**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：2018039**

**姓名：叶振雷**

**学号：20009101064**

**日期：2022.11.6**

一、实验目的（包括实验环境、实现目标等等）

1. 在屏幕上输入要输入的数组元素个数n，后输入两个元素个数为n的数组m[]、b[]，组成一个同余式组。  
   2.利用中国剩余定理求出同余式组的解并输出在屏幕上。

二、方案设计

（包括背景、原理、必要的公式、图表、算法步骤等等）

1.输入的数组m[]要满足两两互素的性质，若不满足则无法带入中国剩余定理中去，则先设计一个利用广义欧几里得除法判断两个数是否互素的函数，并在输入时判断数组是否两两互素：#我们称列表互素检验函数

*def* *mutual\_prime\_check*(m: list):

    size *=* len(m)

*for* i *in* range(size):

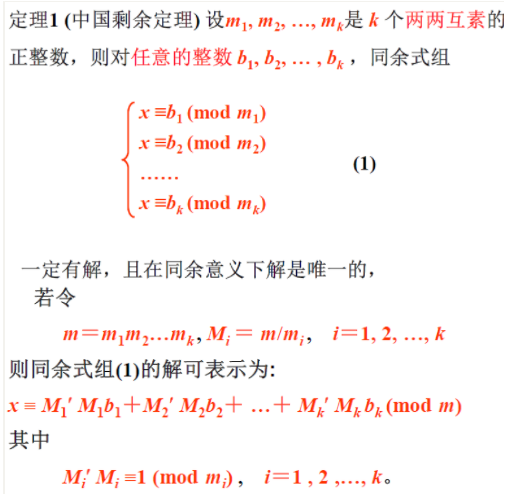
*for* j *in* range(i*+*1, size):

*if* gcd(m[i], m[j]) *!=* 1:

*return* False

*return* True

1. 主函数编写



根据此流程依次编写内容，本次实验每组均有三个方程，所以设置equation\_num=3

*def* *CRT*(a,m):

    equation\_num *=* 3

*for* i *in* range(len(a)):

        print("a",i,":",a[i])

*for* i *in* range(len(m)):

        print("m",i,":",m[i])

*if* *not* mutual\_prime\_check(m):  *# 互素检查*

        print("不能直接利用中国剩余定理")

        print()

*return*

*#求乘积*

    M *=* prod(m)

*#求Mj*

    Mj *=* [M*//*\_m *for* \_m *in* m]

*#求Mj的逆*

    inv\_Mj *=* [invert(M*//*\_m,\_m)*for* \_m *in* m]

    xj*=*[(Mj[j]*\**inv\_Mj[j]*\**a[j]) *%*  M *for* j *in* range(equation\_num)]

*# 输出x结果*

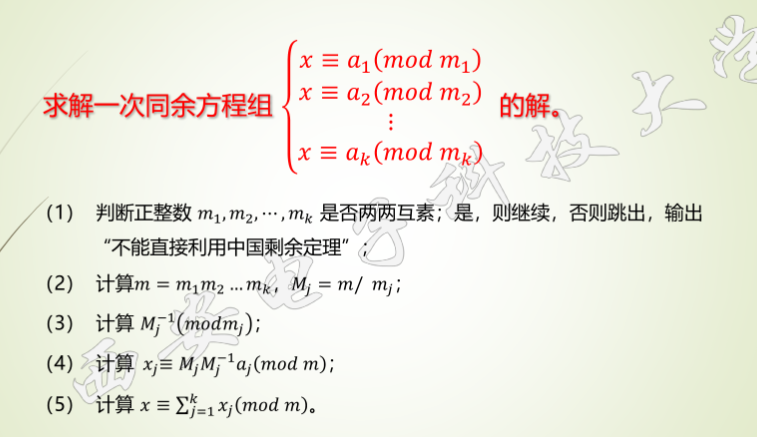
    print(*f*"解得：x ≡ {sum(xj) *%* M}(mod {M})")

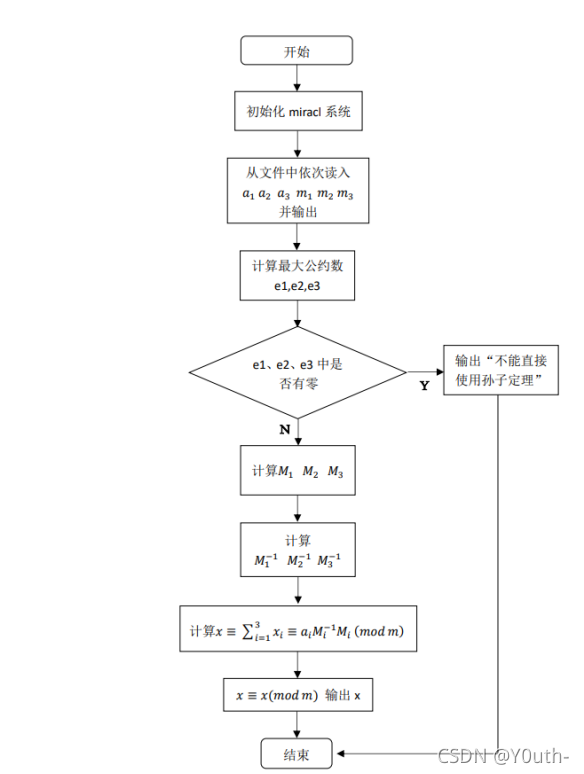
    print()

