Дмитриев Егор Андреевич

студент

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

г. Самара, Самарская область

ТЕСТ МИЛЛЕРА – РАБИНА

Аннотация: *в данной работе рассматривается один из основных алгоритмов определения простоты числа – тест Миллера – Рабина. Автор рассмотрел реализацию алгоритма, определил его практическую ценность.*

Ключевые слова: *натуральное число, простое число, тест простоты.*

Основные понятия

Введем некоторые определения, которые будут использованы в работе.

Определение 1. Сравнение по модулю двух чисел натурального m – операция, позволяющая определить, имеют ли два числа один и тот же остаток при делении на m.

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

Определение 3. Тест простоты – алгоритм, который по заданному натуральному числу ℕ позволяет точно или с некоторой долей вероятности определить, является ли это число простым.

Введение

Тест простоты – алгоритм, который является достаточно критичным в криптографии в системе с открытым ключом.

Тесты простоты

Следует отметить, что существующие алгоритмы проверки простоты могут быть разделены на две больших категории: истинные (детерминированные) и вероятностные тесты. Алгоритмы первой категории позволяют точно определить

простоту или составность числа. А те, что относятся ко второй категории, позволяют это выяснить, но с некоторой вероятностью ошибки.

Тест Миллера – Рабина

Тип теста: вероятностный.

*Вычислительная сложность алгоритма: O(k*log²n), k*-количество раундов

Описание: пусть $n > 2$ – натуральное число, тогда представим число $n - 1$ в виде $n - 1 = 2^s * t$, где t – нечетно, а s – неотрицательно. Число a является свидетелем простоты для числа n, если выполняется одно из условий: $a^t \equiv 1(mod\ n)$ или $a^{2^r d} \equiv -1 (\mathrm{mod}\, n)$. Количество свидетелей простоты увеличивают достоверность алгоритма.

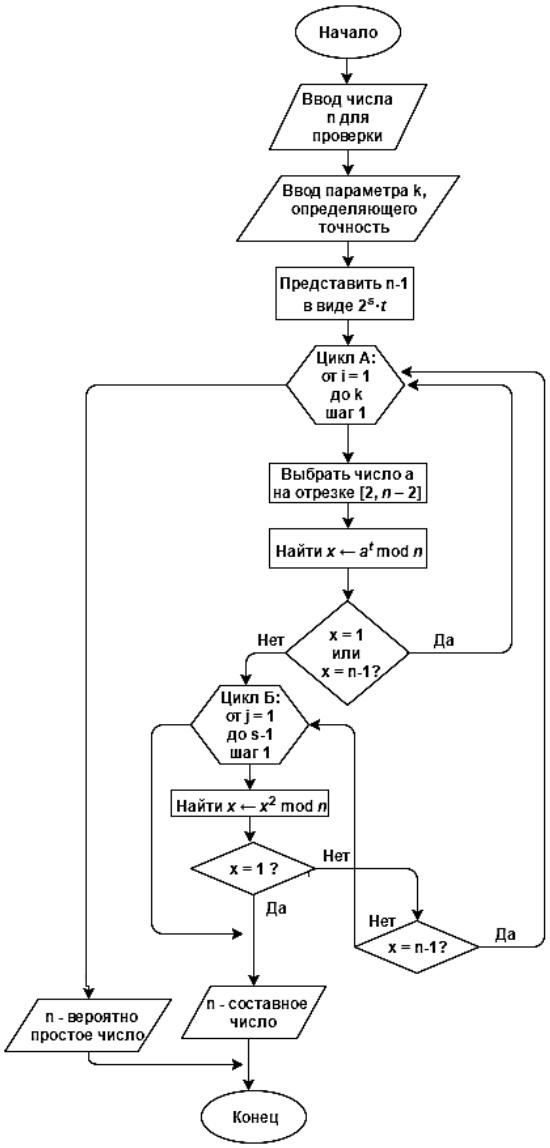

Рис. 1. Алгоритм проверки числа на простоту
при помощи теста Миллера-Рабина

Практическое применение: используется в криптосистемах с открытым ключом. Позволяет проверить число на простоту за малое время и давать при этом малую вероятность того, что оно окажется псевдопростым.

Заключение

Подводя итоги, можно констатировать, что были алгоритм определения простоты числа. Данный алгоритм является основным алгоритмом, применяемым на практике.

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.