w_2 =105/5=21$

$M_3= P / w_3 =105/7=15$

$M_1*M_1^{-1} \% W_1 ==1$

$M_2*M_2^{-1} \% W_2 ==1$

$M_3*M_3^{-1} \% W_3 ==1$

即：$35*M_1^{-1} \% 3==1$　　解得：$M_1^{-1} = 2$

$21*M_2^{-1} \% 5==1$　　$M_2^{-1} = 1$

$15*M_3^{-1} \% 7==1$　　$M_3^{-1} = 1$

$$X=(M_1*M_1^{-1}*b_1 + M_2*M_2^{-1}*b_2 + M_3*M_3^{-1}*b_3\ ) \% P$$

$=(70*b_1 + 21*b_2 + 15*b_3)\%105$

$=(70*2+21*3+15*2) \% 105$

$=23 \% 105$

$=23$

例1

$M_i * M_i^{-1} \equiv 1 \bmod W_i$

已知M_i和W_i，怎样求M_i的逆元M_i^{-1}？

$a*x \equiv 1 \bmod c$，已知a和c,求x

求解 a*x-y*c=1

$M_i * M_i^{-1} - W_i * y == 1$

扩展欧几里德求解即可

中国剩余定理 参考代码

```
int China(int B[ ],int W[ ],int k)
{
    int i,d , x , y , ans=0 , Mi , P=1;
    for(i=1;i<=k;i++)  P*=W[i];
    for(i=1;i<=k;i++)
    {
        Mi=P/W[i];
        d=ext_euclid(Mi,W[i],x,y);          //扩欧求Mi的逆元
        ans=(ans+x*Mi*B[i])%P;
    }
    if(ans>0)return ans;  else return(ans+P);
}
```

$X=(M_1*M_1^{-1}*b_1 + M_2*M_2^{-1}*b_2 +\ldots+ M_k*M_k^{-1}*b_k) \% P$

$P = W_1*W_2*\ldots*W_k$

$M_i = P / W_i$

$M_i*M_i^{-1} \% W_i==1$

例2：POJ1006 周期

人生来就有三个周期，分别为体力、感情和智力周期，它们的周期长度为23天、28天和33天。

每一个周期中有一天是高峰。在高峰这天，人会在相应的方面表现出色。因为三个周期的周长不同，所以通常三个周期的高峰不会落在同一天。

我们想知道何时三个高峰落在同一天。对于每个周期，我们会给出从当前年份的第一天开始，到出现高峰的天数（不一定是第一次高峰出现的时间）。你的任务是给定一个从当年第一天开始数的天数，输出从指定时间开始（不包括指定时间）下一次三个高峰落在同一天的时间。

例如：指定时间为10，下次出现三个高峰同天的时间是12，则输出2。

输入：

四个整数：a, b, c和d。 a, b, c分别表示体力、情感和智力高峰出现的时间（时间从当年的第一天开始计算）。d 是给定的开始时间，可能小于a, b, 或 c。

输出：

从指定时间起，下一次三个高峰同天的时间。

POJ1006 周期 题目分析：

设 ans 是距离下一个三个高峰同天的天数，
a，b，c，d 如题中所设。
那么就可以得到三个式子：
(ans + d) % 23 == a ;
(ans + d) % 28 == b ;
(ans + d) % 33 == c ;
为方便计算，我们再设x=ans+d, 于是又如下式子：
x % 23 == a ;
x % 28 == b ;
x % 33 == c ;
因为23、28、33两两互质，
我们可以用中国剩余定理求解:

X=(M_1*M_1^{-1}*a + M_2*M_2^{-1}*b +M_3*M_3^{-1}*c) % P
P = 23*28*33=21252
M_1 = P / a=28*33=924
M_2 = P / b=23*33=759
M_3 = P / c=23*28=644
M_1*M_1^{-1} % 23==1 →M_1^{-1} =6
M_2*M_2^{-1} % 28==1 →M_2^{-1} =19
M_3*M_3^{-1} % 33==1 →M_2^{-1} =2

X=(924*6*a+759*19*b+644*2*c)%P
= (5544*a+14421*b+1288*c)%21252
ans=X-d
ans= (5544 * a + 14421 * b + 1288 * C - d + 21252) % 21252;

中国剩余定理 课后习题

作业：POJ 1006，
NKOJ 1668，3675
codeforces 710D
思维：NKOJ 4034

1668中国剩余定理代码

```
#include<iostream>
#include<cstdio>
using namespace std;
int w[4],b[4];
int MaxMax(int a,int b,int c){   return max(max(a,b),c);  }
int exgcd(int a,int b,int &x,int &y)
{
        int r,temp;
        if(!b)
        {
                x=1;y=0;
                return a;
        }
        r=exgcd(b,a%b,x,y);
        temp=x;
        x=y;
        y=temp-a/b*y;
}
int china(int b[],int w[],int k)
{
        int i,d,x,y,ans=0,p=1,m[4];
        for(i=1;i<=k;i++)p*=w[i];
        for(i=1;i<=k;i++)
        {
                m[i]=p/w[i];
                d=exgcd(m[i],w[i],x,y);
                ans=(ans+x*m[i]*b[i])%p;
        }
        while(ans<MaxMax(w[1],w[2],w[3]))ans+=p;
        return ans;
}
int main()
{
        scanf("%d%d%d%d%d%d",&w[1],&b[1],&w[2],&b[2],&w[3],&b[3]);
        printf("%d",china(b,w,3));
}
```

奋斗吧少年

巨大的成功需要付出巨大的代价

no sacrifice, no success