УДК 51

ОБ ОДНОМ КРИТЕРИИ ДЕЛИМОСТИ ЧИСЕЛ МЕРСЕННА

Ибрагимов Р., Уштенов Е.Р.

Южно-Казахстанский инженерно-педагогический университет Дружбы народов, Шымкент, e-mail: raskul1953@mail.ru

Проблемы простых чисел имеют историю нескольких веков.Одной из задач является определение чисел на простоту, т.е. является число простым или нет. Среди специальных простых чисел есть простые числа Мерсенна. И стоит вопрос их нахождения и определения их простоты. В этой статье рассматривается альтернативный метод проверки простоты числа Мерсенна методу Люка-Лемера и дается сравнительный анализ этих способов решения поставленной задачи.

Ключевые слова: простые числа Мерсенна, метод Люка-Лемера, критерии простоты числа, альтернативный метод

ONE CRITERION FOR DIVISIBILITY MERSENNE NUMBERS

Ibragimov R., Ushtenov Y.R.

South Kazakhstan Engineering and Pedagogical University of Friendship of Nations, Shymkent, e-mail: raskul1953@mail.ru

Problems of prime numbers have a history of century. One of the tasks is to determine the numbers of simplicity, is the a number of simple or not. Among the special primes have Mersenne primes. And there is a question of finding and determining their simplicity. This article discusses an alternative method of checking the simplicity of the method Mersenne Lucas-Lehmer and provides a comparative analysis of these methods to solve this problem.

Keywords: Mersenne primes, the method of Lucas-Lehmer, the criteria of simplicity, an alternative method

Простые числа Мерсенна относятся к специальным числам и играют важную роль в Теории чисел и имеют прикладное значение. В частности, на основе простых чисел Мерсенна создается генератор случайных чисел, являющихся базовыми элементами криптографии.

Числа вида

$$2^n - 1, \qquad (1.1)$$

где n – 1, 2, 3…, называются числами Мерсенна. Марен Мерсенн (1588–1648 гг.) – французский математик, физик, философ и богослов, теоретик музыки.

Если число $2^n - 1$ – простое, то это число называется простое число Мерсенна, а число n – простое число и записывается оно так:

$$2^p - 1, \qquad (1.2)$$

где p – простое число [9, 234].

В настоящее время известно 48 простых чисел Мерсенна. Это числа с показателями p: 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, … , и последнее 48-е число с показателем p = 55885161. Простые числа Мерсенна записывается так:

$$M_2 = 3, M_3 = 7, \ldots, M_{13} = 8191, \ldots \quad (1.3)$$

Первые 7 простых чисел были вычислены Мерсенном, простота числа M_{31} была доказана Л. Эйлером, а число M_{61} было вычислено русским математиком-самоучкой, священником И.М. Первушиным. Простые числа Мерсенна начиная с показателя p = 521 были вычислены электронными вычислительными машинами и суперсовременными компьютерами [9, 234–235; 11, 77–79].

Число простых чисел бесконечно. Первым это утверждение доказал древнегреческий математик в 3-м веке до н.э. Евклид, затем были доказательства Л. Эйлера и других математиков. Хотя простые числа Мерсенна удерживают лидерство среди всех известных простых чисел по размерности вопрос бесконечности простых чисел Мерсенна остается открытым. [4, 7–8; 5, 9–10; 6, 11–12; 7, 28–31].

Критерии простоты чисел Мерсенна

Необходимым условием простоты чисел $2^n - 1$ является простота числа n, ведь если число n – составное, то и число $2^n - 1$ – составное. Но это условие не является достаточным. На самом деле, числа M_{11}, M_{23}, M_{29} и многие другие числа Мерсенна с простыми показателями являются составными. В 1878 году французский математик Э. Люка нашел метод определения простоты чисел Мерсенна, а позже, в 1932 году американский математик Д.Х. Лемер упростил этот метод и поэтому он носит название Метода Люка-Лемера:

Число $M_p = 2^p - 1$, где p – простое число, является простым тогда и только тогда, когда $(p - 1)$-й член реккурентной последовательности

$$c_1 = 4, c_2 = 4^2 - 2 = 14, c_3 = 14^2 - 2 = 194, \ldots, c_k = c_{k-1}^2 - 2 \qquad (2.1)$$

