第三次编程练习报告

姓名：张洋　　学号：2111460　　班级：信安二班

编程练习 1——编程实现中国剩余定理

```
#include<iostream>
using namespace std;
void swap(int& a, int& b) {
    int t = a;
    a = b;
    b = t;
}
int inverse(int x, int y) { //求x模y的乘法逆元
    int flag = 0; //记录是否交换x，y
    if (x < y) { //令x为较大的那一个
        flag = 1;
        swap(x, y);
    }
    //以下利用扩展欧几里得算法求乘法逆元
    int i = 1, s[100], t[100], r[100], q[100];
    r[0] = x;
    r[1] = y;
    s[0] = t[1] = 1;
    s[1] = t[0] = 0;
    while (r[i] != 0) { //当余数不为0时
        q[i] = r[i - 1] / r[i];
        s[i + 1] = s[i - 1] - q[i] * s[i];
        t[i + 1] = t[i - 1] - q[i] * t[i];
        i++;
        r[i] = r[i - 2] % r[i - 1];
    }
    if (flag == 1) {
        if (t[i - 1] < 0)
            return t[i - 1] + x;
        else
            return t[i - 1];
    }
    else {
        if (s[i - 1] < 0)
            return s[i - 1] + y;
        else
            return s[i - 1];
    }
```

```
}
int main() {
    int n; //同余方程的个数
    cout << "n=";
    cin >> n; //利用中国剩余定理求同余方程组的解
    int* b = new int[n],
        * m = new int[n],
        * a = new int[n],
        * a_inverse = new int[n];
    int mul = 1; //模的数的乘积 mul = m1*m2...*mn
    for (int i = 0; i < n; i++) {
        cout << " b_" << i << "=";
        cin >> b[i];
    }
    for (int i=0;i<n;i++){
        cout << " m_" << i << "=";
        cin >> m[i];
        mul *= m[i];
    }
    for (int i = 0; i < n; i++) {
        a[i] = 1;
        for (int j = 0; j < n; j++) { //计算除m[i]外的其他数的乘积放进a[i]中
            if (j == i)
                continue;
            a[i] *= m[j];
        }
        a_inverse[i] = inverse(a[i], m[i]); //求乘法逆元
    }
    int result = 0;
    for (int i = 0; i < n; i++)
        result += a_inverse[i] * a[i] * b[i];
    result %= mul;
    cout << "x≡" << result << " (mod " << mul << ")" << endl;
    system("PAUSE");
}
```

说明部分：

思路如下：设$m_1, m_2, \ldots\ldots, m_k$是 k 个两两互素的正整数，若令：

$$m = m_1 m_2 \cdot \cdots \cdot m_k,$$

$$M_i = m_1 m_2 \cdot \cdots \cdot m_{i-1} m_{i+1} \cdot \cdots \cdot m_k,$$

$$(\text{即 } m = m_i M_i), \quad i = 1,2,\ldots,k$$

则对任意的整数$b_1, b_2, \ldots\ldots, b_k$，同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \quad\quad \vdots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

有唯一解

$$x \equiv M_1' M_1 b_1 + M_2' M_2 b_2 + \cdots + M_k' M_k b_k \pmod{m},$$

其中

$$M_i' M_i \equiv 1 \pmod{m_i}, \quad i = 1,2,\ldots,k.$$

运行示例：

```
n=4
 b_0=1
 b_1=2
 b_2=4
 b_3=6
 m_0=3
 m_1=5
 m_2=7
 m_3=13
x≡487 (mod 1365)
请按任意键继续. . .
```