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

АЛГОРИТМЫ АЛГЕБРЫ И ТЕОРИИ ЧИСЕЛ

ЛАБОРАТОРНАЯ РАБОТА №5

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 свойств чисел Кармайкла

2 Теоретическая часть

2.1 Теоремы Бигера и Дюпарка

В 1956 году Бигер доказал, что если для простых чисел p, q, r выполняется соотношение $p < q < r$ и pqr — число Кармайкла, то $q < 2p^2$ и $r < p^3$. Таким образом, количество чисел Кармайкла, получаемых произведением трёх простых множителей, один из которых известен, конечно.

Дюпарк позже обобщил этот результат, чтобы показать, что если $n = mqr$ — число Кармайкла, где q и r — простые, тогда $q < 2m^2$ и $r < m^3$. Следовательно, существует не более чем конечное количество чисел Кармайкла со всеми, кроме двух, определёнными множителями.

Случай $m = 1$ показывает, что любое кармайклово число содержит как минимум 3 простых множителя, к этому выводу впервые пришёл сам Кармайкл.

Итак, для того, чтобы показать, что число, проверяемое с помощью теста Ферма на простоту было действительно простым, то требуется показать, что у данного числа не найдется как минимум один простой делитель.

3 Практическая часть

3.1 Пример работы алгоритма

```
Введите число, которое требуется проверить на простоту: 41041
Число 41041 является простым по тесту на основе малой теоремы Ферма, поэтому требуется проверить, не является ли оно числом Кармайкла
Число 41041 не является простым

Проверить число на простоту тестом Ферма, а также по свойствам чисел Кармайкла - \enter
Выход из программы - 2
Введите значение:

Введите число, которое требуется проверить на простоту: 825265
Число 825265 является простым по тесту на основе малой теоремы Ферма, поэтому требуется проверить, не является ли оно числом Кармайкла
Число 825265 не является простым

Проверить число на простоту тестом Ферма, а также по свойствам чисел Кармайкла - \enter
Выход из программы - 2
Введите значение: 321197185

Проверить число на простоту тестом Ферма, а также по свойствам чисел Кармайкла - \enter
Выход из программы - 2
Введите значение:

Введите число, которое требуется проверить на простоту: 321197185
Число 321197185 является простым по тесту на основе малой теоремы Ферма, поэтому требуется проверить, не является ли оно числом Кармайкла
Число 321197185 не является простым

Проверить число на простоту тестом Ферма, а также по свойствам чисел Кармайкла - \enter
Выход из программы - 2
Введите значение: 2
Работа программы завершена
```

Рисунок 1

3.2 Код программы, реализующей рассмотренный алгоритм

```
1  import random
2  import math
3
4  def modula_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 is_real_prime(number):
12     for i in range(3, number - 1, 2):
13         if not number % i:
14             return False
15     return True
16
17
18 def gcd(a, b):
19     if b == 0:
20         return a
21     else:
```

```
22          return gcd(b, a % b)
23
24
25  def ferma_test(n):
26
27      number = random.randint(2, n - 1)
28      if gcd(number, n) != 1:
29          return False
30      elif modula_pow(number, n) != 1:
31          return False
32
33      return True
34
35
36  def check_prime():
37
38      n = int(input('\nВведите число, которое требуется проверить на простоту:
        ↪  '))
39
40      if not ferma_test(n):
41          print(f'Число {n} не является простым по тесту на основе малой
            ↪  теоремы Ферма')
42      else:
43          print(f'Число {n} является простым по тесту на основе малой теоремы'
            ↪  \
44              ' Ферма, поэтому требуется проверить, не является ли оно числом
                ↪  Кармайкла')
45
46          if not is_real_prime(n):
47              print(f'Число {n} не является простым')
48          else:
49               print(f'Число {n} действительно является простым')
50      return
51
52  def main():
53
54     while True:
55
56          print('\nПроверить число на простоту тестом Ферма, а также по
            ↪  свойствам чисел Кармайкла - \enter')
57          print('Выход из программы - 2')
```

```
58
59          try:
60              value = int(input('Введите значение: '))
61          except ValueError:
62              value = 1
63
64          if value == 1:
65              check_prime()
66          elif value == 2:
67              print('Работа программы завершена')
68              return
69
70  if __name__ == '__main__':
71      main()
```