Дмитриев Егор Андреевич

студент

ФГАОУ ВО «Самарский национальный исследовательский университет им. академика С.П. Королева»

г. Самара, Самарская область

РЕШЕТО ЭРАТОСФЕНА ДЛЯ ПОИСКА ПРОСТЫХ ЧИСЕЛ

Аннотация: *в данной работе рассматривается один из основных алгоритмов поиска простых чисел – решето Эратосфена.*

Ключевые слова: *криптография, простое число, вычислительная сложность, тест простоты, пространственная сложность.*

Основные понятия

Введем некоторые определения, которые будут использованы в работе.

Определение 1. Криптография – наука о методах обеспечения конфиденциальности, целостности данных, аутентификации, а также невозможности отказа от авторства.

Определение 2. Простое число – натуральное (целое положительное) число ℕ, которое имеет ровно два различных натуральных делителя – единицу и самого себя.

Определение 3. Вычислительная сложность – функция, показывающая взаимосвязь между объемом работы, выполняемой алгоритмом, от размера входных данных.

Определение 4. Тест простоты – алгоритм, который по заданному натуральному числу ℕ позволяет точно или с некоторой долей вероятности определить, является ли это число простым.

Определение 5. Пространственная сложность – функция зависимости объема занимаемой памяти алгоритмом от размера входных данных.

Введение

Простые числа находят широкое применение в современном мире, например, в криптографии. Несмотря на то, что простые числа изучаются на протяжении длительного времени, проблема поиска простых чисел в наше время наиболее актуальна, в связи с потребностью получать большие простые числа для криптографических алгоритмов.

Решето Эратосфена

Вычислительная сложность алгоритма: $O(Nlog(logN))$.

Пространственная сложность алгоритма: $O(\sqrt{N})$.

Описание. Детерминированный алгоритм поиска простых чисел на отрезке от единицы до заданного целого числа *n*.

Алгоритм. Выпишем последовательно все целые числа из отрезка *[2,N]*, где *N* – заданное число. Возьмем первое число x_1 из этого списка и вычеркнем все числа кратные $(2x_1, 3x_1, 4x_1...)$ ему. Найдем первое не зачеркнутое число x_2 в списке, большее чем x_1 и повторим операцию вычеркивания кратных чисел. Будем продолжать эти шаги до тех пор, пока это возможно. Таким образом все оставшиеся (не зачеркнутые) числа будут простыми.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Рис. 1. Описание работы алгоритма. Исключение чисел кратных 2

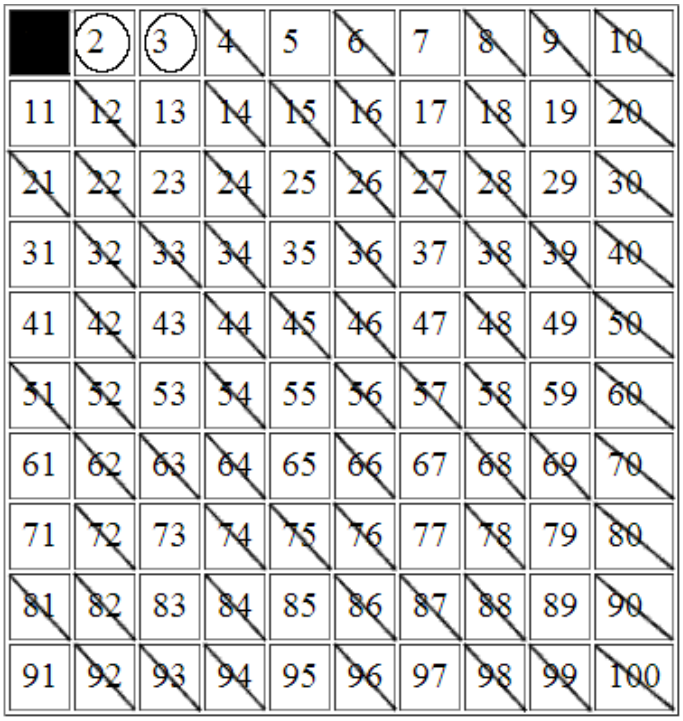

Рис. 2. Описание работы алгоритма. Исключение чисел кратных 2 и 3

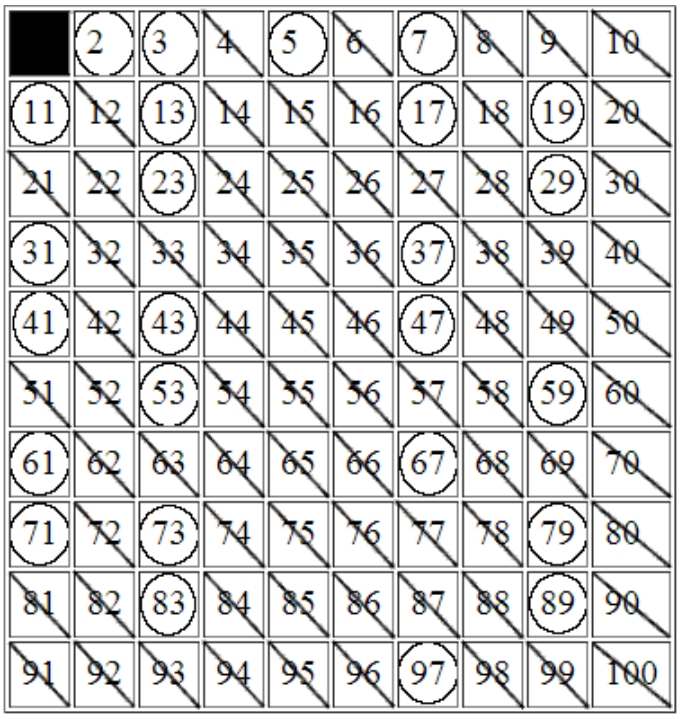

Рис. 3. Результат работы алгоритма

Заключение

В данной работе был изучен алгоритм поиска простых чисел – решето Эратосфена.

Список литературы

1. Шнайер Б.М. Прикладная криптография / Б.М. Шнайер. – Триумф, 2002. – 816 с.

2. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2003. – 328 с.

3. Дональд Кнут. Глава 4.5.4. Разложение на простые множители // Искусство программирования. Т 2. Получисленные алгоритмы. – 3-е изд. – М.: Вильямс, 2007. – С. 832.

4. Нестеренко Ю.В. Введение в криптографию / Под ред. В.В. Ященко. – Питер, 2001. – 288 с.