**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（一）**

**Fermat素性检测算法**

**班级：**

**姓名：**

**学号：**

**日期：2022年10月30日**

一、实验目的（包括实验环境、实现目标等等）

实验环境

Windows11 , Python 3.9.12

二、方案设计

（包括背景、原理、必要的公式、图表、算法步骤等等）

实验原理

1).Fermat小定理

给定素数，则有

如果有一个整数，，使得

则m是素数或者伪素数

如果有一个整数，，使得

则m一定是一个合数

2).引理

奇整数，若任取一整数，，使得，则至少有的概率为素数。

Fermat素性检验算法

(I)输入待检测的大整数和检验次数,令

(II)随机选取整数，

(III)计算，如果，则为合数，跳出循环。

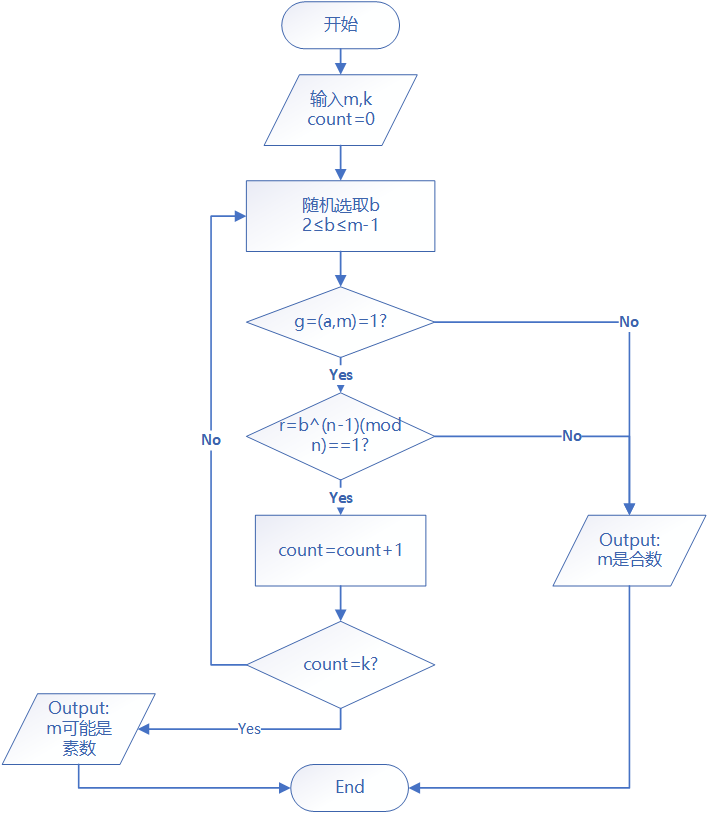
(IV)计算，如果，则为合数，跳出循环。

(V) 则判断可能为素数，且为素数的概率为并跳出循环;否则，，并返回(I)。

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

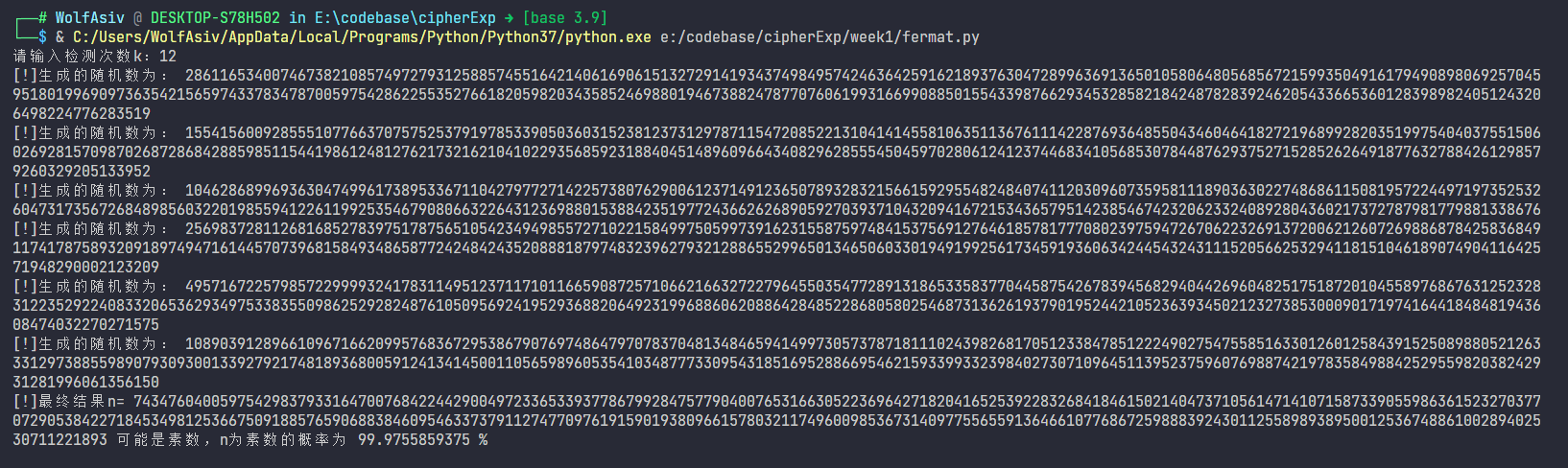
gcd()函数求最大公因数

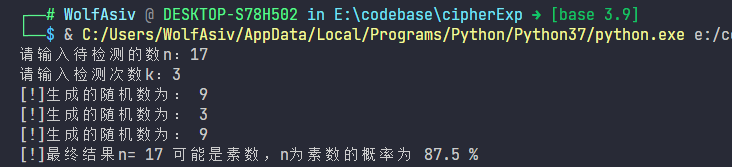
check\_fermat()素性检验

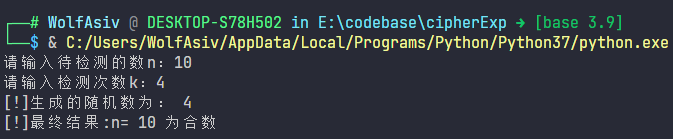
代码块

1. import random
2. *#实验1-Fermat素性检测算法*
3. *#求最大公因数*
4. def gcd(a,b):
5. if a<b:
6. a,b=b,a
7. while b!=0:
8. a,b=b,a%b
9. return a
10. def check\_fermat(n):
11. *#生成[2,n-2]之间一个随机数*
12. b=int(random.randrange(2,n-1))
13. print("[!]生成的随机数为：",b)
14. *#判断是否互素*
15. if gcd(b,n)!=1:
16. *#print("n=",str(n),"不是素数")*
17. return False
18. *#判断是否满足费马小定理*
19. if pow(b,n-1,n)!=1:*#pow(a,b,c)表示a的b次方对c取模*
20. *#print("n=",str(n),"在该次检验中不是素数")*
21. return False
22. *# print("n=",str(n),"可能是素数")*
23. return True
24. *#输入：待检测的数n，检测次数k*
25. *# n=int(input("请输入待检测的数n："))*
