《信息安全基础综合实验》课程实验报告

实验题目：Fermat 素性检验

班级：1918039　　学号 1：19180300017　　姓名 1：王申奥

班级：1918011　　学号 2：19180100060　　姓名 2：贺紫怡

班级：1918031　　学号 3：19180300025　　姓名 3：王乾旭

一、实验目的

（包括实验环境、实现目标等等）

实验环境：python3.8

实现目标：大数的费马素性检测

二、方案设计

（包括背景、原理、必要的公式、图表、算法步骤等等）

原理：Fermat 小定理

给定素数 p，a∈Z，则有$a^{p-1} \equiv 1(mod\ p)$

算法步骤：

给定奇整数 m≥3 和安全参数 k

（1） 随机选取整数 a，2≤a≤m-2

（2） 计算 g=（a,m），如果 g=1，转（3）；否则，跳出，m 为合数

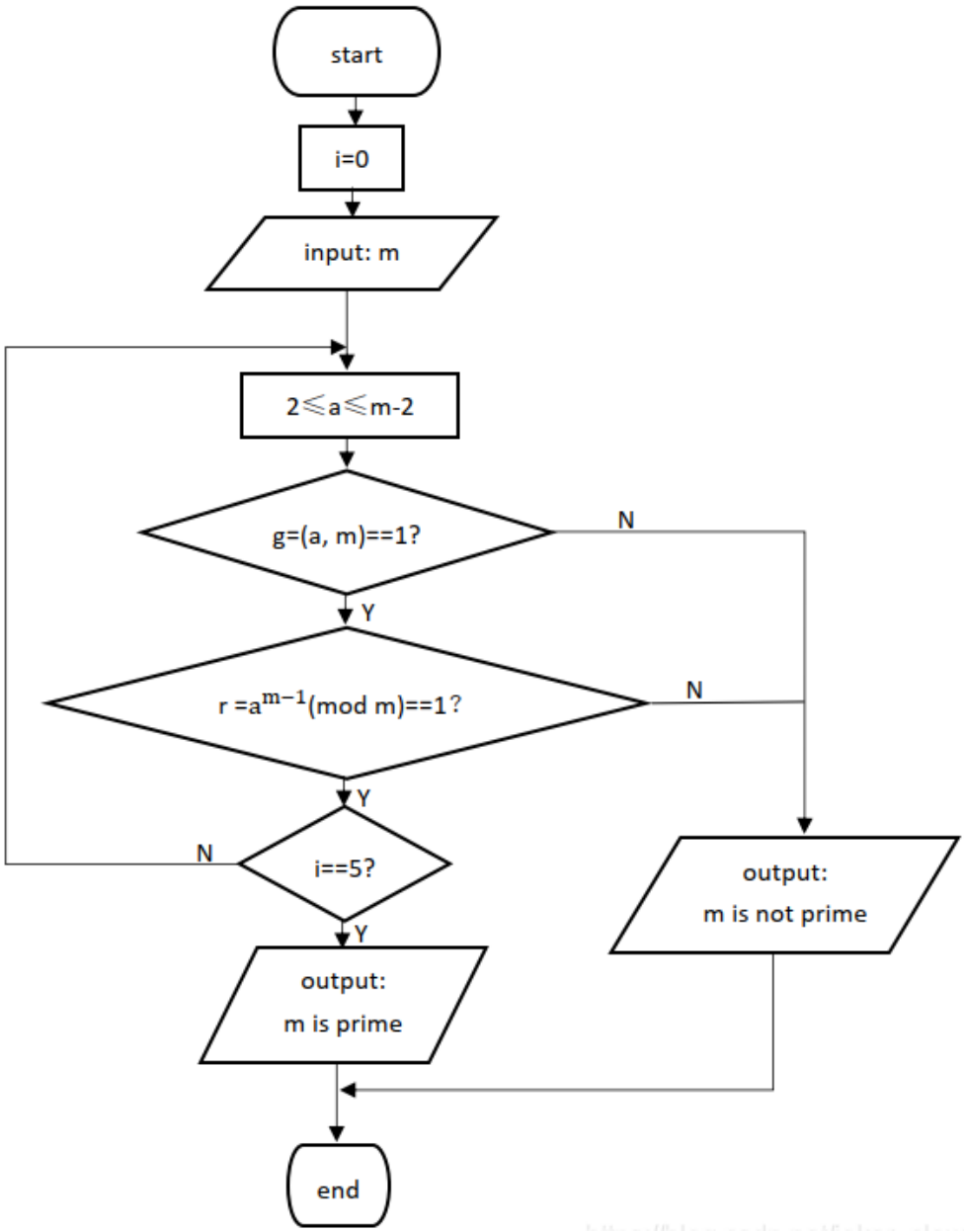
（3） 计算$r = a^{m-1}$(mod m),如果 r=1，m 可能是素数，转（1）；否则，跳出，m 是合数

