ФИЗИКА-МАТЕМАТИКА ҒЫЛЫМДАРЫ

МРНТИ 27.17

Туленбаев К.М.[1], Мамбеталиев Ж.Т.[1], Габдуллин Б.[1], Шаймарданова Ж.[1], Калиева А.А.[1]

[1]Университет имени Сулеймана Демиреля, Казахстан, Каскелен

МОДИФИКАЦИЯ АЛГОРИТМА КОНЯГИНА-ПОМЕРАНСА ПРОВЕРКИ НА ПРОСТОТУ

Аннотация: Предлагается новый способ проверки нечетных чисел на простоту. Данный алгоритм основан на алгоритме Конягина-Померанса и является одним из быстрых алгоритмов для достаточно больших чисел. Реализация данного алгоритма написана на языке Visual C++. В данной статье мы описываем методы, с помощью которых можно проверять простоту натурального числа *N*, если известно полное или частичное разложение *N - 1* на множители. Алгоритмические*N* - 1 - методы проверки простоты. В данное время нам необходимо, в первую очередь, повышать эффективность методов и алгоритмов, как для практической реализации и обоснования стойкости криптографических средств, так и для разработки методов их вскрытия, что является одной из важных задач криптографии. Одним из важных алгоритмов является алгоритм проверки простоты целых чисел.

Ключевые слова: Теория чисел, простые числа, тест простоты, алгоритм Конягина-Померанса.

Введение

Алгоритмическая теории чисел интенсивно развивается последниетридцать лет. Данный раздел теории чисел имеет важные приложения в криптографии. Актуальность того направления неизмеримо увеличилась в 70-е годы XX века в связи с появлением криптосистем Диффи—Хеллмана и RSA. В настоящее время, по некоторым оценкам, практически весь мировой парк средств асимметричной криптографии в математическом плане основан на теоретико-числовых задачах. Одной из важной задач криптографии (как для практической реализации и обоснования стойкости криптографических средств, так и для разработки методов их вскрытия) необходимо в первую очередь повышать эффективность методов и алгоритмов. Одним из важных алгоритмов является алгоритмы проверки простоты целых чисел.

В данной статье мы описываем методы, с помощью которых можнопроверять простоту натурального числа *N*, если известно полное

иличастичное разложение *N - 1* на множители. Алгоритмические*N* - 1 - методы проверки простоты.

Мы используем следующую теорему, относящуюся к (*N* - 1)-методу проверки простоты чисел [2].

Теорема 1. Пусть $n \in N$, $n > 1$,*n* нечетно, $n-1=\prod p_i^{\alpha_i}$ известное разложение $n-1$ на простые множители.Если для каждого $i = 1, \dots, k$ **существует такое** $a_i \in N$, что$a_i \in N$, а$a_i^{n-1} \equiv 1 (mod\ n), a\ a_i^{\frac{n-1}{p_i}} \neq 1 (mod\ n)$то n—простое число.

Доказательство. Обозначим m_i порядок элемента a_i в кольце Z_n. Из условия следует, что $m_i \mid n-1$ и m_i не делит$\frac{n-1}{p_i}$. Поэтому $p_i^{\alpha_i} \mid m_i$ для каждого $i = 1, \dots, k$. Следовательно, $b_i \equiv a_i^{\frac{m_i}{p_i^{\alpha_i}}} (mod\ n)$имеют порядок $p_i^{\alpha_i}$в (Z_n)*, а элемент $b \equiv b_1 * \dots * b_k$ имеет порядок $\$\prod p_i^{\alpha_i} = n-1$ в (Z_n)*. Получаем, что (Z_n)* поле и *n* является простым числом [4].Ч.Т.Д.

Если $n \in N$ и известно полное разложение $n-1$на простые множители, или достаточно большая часть этого разложения, то можно с полиномиальной сложностью проверить, простое *n* или составное.

Наилучшая оценка сложности здесь получена в алгоритме Конягина—Померанса.

Алгоритм проверки простоты числа.

1 этап. Заготавливаем таблицу всех простых чисел, не превосходящих $[\log_2 n] + 1$.

