# 第3次编程练习报告

姓名：齐明杰 学号：2113997 班级：信安二班

##### 编程练习3——中国剩余定理

* **源码部分：**
* #include <bits/stdc++.h>
* #define MAXN 10000
* **using** **namespace** std;
* **int** b[MAXN], m[MAXN];
* **int** inverse(**int** a,**int** m){
* **int** r, q, s1 = 1, s2 = 0, s3, t1 = 0, t2 = 1, t3 = 1, mt = m;
* **while**(1){
* r = m%a; q = m/a;
* **if**(!r) **break**;
* m = a; a = r;
* s3 = s1 - q\*s2;
* t3 = t1 - q\*t2;
* s1 = s2; s2 = s3;
* t1 = t2; t2 = t3;
* }
* **while**(t3 < 0) t3 += mt;
* **return** t3;
* }
* **int** main(){
* **int** n, an = 0, am = 1;
* printf("n="); scanf("%d", &n);
* **for**(**int** i=0;i<n;i++){
* printf(" b\_%d=",i);
* scanf("%d", &b[i]);
* }
* **for**(**int** i=0;i<n;i++){
* printf(" m\_%d=",i);
* scanf("%d", &m[i]);
* am \*= m[i];
* }
* **for**(**int** i=0;i<n;i++){
* **int** mul = am/m[i];
* **int** re\_mul = inverse(mul, m[i]);
* an += re\_mul \* mul \* b[i];
* }
* printf("x≡%d (mod %d)", an % am, am);
* **return** 0;
* }
* **说明部分：**

由于同余方程组均满足x≡bi(mod mi)的形式，故开两个数组(大小取MAXN，即n可能的最大值)来存储每个bi和mi。

int inverse(int a,int m)函数用于求正整数a模m的逆元，采用拓展欧几里得算法进行求解，即不断循环计算余数r和商q，同时带入公式s3=s1-q\*s2，t3=t1-q\*t2中，最终在r=0时得到的结果t3即为所求。但t3有可能为负数，因此采用while循环加为正数。

在main函数中，我们循环读入d[i]和m[i]，同时设置一个变量int am，用于计算m0\*m1\*m2……\*m(i-1)的值(即公式中的m).

根据下图公式，采用一个for循环累加求值。



其中，Mi对应代码中的int mul，Mi’对应代码中的int re\_mul,即Mi模m[i]的乘法逆元。求出逆元后an += Mi\*Mi’\*b[i]，如此进行n轮，最终an为上图等号右边的值。但an有可能过大，故输出的时候取an % am。

* **运行示例：**