26. n=743476040059754298379331647007684224429004972336533937786799284757790400765316630522369642718204165253922832684184615021404737105614714107158733905598636152327037707290538422718453498125366750918857659068838460954633737911274770976191590193809661578032117496009853673140977556559136466107768672598883924301125589893895001253674886100289402530711221893
27. k=int(input("请输入检测次数k："))
28. *#检测*
29. if "\_\_main\_\_"==\_\_name\_\_:
30. possible=(1-1/2\*\*k)\*100
31. while(k>0):
32. if check\_fermat(n):
33. k-=1
34. else:
35. break
36. if(k==0):
37. print("[!]最终结果n=",str(n),"可能是素数，n为素数的概率为",str(possible),"%")
38. else:
39. print("[!]最终结果:n=",str(n),"为合数")

四、数据分析(包括算法测试数据的分析，运行结果截图等等)



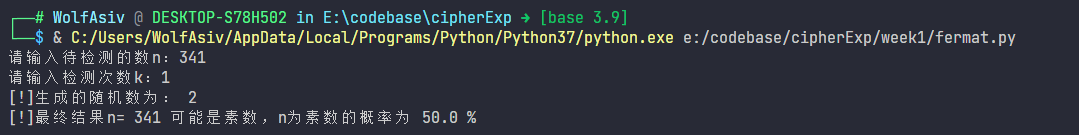




五、思考与总结

1. 如果有一个整数𝒂，(𝒂,𝒎)=𝟏，使得𝒂𝒎−𝟏≡𝟏 𝒎𝒐𝒅 𝒎 则𝒎一定是一个素数吗？为什么？（请简述并举例说明，不能只简单回答“是”或“不是”）

答:不是，当检验的次数比较低时，可能会出现伪素数，如m=341,(341,2)=1,且满足



1. Fermat素性检测中都用到了哪些运算？分别实现什么功能？请简述。

答:模指数运算实现检测是否满足费马小定理

伪随机算法实现生成随机数

辗转相除法实现求最大公因数

1. 你还了解哪种素性检测算法？请简述，并分析其与Fermat素性检测算法的区别与联系。

答:Miller-Rabin素性测试算法,他是在Fermat素性检测算法的基础上为了解决卡迈克尔数，提高素数的检测的正确性而产生的。Fermat素性检测算法基于费马小定理,而Miller-Rabin素性测试算法基于费马小定理和二次检验定理，当然 Miller-Rabin 算法的时间复杂度较高。

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？

发现在生成指定随机数时，如果检验的数字过大,那么如果我们用

random.uniform(2,n-1)这个函数生成随机数会导致溢出，这是因为该方法所依赖的是float类型而不是大整数,这里我们换用了random.randrange(2,n-1)生成随机数。