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）

算法流程图如下：





主要函数介绍：

一个函数用来判断列表元素是否互素，另一个则是直接使用中国剩余定理流程进行求解，里面使用了gmpy2库中的invert函数，以及math库中的gcd函数和prod函数，不必再自己手工编写，极大简化了程序的体量

实现的主要代码：

*#中国剩余定律*

*def* *CRT*(a,m):

    equation\_num *=* 3

*for* i *in* range(len(a)):

        print("a",i,":",a[i])

*for* i *in* range(len(m)):

        print("m",i,":",m[i])

*if* *not* mutual\_prime\_check(m):  *# 互素检查*

        print("不能直接利用中国剩余定理")

        print()

*return*

*#求乘积*

    M *=* prod(m)

*#求Mj*

    Mj *=* [M*//*\_m *for* \_m *in* m]

*#求Mj的逆*

    inv\_Mj *=* [invert(M*//*\_m,\_m)*for* \_m *in* m]

    xj*=*[(Mj[j]*\**inv\_Mj[j]*\**a[j]) *%*  M *for* j *in* range(equation\_num)]

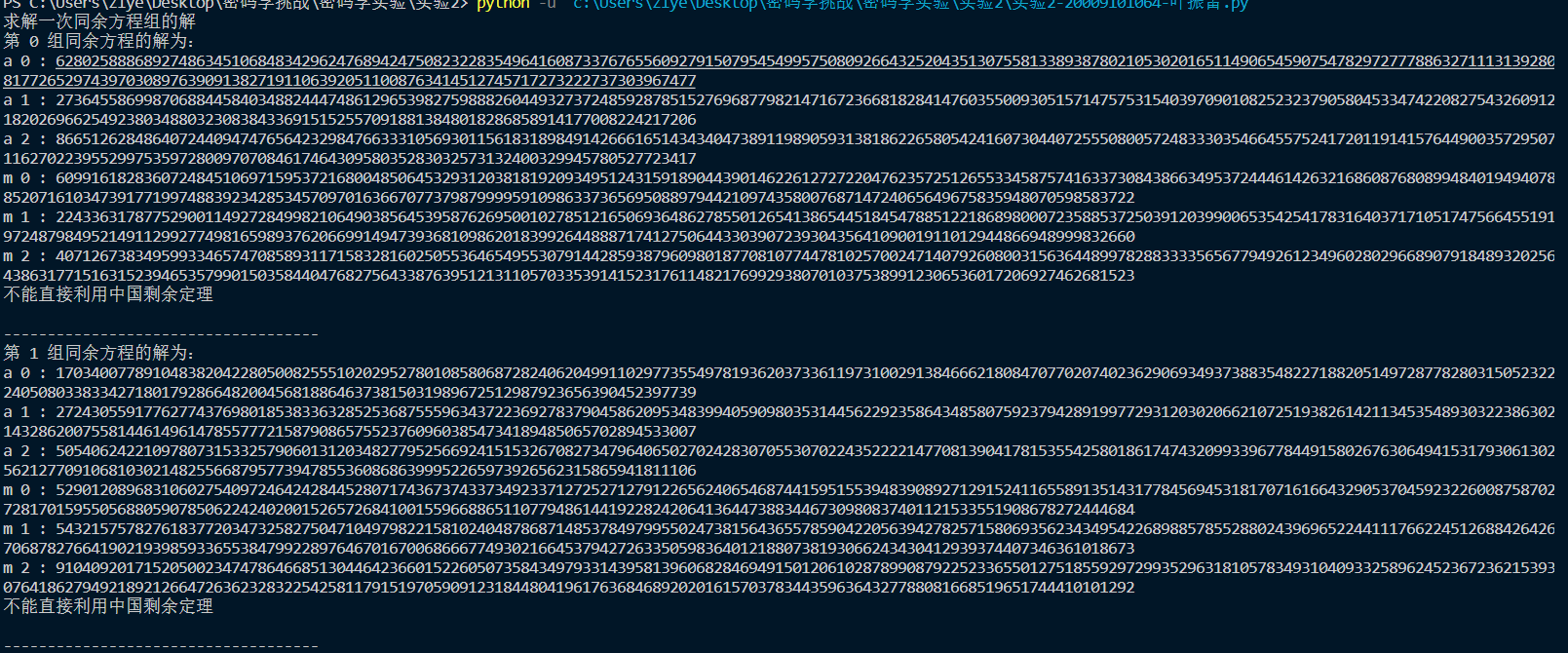
*# 输出x结果*

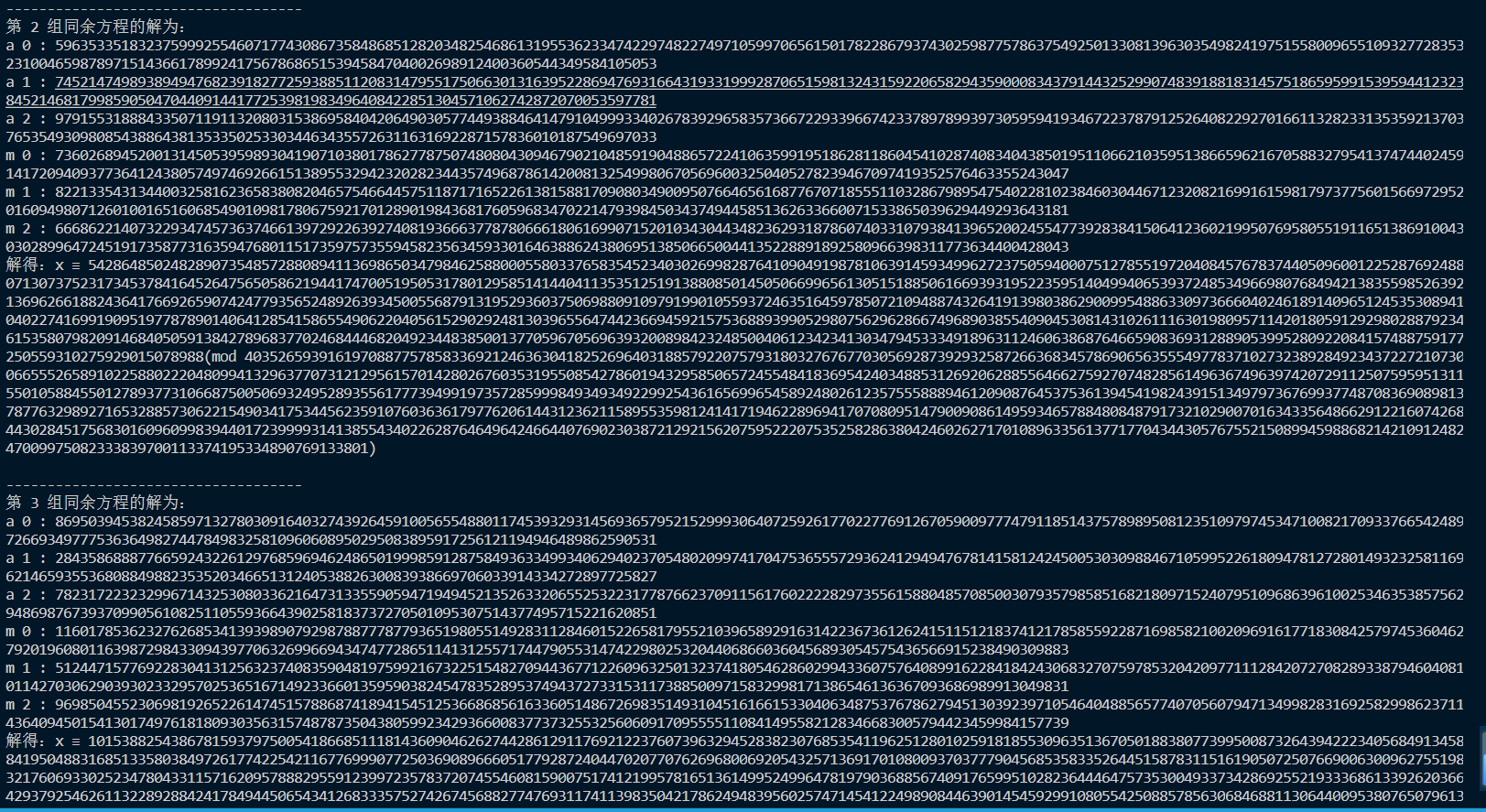
    print(*f*"解得：x ≡ {sum(xj) *%* M}(mod {M})")

    print()

1. 数据分析(包括算法测试数据的分析，运行结果截图等等)

第0、1组-无法使用中国剩余定理



第2、3组-结果如下

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？

不能直接求解，需要将𝒎𝟏，𝒎𝟐，…，𝒎𝒌进行分解至互素，将18分解为3和6，将15分解为3和5然后再进行求解。

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？

在求Mj的模逆过程中，发现手动编写没啥头绪，于是上网搜索了一下，发现gmpy有现成的函数invert可以用来求模逆。

1.通过算法编程，熟悉使用math、gmpy库的基本函数操作  
2.通过编程实现中国剩余定理，加深了对于中国剩余定理的理解与运用  
3.体会了密码学与数论的紧密联系  
4.提高了逻辑思维能力

**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。