Тест схож с методом факторизации Ферма основанный на теореме о представлении числа в виде разности двух квадратов:[1]

Теорема 2. Если *n*> 1 нечетно, то существует взаимно однозначное соответствие между разложениями на множители $n = ab$ и представлениями в виде разности квадратов $n = x^2 - y^2$, с$x > y > 0$ задаваемое формулами $x = \frac{a+b}{2}, y = \frac{a-b}{2}, a = x + y, b = x - y$.

Доказательство теоремы:

Если задана факторизация $n = ab$, то имеет место соотношение: $n = ab = (\frac{a+b}{2})^2 - (\frac{a-b}{2})^2$. Таким образом, получается представление в виде разности двух квадратов. Обратно, если дано, что $n = x^2 - y^2$, то правую часть можно разложить на множители:$(x-y)(x+y)$.

Проверка простоты небольших чисел

Лемма 1. Каждое нечетное простое число представимо в виде разности двух квадратов натуральных чисел и притом только одним способом [1].

Доказательство: Предположим, что простое число *P* разлагается наразность двух квадратов натуральных чисел: $P = x^2 - y^2$, где *x* и*y* - натуральные числа, причем, очевидно, *x*>*y*. Отсюда$P = (x - y)(x + y)$и, значит, $x - y$ и $x + y$ являются натуральнымиделителями числа P,причем первый меньше второго. Но так как P простое число, то $x - y$=1, $x + y = P$ и, следовательно, $x = \frac{P+1}{2}$, $y = \frac{P-1}{2}$.

Таким образом, число P должно быть нечетным, и в этом случае мы имеем единственное разложение:

$$P = (\frac{P+1}{2})^2 - (\frac{P-1}{2})^2$$

Ч.Т.Д.

Если при каком либо целом значении x не превышающим $0 \leq x \leq (\left(\frac{P+1}{2}\right) - 2)$ формулы $y = \sqrt{P + x^2}$значение y принимает целое число, то P является составным, а если иначе, то

P- простое число [1].

Условие: Проверяемое на простоту числоP- должно быть нечетным.

Лемма [1] определяет, что$y^2 < P < x^2$, $x = \frac{P+1}{2}, y = \frac{P-1}{2}$. То есть при минимальном значении *y = 1*, максимальное значение xдля $ $P = x^2 - y^2$, где P простое число, будет $x = \frac{P+1}{2}$.Соответственно, для проверки заданного числа P на простоту надо

брать значения $x < (\left(\frac{P+1}{2}\right) - 2)$ [5].

Описание модифицированного алгоритма Конягина-Померанса проверки на Простоту.

1 этап. Присваиваем *F(1) := 1*. Затем для каждого $a = 2, 3, \ldots, [\log_2 n] + 1$. Осуществляем 2-й этап, пока не докажем, что *n* — простое или же что *n* — составное число. Здесь мы используем изложенный выше алгоритм проверки небольших чисел на простоту.

2 этап. 1 шаг. Если *a* — составное (см. таблицу 1 этапа), то $F(a) := F(a - 1)$ и идем на 6 шаг. Если *a* — простое, и$a^{F(a-1)} \equiv 1 \pmod n$, то $F(a) := F(a - 1)$ и идем на 6 шаг. Иначе проверяем, выполняется ли сравнение: $a^{n-1} 1 (mod n)$. Если нет, то *n* составное.

2 шаг. Используя разложение $n-1$ на простые сомножители, найти порядок числа$a(mod\ n)$, т. е. наименьшее натуральное число $E(a)$, такое, что $a^{E(a)} \equiv 1\ (mod\ n)$.[3]

3 шаг. Проверяем, выполняется ли условие: $\text{НОД}(q\ |E(a)\ q-\text{простое}\left(a^{\frac{E(a)}{q}}-1\right),n)=1$. Если нет, то n— составное.

4 шаг. $F(a) := \text{НОК}(F(a-1), E(a))$.

5 шаг. Если $F(a) \to n^{\frac{1}{2}}$, то n—простое число.

6 шаг. Если $a \leftarrow [(\log n)^2]$, то возвращаемся к началу выполнения 2 этапа для следующего значения a. Если же $a = (\log n)^2 + 1$, то n— составное. Конец алгоритма.

Список использованных источников

1 Серпинский В.Ф. Что мы знаем и чего не знаем о простых числах / В.Ф. Серпинский. – М.: Государственное издательство физико-математической литературы, 1963. – 264 с.

2 Василенко О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М.: МЦНМО, 2003. – 321 с.