（4） 重复上述过程 k 次，如果每次得到 m 可能为素数，则 m 为素数的概率为 $1 - \frac{1}{2^k}$

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：



算法实现代码：

```
import gmpy2 as gp
import random

def is_prime(num, k):
    for _ in range(k):
        print("第"+str(_+1)+"次素性检测")
        a = random.randrange(2, num - 2)
        print("选取随机数：random="+str(a))
        if gp.gcd(a, num)!=1:
            print("第" + str(_ + 1) + "次素性检测失败，可以判定该数不是素数")
            return False
        if pow(a,num-1,num)!=1:
            print("第" + str(_ + 1) + "次素性检测失败，可以判定该数不是素数")
            return False
        print("第"+str(_+1)+"次检测通过\n")
    return True

n = gp.mpz(input("请输入需要检测的整数 n："))
K = int(input("请输入安全参数 K："))
boolean=is_prime(n,K)
if boolean:
    print(str(K)+"次素性检测通过，在"+str((1-1/2**K)*100)+"%的概率下可以认为是素数")
```

四、数据分析

(包括算法测试数据的分析等等)

```
D:\Python\python.exe H:/[粉粉小红花]/[作业]/信息安全数学基础/is_prime.py
请输入需要检测的整数n：5186293680901708283310486635502296344443842997512729390771686489350756041806760063924645249531282938429964410227718907197318118529486849503882119071
请输入安全参数K：5
第1次素性检测
选取随机数：random=39490885563539928191894415648989331901590587215041136012105747835731952108472764813247638503691077790199386278308088487698768805187289594195372464908
第1次检测通过

第2次素性检测
选取随机数：random=34027636889086428630760521086338890243598183980387524852485111946046810337476265457992234773260260682528631477249569260224735993670385891764805160859
第2次检测通过

第3次素性检测
选取随机数：random=27987320191319089373727248740080622287543122891736088508750816303727675218849390577272681750938880911915049507906759836193834053309290430159501394899
第3次检测通过

第4次素性检测
选取随机数：random=37218054266000169386028956542888776154970322951793014630506565449639231352879038340798654273771715727072135390563728817225983662217669783434471370097
第4次检测通过

第5次素性检测
选取随机数：random=35036707608248058846804665747091641152897368671085074414587982761676525218540469361458957297281974626509343978805604254148831341364344834725891379308
第5次检测通过

5次素性检测通过，在96.875%的概率下可以认为是素数
```

输入一个 500 多位的大素数，安全参数 k=5 时，检验结果如图。

5 次素性检测通过，在 96.875%的概率下可以认为是素数

五、总结

（完成的心得和其他，主要是自己碰到的问题，以及解决问题的方法等）

当大数通过 K 次费马素性检测时，要根据安全参数 K 来计算是素数的概率；

当发现输入的数是合数时（不互素，或不满足费马小定理），应直接返回 False。