**西安电子科技大学网信院**

**信息安全基础与密码学**

**综合实验**

**实 验 报 告（二）**

**中国剩余定理**

**班级：2218031**

**姓名：周仙辉**

**学号：22009201377**

**日期：2024-10-27**

一、实验目的（包括实验环境、实现目标等等）

实验环境：ubuntu22.04 c++

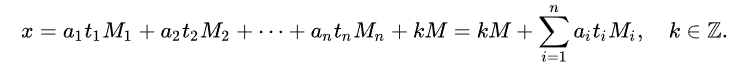
目标：求解大整数同余方程

二、方案设计

（包括背景、原理、必要的公式、图表、算法步骤等等）

背景：求解同余方程组

原理：中国剩余定理

公式：

在模M的意义下，方程组 化为

算法步骤：

(1)判断正整数m1,m2,…,mk是否两两互素;是,则继续,否则跳出,输出

“不能直接利用中国剩余定理”

(2) 计算m=m1m2…mk,Mj ;= m/mj;

(3) 计算Mj-1(modm));

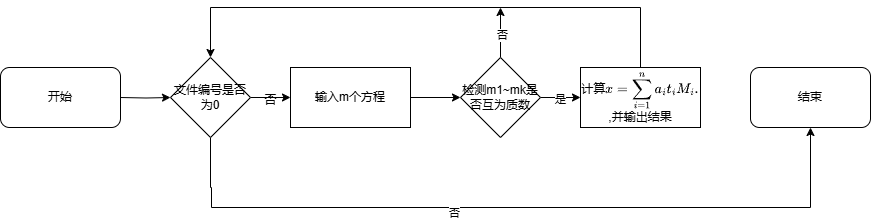
(4) 计算xj=Mj\*Mj-1 \* aj(mod m);

(5) 计算(mod m)。

三、方案实现

（包括算法流程图、主要函数的介绍、算法实现的主要代码等等）

算法流程图：



主要函数介绍：

int gcd(mpz\_class a,mpz\_class b);

主要实现欧几里得算法，用来判断是否互质。

mpz\_class extgcd(mpz\_class a,mpz\_class b,mpz\_class &x ,mpz\_class &y);

拓展欧几里得算法，用于计算模逆。

主要代码：

int main(){

int choice[4] = {2,4,0};

for(int i = 0; choice[i] ; i ++){

vector<mpz\_class> as,ms;

mpz\_class a,m;

string path = "./实验2的报告模板和数据/";

path.append(to\_string(choice[i]));

path.append(".txt");

cout << path << endl;

ifstream in(path);

// input

for(int i=0; i < 3 ; i++){

in >> a;

as.push\_back(a);

}

for(int i=0; i< 3; i++){

in >> m;

ms.push\_back(m);

}

// 判断互质

int flag = 1;

auto len = ms.size();

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

for(int j = i+1; j < len; j++)

{

if(gcd(ms[i],ms[j]) != 1){

cout << "不能直接利用中国剩余定理" << endl;

flag = 0;

break;

}

if(!flag)break;

}

if(!flag) continue;

// 计算m1\*...mk

mpz\_class sum = 1;

for(int i=0; i<len;i++) sum \*= ms[i];

mpz\_class x = 0;

for(int i = 0; i<len; i++){

mpz\_class M,M\_;

M = sum/ms[i]; // M 和 ms[i] 互质,可使用拓展欧几里得算法求m的逆

M\_ = inverse(M,ms[i]);

x = (x + M\_\*M % sum\*as[i] % sum ) % sum;

}

// 可能是负数

x = (x + sum)%sum;

cout << x << endl;

}

return 0;

}

四、数据分析(包括算法测试数据的分析，运行结果截图等等)

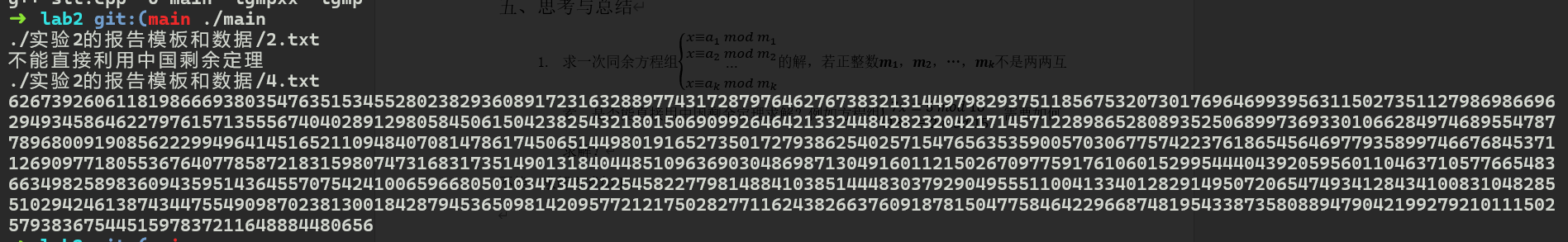
测试数据分析：

全是大整数，每个文件三个方程式。

运行结果截图：

编译指令：g++ slt.cpp -o main -lgmpxx -lgmp

选择2和4两个文件



五、思考与总结

1. 求一次同余方程组的解，若正整数𝒎𝟏，𝒎𝟐，…，𝒎𝒌不是两两互素，是否能直接用中国剩余定理求解？例如方程组，需要如何求解？

不能。求解方式如下：

1. 变形

转化为

然后就可以进行中国剩余定理了。

2.中国剩余定理

通过程序计算得到 29

1. 实验过程中还遇到了什么问题，如何解决的？通过该实验有何收获？

问题：C++取余结果可能为负数，需要取模在加模数，再取模。

**收获：了解了中国剩余定理，并使用它解决同余方程组。**

**实验报告提交说明**：

1. 实验报告同时提交word文档与源代码（.c或者.py）。
2. 实验报告与源代码命名规则：实验2-学号-姓名，例如：实验2-20009200400-张三。
3. 请于截止日期前在西电智课平台（学在西电）提交相关文档，逾期未提交，该部分成绩记为0分，周知。