Дмитриев Егор Андреевич

студент

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

г. Самара, Самарская область

ТЕСТ АГРАВАЛ – КАЙАЛ – САКСЕНА НА ПРОСТОТУ ЧИСЛА

Аннотация: *в данной работе рассматривается один из основных алгоритмов определения простоты числа – тест Агравал – Кайал – Саксена. Автор приводит реализацию алгоритма, определяет его практическую ценность.*

Ключевые слова: *алгоритм, практическая ценность, простота числа.*

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. Составное число – натуральное (целое положительное) число ℕ, которое не является простым.

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. *НОД(a,b) = d, d*-наибольший общий делитель, если

1) $a \vdots d \wedge b \vdots d$

2) $a \vdots d_1 \wedge b \vdots d_1 \Rightarrow d \vdots d_1$

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. Многократное их повторение для одного числа, но с разными параметрами, обычно позволяет сделать вероятность ошибки сколь угодно малой величиной.

Тест Агравал – Кайал – Саксена (*AKS*)

Тип теста: детерминированный.

Вычислительная сложность алгоритма: $O(\log^{19} N)$

Описание: единственный полиномиальный детерминированный алгоритм проверки числа на простоту. Если существует $r \in Z$ такое что $O_r(n) > \log^2 n$ и для любого a от 1 до $\lfloor \sqrt{\varphi(r)} \log(n) \rfloor$ выполняется сравнение $(x+a)^n \equiv (x+a)^n (\mathrm{mod}\, x^r, n)$, то n – либо простое число, либо степень простого числа.

Алгоритм: представлен на рисунке 1 в виде блок-схемы.

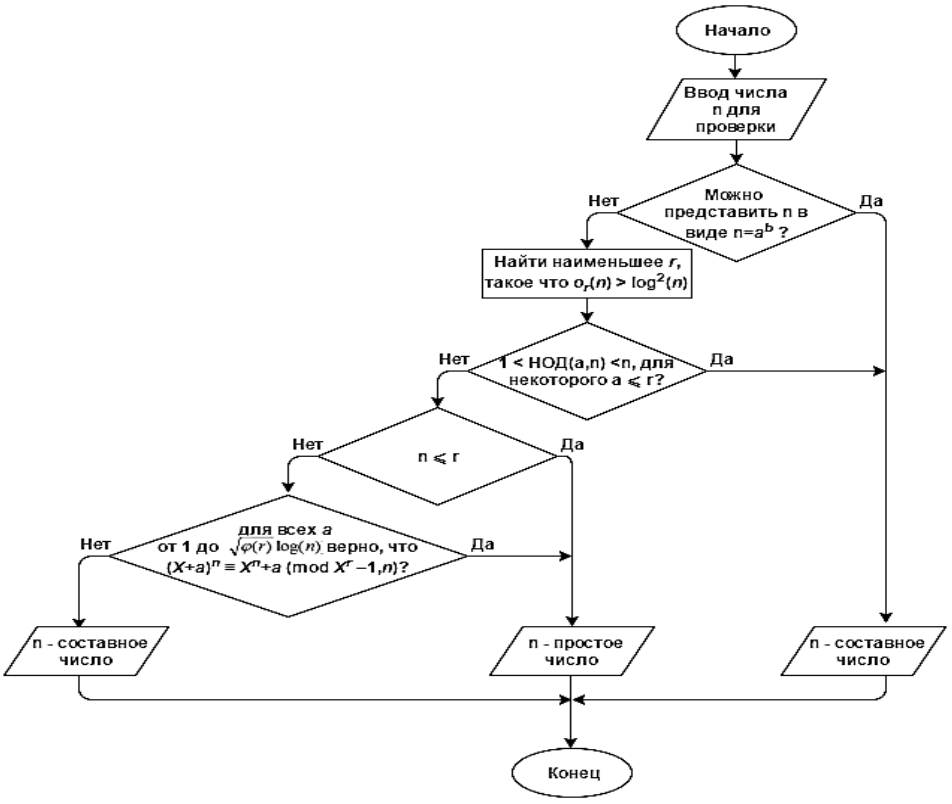

Рис. 1. Алгоритм проверки числа на простоту при помощи теста AKS

Практическое применение: в качестве детерминированной полиномиальной проверки на простоту.

Заключение

Подводя итоги, можно констатировать, что был рассмотрен алгоритм определения простоты числа. Проведённые исследования позволяют сделать вывод о том, алгоритм достаточно трудоемок в вычислительном плане, несмотря на то, что он лучше, чем алгоритм простого перебора.

Список литературы

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

2. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2003. – С. 12–56.

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.

5. Швейкин В.В. Сравнительный анализ алгоритмов определения простоты числа / В.В. Швейкин, И.В. Танаев, Е.А. Дмитриев [и др.] // Научное сообщество студентов XXI столетия. Технические науки: Сб. ст. по мат. XIIII междунар. студ. науч.-практ. конф. – № 6 (42) [Электронный ресурс]. – Режим доступа: https://sibac.info/studconf/tech/xliii/57352 (дата обращения: 01.08.2017).