Дмитриев Егор Андреевич

студент

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

г. Самара, Самарская область

ТЕСТ ВИЛЬСОНА

Аннотация: *в данной работе рассматривается один из основных алгоритмов определения простоты числа – тест Вильсона. В работе построена блок-схема алгоритма и определена сложность алгоритма.*

Ключевые слова: *простое число, составное число, тест простоты, наибольший общий делитель.*

Основные понятия

Введем некоторые определения, которые будут использованы в работе.

Определение 1. Простое число – натуральное (целое положительное) число $\mathbb{N}$, которое имеет ровно два различных натуральных делителя – единицу и самого себя.

Определение 2. Составное число – натуральное (целое положительное) число $\mathbb{N}$, которое не является простым.

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

Определение 4. *НОД (a, b) = d, d* – наибольший общий делитель, если

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

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

Определение 5. Вычислительная сложность – функция, показывающая взаимосвязь между объемом работы, выполняемой алгоритмом, от размера входных данных.

Введение

Дискретная математика – важнейшее направление современной математики. Задачи этой дисциплины являются одними из самых трудноразрешимых. Например, решение задачи факторизации, которая заключается в разложении числа на простые множители, на практике сводится к поиску простых чисел, что приводит к проблеме простоты.

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.

Теорема Вильсона

Тип теста: детерминированный.

Вычислительная сложность алгоритма: $O(N!)$.

Описание: натуральное число $n > 1$- простое число тогда и только тогда, когда $(n-1)! \equiv -1 (mod\ n)$.

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

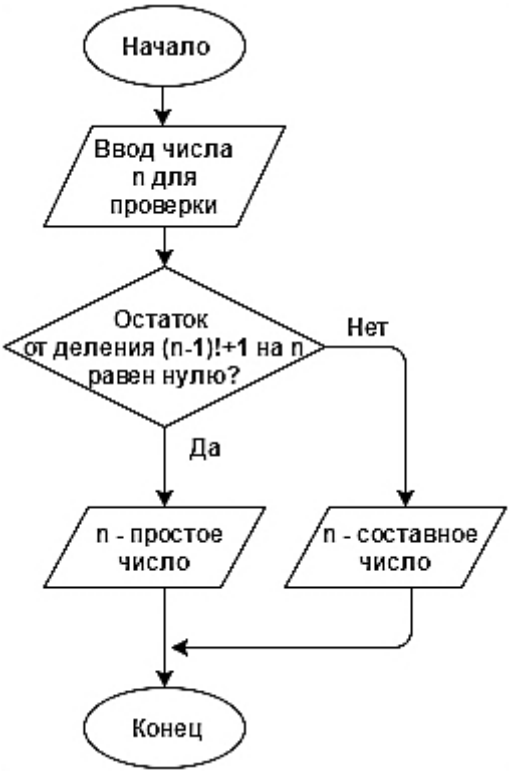

Рис. 1. Алгоритм проверки числа на простоту при помощи теоремы Вильсона

Практическое применение: не применяется из-за трудности вычисления *(n-1)!* при больших числах *n.*

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. – 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.