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

АЛГОРИТМЫ АЛГЕБРЫ И ТЕОРИИ ЧИСЕЛ

ЛАБОРАТОРНАЯ РАБОТА №3

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 критерия Вильсона.

2 Теоретическая часть

Теорема Вильсона

Если p — простое число, то выполняется соотношение $(p-1)! + 1 \equiv 0\ (mod\ p)$, а если p – составное, то соотношение не выполняется.

Для доказательства потребуется вспомогательное утверждение:

Если НОД(a, b) = 1, то $\exists u, v \in \mathbf{Z} : au + bv = 1$.

Итак, докажем теорему.

Очевидно, достаточно доказать утверждение для случая, когда a, b — натуральные числа. Нетривиальной частью доказательства является идея индукции по сумме $a + b$. При $a + b = 2$ имеем $a = b = 1$ и $au + bv = 1$ выполняется с $u = 1$, $v = 0$. Пусть теорема верна для всех a, b : НОД(a,b)=1, $a + b < k$, где $k > 2$. Тогда, так как $a + b > 2$, НОД(a,b)=1, то $a \neq b$. Не теряя общности можно считать, что $a > b$. Поскольку, очевидно, НОД(a-b,b)=1 и $(a - b) + b = a < k$, по индуктивному предположению существуют целые x, y, такие, что:

$$(a - b)x + by = 1 \text{ или } ax + b(y - x) = 1.$$

Положив $x = u$, $y - x = v$, получим $au + bv = 1$, что и требовалось доказать.

3 Практическая часть

3.1 Пример работы алгоритма

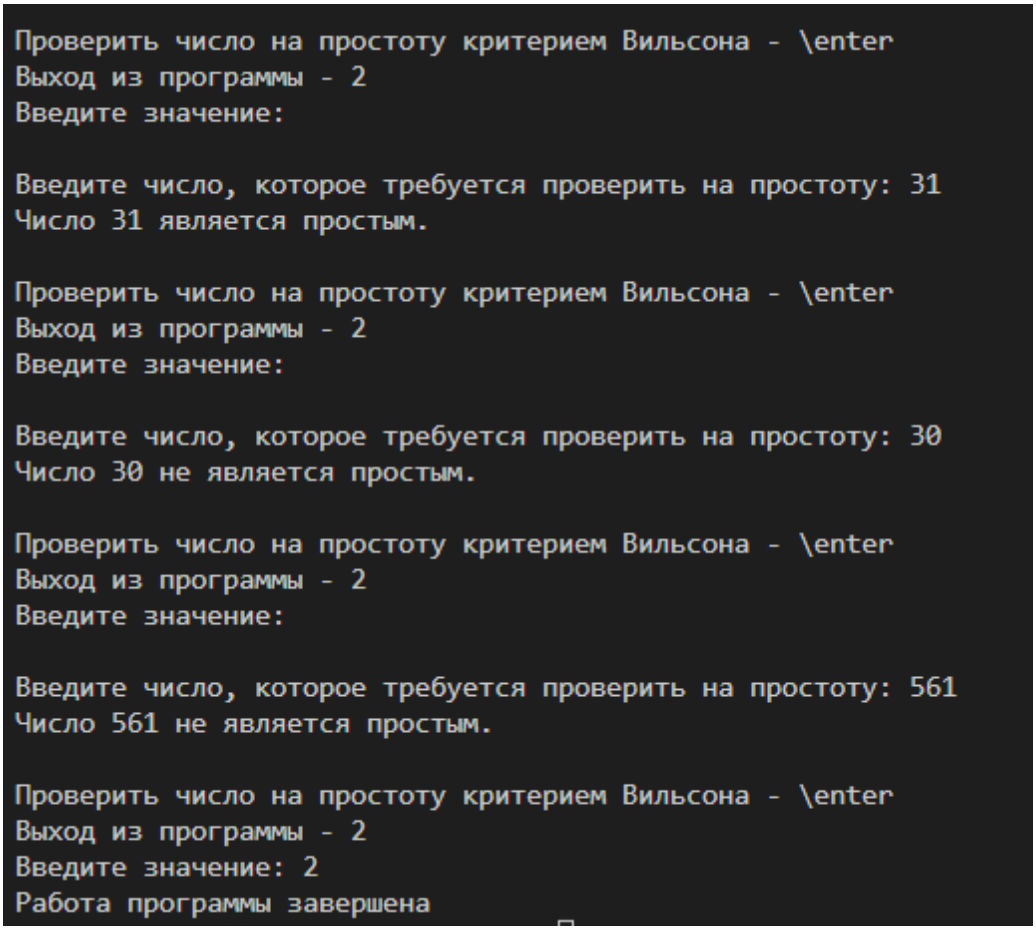

Рисунок 1

3.2 Код программы, реализующей рассмотренный алгоритм

```
1  def fact(n):
2      res = 1
3      for i in range(2, n + 1):
4          res *= i
5      return res
6
7
8  def vislon_criteria(n):
9      return not (fact(n - 1) + 1) % n
10
11
12 def main():
13
14     while True:
```

```
15
16          print('\nПроверить число на простоту критерием Вильсона - \enter')
17          print('Выход из программы - 2')
18
19          try:
20              value = int(input('Введите значение: '))
21          except ValueError:
22              value = 1
23
24          if value == 1:
25
26              n = int(input('\nВведите число, которое требуется проверить на
                ↪  простоту: '))
27              if vislon_criteria(n):
28                  print(f'Число {n} является простым.')
29              else:
30                  print(f'Число {n} не является простым.')
31
32          if value == 2:
33              print('Работа программы завершена')
34              return
35
36
37  if __name__ == '__main__':
38      main()
39
```