信安数基编程作业3报告

姓名：艾明旭 学号2111033

本次编程作业要求实现中国剩余定理，其核心内容是通过求每一个剩余组所对应的m1和m1’求得的数套用中国剩余定理的公式得到M，最终M取模得到了最终的计算结果。

其中求乘法逆元得部分可以用扩展欧几里得算法实际操作当中，如果计算的数量太小，这里采用了直接遍历的方法，在手算较小元素时可以采用，但更推荐扩展欧几里得算法可以应用于更广义的情况。

#include <iostream>

using namespace std;

const int Maxn = 1010;

int main()

{

int n;

cin >> n;

int m[Maxn], b[Maxn],a[Maxn],a0[Maxn],t[Maxn];

int x = 1,y=0;

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

{

cin >> b[i] >> m[i];

x \*= m[i];//x作为最终的除数

}

cout << "n=" << n << endl;

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

{

cout << " " << "b\_" << i << "=" << b[i] << endl;

cout << " " << "m\_" << i << "=" << m[i]<<endl;

a[i] = x / m[i];

for (int j = 1; j < m[i]; j++)

{

t[i] = a[i] \* j;

if (t[i] % m[i] == 1)

{

a0[i] = j;//用遍历的方法求出乘法逆元m1’，这里可以套用上一次作业的扩展欧几里得算法。

j = m[i];

}

}

}

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

{

y += a[i] \* a0[i] \* b[i];

y = y % x;

}

cout << "x≡" << y << " (mod " << x << ")";

}