# 第3次编程练习报告

姓名：孙蕗 学号：2112060 班级：信安一班

##### **编程练习1——中国剩余定理**

* **源码部分：**

#include<iostream>

using namespace std;

int Inverse(int a, int b)//扩展欧几里得定理求逆元

{

int s[100], t[100], q[100], r[100];

s[0] = 1;

t[0] = 0;

s[1] = 0;

t[1] = 1;

r[0] = a;

r[1] = b;

q[0] = 0;

q[1] = a / b;

int i = 2;

while (true)

{

r[i] = r[i - 2] % r[i - 1];

//cout << "r" << i << "=" << r[i] << endl;

if (r[i] == 0)

{

break;

}

q[i] = r[i - 1] / r[i];

//cout << "q" << i << "=" << q[i] << endl;

s[i] = s[i - 2] - s[i - 1] \* q[i - 1];

//cout << "s" << i << "=" << s[i] << endl;

t[i] = t[i - 2] - t[i - 1] \* q[i - 1];

//cout << "t" << i << "=" << t[i] << endl;

i++;

//cout << endl;

}

return s[i - 1];

}

int main()

{

int n;

cout << "n=";

cin >> n;

int\* b = new int[n];

int\* M = new int[n];

int\* M1 = new int[n];

for (int i = 0; i < n; i++)

{

M1[i] = 1;

}

int \*M\_=new int [n];

int m = 1;

for (int i = 0; i < n; i++)//输入b

{

cout << "b\_" << i << "=";

cin >> b[i];

}

for (int i = 0; i < n; i++)//输入mi

{

cout << "m\_" << i << "=";

cin >> M[i];

m \*= M[i];//计算m，累乘

}

//cout << m << endl;

for (int i = 0; i < n; i++)//求Mi

{

M1[i] = m / M[i];

}

//for (int i = 0; i < n; i++)//输出Mi

//{

// cout << M1[i] << " ";

//}

//cout << endl;

for (int i = 0; i < n; i++)//求Mi^-1

{

M\_[i] = Inverse(M1[i], M[i]);

if (M\_[i] < 0)

{

M\_[i] = M[i] + M\_[i];

}

}

//for (int i = 0; i < n; i++)//输出逆元

//{

// cout << M\_[i] << " ";

//}

//cout << endl;

int sum = 0;

for (int i = 0; i < n; i++)

{

sum += M\_[i] \* M1[i] \* b[i];

}

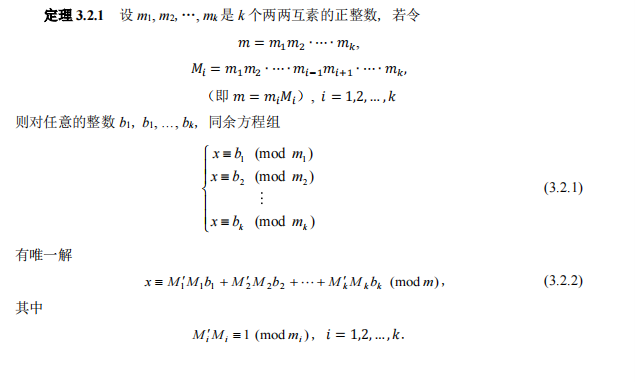
//cout << sum << endl;

cout << "x≡" << sum % m << "(mod " << m << ")" << endl;

}

* **说明部分：**

中国剩余定理：



int m = 1记录m，int\* b = new int[n]用来存bi,int\* M = new int[n]用来存mi,int\* M1 = new int[n]用来存Mi，int \*M\_=new int [n]用来存Mi的逆元。m通过累乘mk(k=1,2,…，k)可计算得到，Mi可以通过m/mi计算得到，Mi的逆元Mi’可以通过扩展欧几里得定理计算得到。方程的解为





* **运行示例：**