делится на M_p, т. е. когда

$$c_{p-1} \equiv 0 (\mathrm{mod}\ M_p) \text{ [9, 234–235; 11,78–79]. } (2.2)$$

Этот метод является очень трудоемким, т.к. число M_p и число c_{p-1} при больших значениях p вырастают до гигантских численных значений и вследствие этого выполнение всех математических действий становится сложным. Например, для вычисления последнего найденного 48-го простого числа Мерсенна потребовались мощности 360-ти процессорных ядер в течении 39 суток, т.е. чуть менее одной тысячи непрерывных машинных часов. [http://www.46tv.ru/line/world/013649/, Great Internet Mersenne Prime Search].

Существуют также критерии проверки чисел Мерсенна на делимость.

Критерий делимости числа Мерсенна, установленный Л. Эйлером: если $p = 4n + 3$ и $q = 2p + 1 = 8n + 7$ оба простые, то

$$M_p \equiv 0 \pmod{q} \text{ [9, 235]} \qquad (2.3)$$

Критерий делимости чисел Мерсенна вида $p = 4n + 1$ не установлен, вследствие невозможности определения формулы числа q, и потому числа Мерсенна требуют общего критерия делимости и для чисел вида $p = 4n + 1$ и для чисел вида $p = 4n + 3$. В случае нахождения такого критерия появится возможность определения простоты числа Мерсенна, кроме метода Люка-Лемера. Но возможно ли такое?

Нахождение делителя числа Мерсенна

Л. Эйлер указал на обязательное условие делителя числа Мерсенна: это простое число имеет вид $2pk + 1$, где p – показатель степени, $k = 1, 2, 3, \ldots$, [9, 234–235].

На основании теоремы Ферма $a^p \equiv a(mod\ p)$ т.е. $2^p \equiv 2(mod\ p)$, имеем $2^p - 1 \equiv 1(mod\ p)$, [1, 44–46; 3, 757–761; 8, 47–48; 10, 90–91]. Поэтому второй сомножитель этого числа будет иметь также вид $2pk_2 + 1$, где – $k_2 = 1, 2, 3, \ldots$, причем $k \neq k_2$, иначе число $2^p - 1$ будет квадратом некоторого натурального числа, что невозможно изначально.

Итак, мы установили, что если число Мерсенна составное, то оно представимо в виде:

$$2^p - 1 = (2pk_1 + 1)(2pk_2 + 1). \qquad (3.1)$$

Примем, что $k_1 < k_2$, и, соответственно будет $2pk_1 + 1 < 2pk_2 + 1$, а вследствие этого

$$2pk_1 + 1 < \sqrt{2^p - 1}\,,\ 2pk_2 + 1 > \sqrt{2^p - 1}\,. \qquad (3.2)$$

Равенство (3.1) преобразуем:

$$2^p - 1 = (2pk_1 + 1)(2pk_2 + 1) = \\ = 4p^2k_1k_2 + 2pk_1 + 2pk_2 + 1, \qquad (3.3)$$

далее,

$$2^p - 2 = 2p(2pk_1 + k_1 + k_2), \qquad (3.4)$$

или

$$\frac{2^{p-1} - 1}{p} = 2pk_1k_2 + k_1 + k_2, \qquad (3.5)$$

или

$$2pk_1k_2 + k_1 + k_2 - \frac{2^{p-1} - 1}{p} = 0. \qquad (3.6)$$

Мы получили Диафантово уравнение 1-ой степени вида:

$$ax + by + cz + d = 0, \qquad (3.7)$$

где

$$a = 2p,\ x = k_1k_2,\ b = 1,\ y = k_1,\ c = 1,$$

$$z = k_2,\ d = -\frac{2^{p-1} - 1}{p}.$$

До настоящего времени это уравнение считается неразрешимым. В случае решения этого вида Диофантового уравнения будет решен вопрос определения простоты чисел Мерсенна. Эти задачи разрешимы в случае решения вопроса матричных операторов, составленных из коэффициентов вышеуказанного уравнения. Но таковых пока нет [2, 265–279; 10, 4–5].

