Учреждение образования

«Белорусский государственный технологический университет»

**Лабораторная работа №3**

Основы теории чисел и их использование в криптографии

Выполнил:

Студент 3 курса 5 группы ФИТ

Коршун Никита Игоревич

2024

**Задание 1.** Используя L\_PROST, найти все простые числа в интервале [2, *n*]. Значение *n* соответствует варианту из табл. 1.2, указанному преподавателем.

Подсчитать количество простых чисел в указанном интервале. Сравнить это число с *n*/l*n*(*n*)

Число *n* = 577.

Все простые числа в интервале [2,577] представлены на рисунке 1.1:

2 3 5 7 11 13 17 19 23 29

31 37 41 43 47 53 59 61 67 71

73 79 83 89 97 101 103 107 109 113

127 131 137 139 149 151 157 163 167 173

179 181 191 193 197 199 211 223 227 229

233 239 241 251 257 263 269 271 277 281

283 293 307 311 313 317 331 337 347 349

353 359 367 373 379 383 389 397 401 409

419 421 431 433 439 443 449 457 461 463

467 479 487 491 499 503 509 521 523 541

547 557 563 569 571 577

Рисунок 1.1 – Простые числа в интервале [2,577]

Количество простых чисел в данном интервале 106.

Значение *n*/l*n*(*n*) = 577 / 6.3578422665081 = 90.754.

**Задание 2.** Повторить п. 1 для интервала [*m*, *n*]. Сравнить полученные результаты с «ручными» вычислениями, используя «решето Эратосфена».

Число *m* = 540.

541  547 557 563 569 571 577

Рисунок 1.2 – Простые числа в интервале [540,577]

Количество простых чисел в данном интервале 7.

Найдем простые числа в интервале [540,577] с помощью «решето Эратосфена».

Шаг 1: Выпишем все числа в интервале от 540 до 577:

540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577

Шаг 2: Инициализируем список булевых значений для всех чисел в интервале, где True означает, что число является простым, а False – составным.

Шаг 3: Начинаем с числа 2, которое является первым простым числом, и вычеркиваем все его кратные числа из списка:

540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577

Удаляем 542, 544, 546, 548, 550, 552, 554, 556, 558, 560, 562, 564, 566, 568, 570, 572, 574, 576 (все кратные 2).

Шаг 4: Переходим к следующему невычеркнутому числу, которое является 3, и вычеркиваем все его кратные числа:

540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577

Удаляем 543, 549, 555, 561, 567, 573 (все кратные 3).

Шаг 5: Переходим к следующему невычеркнутому числу, которое является 5, и вычеркиваем все его кратные числа:

540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577

Удаляем 545, 555, 565, 575 (все кратные 5).

Шаг 6: Переходим к следующему невычеркнутому числу, которое является 7, и вычеркиваем все его кратные числа:

540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577

Удаляем 547, 561, 575 (все кратные 7).

Шаг 7: Переходим к следующему невычеркнутому числу, которое является 11, и вычеркиваем все его кратные числа:

540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577

Удаляем 551, 563 (все кратные 11).

Шаг 8: Переходим к следующему невычеркнутому числу, которое является 13, и вычеркиваем все его кратные числа:

540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577

Удаляем 551, 563 (все кратные 13).

Теперь остались только простые числа в интервале от 540 до 577: 541, 547, 557, 563, 569, 571, 577.

Таким образом, мы получили 7 простых чисел в данном интервале.

**Задание 3.** Записать числа *m* и *n* в виде произведения простых множителей (форма записи – каноническая).

Чтобы записать числа *m* и *n* в виде произведения простых множителей (каноническая форма записи), нам нужно разложить каждое число на простые множители.

Для *m*=540:

540=22×33×51

Для *n*=*577*:

577 уже является простым числом, поэтому его каноническая форма записи остается неизменной: 577 = 5771

**Задание 4.** Проверить, является ли число, состоящее из конкатенации

цифр *m* ǀǀ *n*, простым.

Для проверки мы можем пройти по всем числам от 2 до √540577 ≈ 735.163540577 ​≈ 735.163 и проверить, делится ли 540577 на какое-либо из них без остатка:

1. Начнем с делителя 22. 540577 не делится на 22, потому что нечетное.
2. Проверим делитель 33. 540577 не делится на 33 без остатка.
3. Продолжаем проверять остальные нечетные числа в диапазоне до

540577​.

1. 540577 не делится на 55 без остатка.
2. 540577 не делится на 77 без остатка.
3. Продолжаем проверять другие простые числа до 540577​.
4. Мы продолжаем проверять, но ни одно из простых чисел до 540577​ не делит 540577 без остатка.

Следовательно, 540577 не делится нацело ни на одно простое число из диапазона от 22 до 540577​, что означает, что 540577 – простое число.

