МИНОБРНАУКИ РОССИИ
ФГБОУ ВО «СГУ ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»

АЛГОРИТМЫ АЛГЕБРЫ И ТЕОРИИ ЧИСЕЛ

ЛАБОРАТОРНАЯ РАБОТА №4

студента 4 курса 431 группы
направления 10.05.01 — Компьютерная безопасность
факультета КНиИТ
Никитина Арсения Владимировича

Проверил
доцент _____ А. С. Гераськин

Саратов 2022

СОДЕРЖАНИЕ

1 Задание лабораторной работы

Осуществить проверку чисел на простоту с помощью теста на основе малой теоремы Ферма.

2 Теоретическая часть

Согласно малой теореме Ферма, для простого числа p и произвольного числа $a = \overline{2, p-1}$ выполняется сравнение:

$$a^{p-1} \equiv 1 \, (mod \, p).$$

Это означает, что если для нечетного числа n существует такое целое число $a = \overline{2, n-1}$, что $a^{n-1} \equiv 1 \, (mod \, n)$, то число n вероятно является простым. Таким образом получаем следующий вероятностный алгоритм проверки числа на простоту:

Вход: Нечетное число $n \geq 5$.

Выход: "Число n, вероятно, простое"или "Число n не является простым".

1. Выбрать случайное целое число $a = \overline{2, n-1}$.
2. Вычислить $r = a^{n-1} \, (mod \, n)$.
3. Если $r = 1$, то ответ — "Число n, вероятно, простое а если $r \neq 1$, то ответ — "Число n не является простым".

Стоит отметить, что тест будет давать неверные ответы для чисел Кармайкла.

3 Практическая часть

3.1 Пример работы алгоритма

```
Введите число, которое требуется проверить на простоту тестом Ферма: 561
Введите количество тестов, которое требуется провести: 1
По совокупности тестов, число является простым

Проверить число на простоту тестом Ферма - \enter
Выход из программы - 2
Введите значение:

Введите число, которое требуется проверить на простоту тестом Ферма: 10
Введите количество тестов, которое требуется провести: 1
По совокупности тестов, число не является простым

Проверить число на простоту тестом Ферма - \enter
Выход из программы - 2
Введите значение:

Введите число, которое требуется проверить на простоту тестом Ферма: 31
Введите количество тестов, которое требуется провести: 10
По совокупности тестов, число является простым
```

Рисунок 1

3.2 Код программы, реализующей рассмотренный алгоритм

```
1  import random
2
3
4  def pow(number, modula):
5      number_save = number
6      for _ in range(modula - 2):
7          number = number * number_save % modula
8      return number
9
10
11 def gcd(a, b):
12     if b == 0:
13         return a
14     else:
15         return gcd(b, a % b)
16
17
18 def ferma_test(n):
19
20     number = random.randint(2, n - 1)
21     if gcd(number, n) != 1:
```

```
22          return False
23      elif pow(number, n) != 1:
24          return False
25
26      return True
27
28
29  def main():
30
31      while True:
32
33          print('Проверить число на простоту тестом Ферма - \enter')
34          print('Выход из программы - 2')
35
36          try:
37              value = int(input('Введите значение: '))
38          except ValueError:
39              value = 1
40
41          if value == 1:
42
43              n = int(input('\nВведите число, которое требуется проверить на
                ↪  простоту тестом Ферма: '))
44              number_of_tests = int(input('Введите количество тестов, которое
                ↪  требуется провести: '))
45
46
47              if all([ferma_test(n) for _ in range(number_of_tests)]):
48                  print('По совокупности тестов, число является простым\n')
49              else:
50                  print('По совокупности тестов, число не является простым\n')
51
52          if value == 2:
53              break
54
55
56  if __name__ == '__main__':
57      main()
```