Вернемся к первому неравенству в выражении (3.2) и преобразуем его:

$$2pk_1 + 1 < \sqrt{2^p - 1}\,,$$

т.е.

$$1 \le k_1 < \frac{\sqrt{2^p - 1} - 1}{2p}, \qquad (3.8)$$

и, пренебрегая единицами в последней формуле, получаем:

$$1 \le k_1 < \frac{2^{\frac{p}{2}-1}}{p}. \qquad (3.9)$$

Теперь подставляя значения k_1 от единицы до максимального значения в формулу $2pk_1 + 1$ и проводя операции до результата

$$M_p \equiv 0\left(mod\left(2pk_1 + 1\right)\right) \qquad (3.10)$$

получим первый наименьший простой делитель числа Мерсенна.

В противном случае, т.е. если при всех возможных значениях k_1 по формуле (3.9) получим

$$M_p \not\equiv 0(\mathrm{mod}(2pk_1 + 1)), \qquad (3.11)$$

то число M_p – простое.

Заключение

Практическое применение нашего способа лучше метода Люка-Лемера в том, что

при расчетах нет необходимости вычислять число Мерсенна, ведь оно содержит огромное число цифр. В нашем методе необходимо вести расчет до величины $\left(2pk_1+1\right)^2$, которое несопостовимо меньше самого числа Мерсенна.

При программном обеспечении расчет целезообразнее вести по формуле:

$$M_p+1\equiv 1\left(mod\left(2pk_1+1\right)\right), \qquad (4.1)$$

т.е.

$$2^p\equiv 1\left(mod\left(2pk_1+1\right)\right), \qquad (4.2)$$

так как число 2^p можно разделить по частям для облегчения расчетов. При программном обеспечении можно минимизировать число математических действий на основании свойств чисел Мерсенна и его делителей, что намного разгрузит компьютеры по сравнению с вычислениями по методу Люка-Лемера.

Список литературы

1. Davenport Harold. The Higher Arithmetic: An Introduction to the Theory of Numbers. Cambridge University Press, 1999.

2. Derbyshire John. Prime Obsession – Bernhard Riemann and the Greatest Unsolved Problem in Mathematicsa. Joseph Henry Press. Washington, D.C. 2003.

3. Gauss C.F. DisqnisitionesArithmeticae, 1801. Springer, 1986.

4. Ingham A.E. The Distributhionof Prime Numbers. Cambridge University Press, 1990.

5. Prachar K. Primzahlverteilung. Spinger-Verlag. Berlin, Gettingtn, Heidelberg. 1957.

6. Trost E. Primzahlen.Basel, Birkhauser, 1953.

7. Бухштаб А.А. Теория чисел. – М.: Издательство «Просвещение», 1966.

8. Виноградов И.М. Основы теории чисел. – Санкт-Петербург: Идательство Лань, 2009.

9. Михелович Ш.Х. Теория чисел. – М.: Издательство «Высшая школа», 1967.

10. Нестеренко Ю. В. Теория чисел. – М.: Издательский центр «Академия», 2008.

11. Серпинский В. Что мы знаем и чего не знаем о простых числах. – М., Ленинград, Государственное издательство физико-математической литературы, 1963.

12. Ushtenov E.R. «The central problem in number theory and the mean value theorem of primes up to a qiven number x». Журнал «Eastern European Scientific Journal», Германия, Дюссельдорф, Издат. Auris-Verlag, 2014. – № 5. – С. 215–232.

13. Ushtenov E.R., Akulbaev M.I. «Terms of primality of a number. Number theorem 2 of prime number criteria» Журнал «Life Science of Jornal». США. 2014. – № 11 6(S). – P. 90–92.

14. Уштенов Е.Р., Мамараимов М.Т. «Проблемы простых чисел и теорема о критерии простого числа». Журнал «THEORY AND PRACTICE IN THE PHISICAL, MATEMATICAL AND TECHNICAL SCIENES», Лондон, Великобритания, 3–13 мая, МАНВО. С. 16–18.

15. Акылбаев М.И., Уштенов Е.Р. « Новая теорема о критерии простого числа». Журнал «Международный журнал фундаментальных и прикладных исследований». – Москва, 2014. – № 1, часть 1. – С. 255–257. ISSN 1996-3955.

16. Ushtenov E.R., Mamaraimov M.T. «The new theorem on prime number criterion with few operaitions for the identification of prime number». Журнал «World Applied Sciences Journal». ISSN 1818-4952. Пакистан, Карачи, 29.05.2014 г. С. 655–659