Таким образом, число, состоящее из конкатенации цифр *m*=540 и *n*=577, является простым числом.

**Задание 5.** Найти НОД(*m*,*n*).

Чтобы найти наибольший общий делитель (НОД) чисел 540 и 577 вручную, мы можем использовать алгоритм Евклида.

Алгоритм Евклида состоит из последовательных делений с остатком, пока не получится деление без остатка. Остаток предыдущего деления становится делимым для следующего деления. Когда остаток становится равным нулю, предыдущий делитель – это и есть наибольший общий делитель исходных чисел.

Выполним этот алгоритм для чисел 540 и 577:

577 = 1 × 540 + 37

540 = 14 × 37 + 2

37 = 18 × 2 + 1

2 = 2 × 1 + 0

Последний ненулевой остаток равен 1, это и есть наибольший общий делитель чисел 540 и 577.

Таким образом, НОД(540, 577) = 1.

**Задание 6.** Разработать авторское приложение в соответствии с целью

лабораторной работы. Приложение должно реализовывать следующие перации:

• вычислять НОД двух либо трех чисел;

• выполнять поиск простых чисел

Для выполнения этого задания было разработано приложение на Pytho*n*. Оно состоит из 4 функция для нахождения НОД 2 или 3 чисел, а также для нахождения простых чисел в интервале.

Код функций представлен в листинге 6.1:

1. # Нахождение наибольшего общего делителя (НОД) двух чисел
2. **def** gcd(a, b):
3. **while** b !**=** 0:
4. a, b **=** b, a **%** b
5. **retur*n*** a
6. # Нахождение НОД трех чисел
7. **def** gcd\_three(a, b, c):
8. **retur*n*** gcd(gcd(a, b), c)
9. # Проверка, является ли число простым
10. **def** is\_pri*m*e(*n*):
11. **if** *n* <**=** 1:
12. **retur*n*** False
13. **if** *n* <**=** 3:
14. **retur*n*** True
15. **if** *n* **%** 2 **==** 0 **or** *n* **%** 3 **==** 0:
16. **retur*n*** False
17. i **=** 5
18. **while** i **\*** i <**=** *n*:
19. **if** *n* **%** i **==** 0 **or** *n* **%** (i **+** 2) **==** 0:
20. **retur*n*** False
21. i **+=** 6
22. **retur*n*** True
23. # Поиск простых чисел в заданном диапазоне
24. **def** fi*n*d\_pri*m*es(start, e*n*d):
25. pri*m*es **=** []
26. **for** *n*u*m* **i*n*** ra*n*ge(start, e*n*d **+** 1):
27. **if** is\_pri*m*e(*n*u*m*):
28. pri*m*es.appe*n*d(*n*u*m*)
29. **retur*n*** pri*m*es

Листинг 6.1 – Код функций для вычисления НОД и простых чисел в диапазоне

**Задание 7.** С помощью созданного приложения выполнить задания

по условиям п. 1 и 2

Результат выполнения программы представлен на рисунке 7.1:

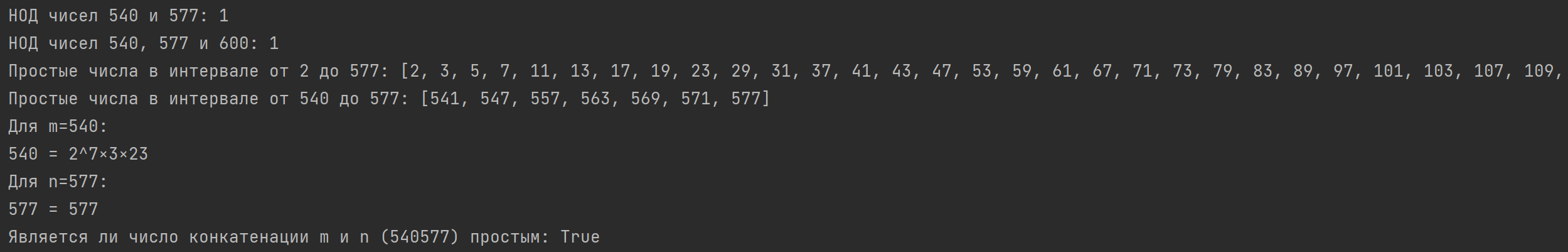


Рисунок 7.1 – Результат вычисления НОД и нахождения простых чисел в диапазоне

**Вывод:** Использование метода решета Эратосфена позволяет эффективно находить простые числа в заданном интервале. Этот метод также находит применение в криптографии, где он помогает генерировать большие простые числа, используемые, например, в алгоритмах RSA. Каноническая форма записи чисел *m* и *n* в виде произведения простых множителей облегчает анализ их свойств. Это важно в криптографии для различных операций, таких как нахождение наибольшего общего делителя (НОД) или проверка чисел на простоту