3 Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: Издательство ТРИУМФ, 2002. – 381 с.

4 Боревич З.И., Шафаревич И.Р. Теория чисел / З.И. Боревич, И.Р. Шафаревич. – М.: Наука, 1985. – 297 с.

5 Галочкин А.И., Нестеренко Ю.В., Шидловский А.Б. Введение в теорию чисел / А.И. Галочкин, Ю.В. Нестеренко, А.Б. Шидловский. – М.: МГУ, 1995. – 318 с.

K.M. Tulenbaev[1], J.T. Mambetaliyev[1], B. Gabdullin[1], J. Shaimardanova[1], A.A. Kaliyeva[1]

[1]Suleyman Demirel University, Kazakhstan, Kaskelen

MODIFICATION OF THE ALGORITHM KONYAGIN-POMERANCE CHECKS ON SIMPLICITY

Abstract: A new way to check the odd numbers on simplicity. This algorithm is based on an algorithm Konyagin-Pomerance and it is one of the fastest algorithms for sufficiently large numbers. The implementation of this algorithm is written in Visual C ++. In this article, we describe the methods by which it is possible to check the ease of a natural number *N*, if you know the complete or partial decomposition of the *N* - 1 factoring. Algorithmic *N* - 1 - methods ease of inspection. At this time, we need first of all to improve the efficiency of methods and algorithms for practical implementation and validation of cryptographic resistance, and to develop methods of their opening, which is

one of the important tasks of cryptography. One of the most important algorithms for checking algorithms is simplicity integers.

Key words: theory of numbers, prime numbers, primality test, algorithm Konyagin-Pomerance.

К.М. Туленбаев[1], Ж.Т. Мамбеталиев[1], Б. Габдуллин[1], Ж. Шаймарданова[1], А.А. Калиева[1]

[1]Сулейман Демирел атындағы университет, Қаскелен, Қазақстан

Аңдатпа: Тақ сандарды жай сан екенба екендігіне тексерудің жаңа әдісі. Бұл алгоритм Конягин-Памеранстың алгоритмі ненегізделген және де улкен сандарға арнаған ең тез алгоритм болып табылады. Бұл алгоритмнің іске асырылуы Visual C++ тілінде жазылған. Бұл мақалада *N*– 1-дің толық немесе бөлшектеп көбейткішке ыдырауы белгілі болған жағдайдағы, *N* Натурал санының жай сан екендігін тексеретін түрлі әдіс- тәсілдерді қарастырамыз. Алгоритмдік *N*– 1-ді жай сан екендігін тексеретін әдіс. Қазіргі уақытта біріншіден әдістердің сонымен қатар алгоритмдердің тиімділігін арттыру, криптографиялық құралдардың практикалық жүзеге асыруымен төзімділік негіздемесі секілді, криптографияның негізгі мәселелерінің бірі болып табылатын әдістерді ашуды дамыту үшін де маңызды. Бүтін сандардың жай сан екендігін тексеретін алгоритм, ең маңызды алгоритмдердің бірі болып табылады.

Түйінді сөздер: сандар теориясы, жай сандар, тест қарапайымдылығы, алгоритм Конягин-Померанс.

МРНТИ 27.31

А.К. Кудайкулов[1], А.А. Ташев[1], А.К. Жумадилдаева[1], Н. Курманбеккызы[1]

[1] Институт информационных и вычислительных технологий, Алматы, Казахстан

МЕТОДЫ ПОСТРОЕНИЯ РАЗРЕШАЮЩИХ СИСТЕМ УРАВНЕНИЙ НЕСТАЦИОНАРНОЙ ТЕПЛОПРОВОДНОСТИ СТЕРЖНЯ ОГРАНИЧЕННОЙ ДЛИНЫ С УЧЕТОМ НАЛИЧИЯ ЛОКАЛЬНОГО ТЕПЛОВОГО ПОТОКА, ТЕПЛООБМЕНА И БОКОВОЙ ТЕПЛОИЗОЛЯЦИИ

Аннотация: В статье рассмотрены постановка и вариационый подход решения нестационарной задачи распространения тепла в стержне при воздействии теплового потока и в условиях теплообмена, показано, что вариационный метод и метод Галеркина при решении нестационарной задачи распространения тепла в стержне приводят к