(cc) BY

Мажара Вероника Викторовна
студентка
Научный руководитель
Деревянко Елена Юрьевна
преподаватель

Филиал ФГБОУ ВО «Кубанский
государственный университет»
г. Тихорецк, Краснодарский край

АЛГОРИТМЫ ФАКТОРИЗАЦИИ ЦЕЛЫХ ЧИСЕЛ С ЭКСПОНЕНЦИАЛЬНОЙ СЛОЖНОСТЬЮ

Аннотация*: в статье рассматриваются основные алгоритмы факторизации целых чисел с экспоненциальной сложностью.*

Ключевые слова*: простое число, составное число, факторизация натурального числа.*

Простое число – это натуральное число, имеющее ровно два различных натуральных делителя.

Составное число – это натуральное число, имеющее делители, отличные от единицы и самого себя.

Факторизация натурального числа – разложение в произведение простых множителей.

Алгоритмы факторизации делятся на две группы: экспоненциальные и субэкспоненциальные. Сложность экспоненциальных алгоритмов зависит от длины входного числа N в двоичном представлении, а субэкспоненциальных – меньше, чем экспоненциальных, но больше, чем полиномиальных.

Алгоритм Ферма

Сложность алгоритма: $0(logN)$

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

Впервые данный метод был предложен Пьером Ферма в 1643 году. Основан на поиске таких целых чисел x и y, которые удовлетворяют соотношению $x^2 - y^2 = n$, что ведёт к разложению $n = (x - y)(x + y)$.

Равенство $x^2 - y^2 = n$ равносильно $x^2 - n = y^2$, то есть тому, что $x^2 - n$ является квадратом.

Поиск начинается с наименьшего числа, при котором разность $x^2 - n$ неотрицательна – ($\sqrt{n}$).

Для каждого значения последующего значения ($\sqrt{n}$) + k вычисляют $((\sqrt{n})+k)^2 - n$ и проверяют, не является ли это число точным квадратом.

Значение расчетного выражения на очередном шаге может вычисляться с учетом значения на предыдущем шаге: $(k + 1)^2 - n = k^2 + 2k + 1 - n = (k^2 - n) + 2k + 1$

Метод работает быстро, если n является произведением двух близких к друг другу сомножителей.

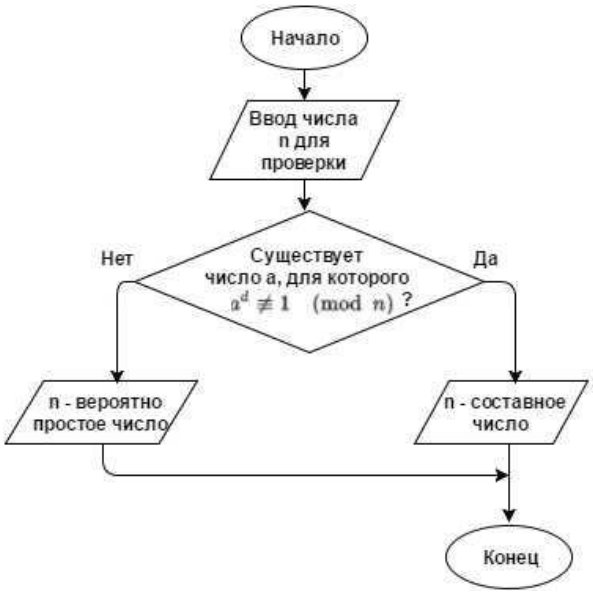

Рис. 1

Алгоритм Полларда-Штрассена

Сложность алгоритма: $0(N\,1/4\,log^4 N)$

Теорема: пусть $z \in N, y = z^2$. Тогда для любого натурального числа t наименьший простой делитель числа НОД (t, y!) может быть найден за $0(zlog^2 zlog^2 t$ арифметических операций.

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

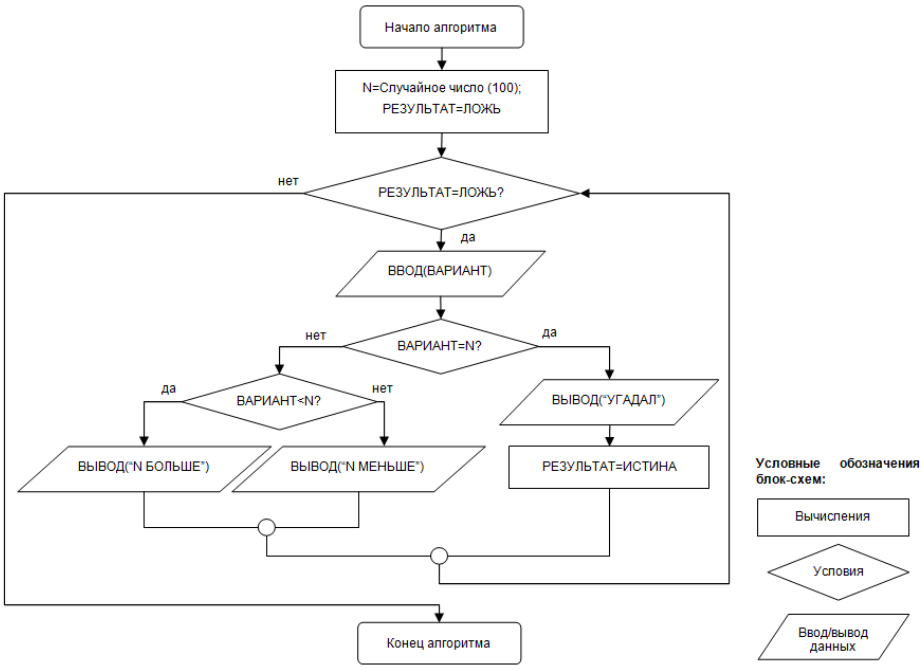

Рис. 2

Данный алгоритм является самым популярным из алгоритмов факторизации целых чисел с экспоненциальной сложностью. Применяется для факторизации не очень больших целых чисел.

Таким образом, были рассмотрены и изучены алгоритмы факторизации числа с экспоненциальной сложностью. Алгоритм факторизации Поллярда-Штрассена является наиболее эффективным и универсальным ввиду наименьшей зависимости от факторизуемого числа.

Список литературы

1. Малыхин В.И. Высшая математика: учебное пособие / В.И. Малыхин. – М.: ИНФРА-М, 2018. – 365 с.

2. Крицков Л.В. Высшая математика в вопросах и ответах: учебное пособие / Л.В. Крицков; под ред. В.А. Ильин. – М.: Проспект, 2017. – 176 с.

3. Мерзляк А.Г. Алгебра 9 класс. Дидактические материалы. – А.Г. Мерзляк, В.Б. Полонский, Е.М. Рабинович [и др.]. – 2017. – 128 с.

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)