УДК 511.17

ПРОСТЫЕ ЧИСЛА МЕРСЕННА

Бондаровец В.В, Доманькова В.В, студенты гр.473901

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Лобанок Л.В. – старший преподаватель кафедры высшей математики

Аннотация. Статья посвящена простым числам Мерсенна. В её рамках рассматривается их экспоненциальная природа и уникальная связь с совершенными числами. Отдельно рассматриваются основные методы их поиска и практические направления применения объекта исследования с приведением конкретных примеров. Выделяется значение простых чисел Мерсенна в математической науке.

Ключевые слова. Простые числа, совершенные числа, экспоненциальная природа, тест Люка-Лемера, распределенные вычисления, криптография.

Числа Мерсенна – это числа вида $2^n - 1$, где n – натуральное число. Простые из них – те, которые имеют только два делителя, то есть, делятся без остатка только на единицу и сами на себя. Такое определение им дал древнегреческий математик Евклид ещё в античности.

Он также исследовал связь между совершенными числами и числами вида $2^n - 1$ и сделал вывод, что если $\mathrm{M} = 2^n - 1$ — простое число, то число вида

$$N = 2^{n-1} \times \mathrm{M} \tag{1}$$

является совершенным.

Рассмотрим пример.

Для $n = 5$: $\mathrm{M} = 2^5 - 1 = 31$, $N = 2^{5-1} \times 31 = 496$.

Известно, что число является совершенным в том случае, если оно равно сумме своих собственных делителей.

Выполним проверку для числа $N = 496$:

Делители числа 496: 1, 2, 4, 8, 16, 31, 62, 124, 248.

Сумма делителей: $1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248 = 496$.

Следовательно, можно сделать вывод, что число 496 – совершенное.

Позже, в 1644 году, математик Марен Мерсенн, в чью честь названы исследуемые числа, составил список таких значений n, при которых, как он считал, числа вида $2^n - 1$ окажутся простыми. Некоторые из них в будущем оказались неверными в силу недостатка вычислительных мощностей его времени, однако его работа способствовала изучению математической науки в данном направлении.

Экспоненциальный рост.

Ранее было определено, что экспоненциальный рост характерен для величины, которая увеличивается пропорционально своему текущему значению согласно заданной функции

$$f(t) = a \times b^t \tag{2}$$

Значения простых чисел Мерсенна задаются функцией $2^n - 1$, следовательно, они экспоненциально зависят от n.

Это можно увидеть, рассмотрев следующие примеры:

$$\begin{gathered} \mathrm{M}_3 = 2^3 - 1 = 7; \\ \mathrm{M}_{31} = 2^{31} - 1 = 2{,}147{,}483{,}647; \\ \mathrm{M}_{61} = 2^{61} - 1 = 2{,}305{,}843{,}009{,}213{,}693{,}951. \end{gathered} \tag{3}$$

Методы поиска простых чисел Мерсенна.

На текущий момент основным способом проверки чисел на простоту является *тест Люка-Лемера*, его же называют наиболее эффективным. Данный метод основан на рекуррентной последовательности, задаваемой формулой

$$S_k = \left(S_{k-1}^2 - 2\right) mod M_n \tag{4}$$

при $S_0 = 4$.

Это значит, что каждый новый элемент последовательности будет равен остатку от деления разности квадрата предыдущего числа и двойки на проверяемое число. Если в результате вычисления последовательности одним из её членов окажется 0, это будет являться подтверждением верности нашего утверждения о том, что исследуемое число – простое число Мерсенна.

Используем тест Люка-Лемера, чтобы убедиться, что 31 действительно является простым числом Мерсенна.

$$S_1 = (4^2 - 2) mod 31 = (16 - 2) mod 31 = 14 mod 31 = 14;$$
$$S_2 = (14^2 - 2) mod 31 = (196 - 2) mod 31 = 194 mod 31 = 6;$$
$$S_3 = (6^2 - 2) mod 31 = (36 - 2) mod 31 = 34 mod 31 = 3;$$
$$S_4 = (3^2 - 2) mod 31 = (9 - 2) mod 31 = 7 mod 31 = 7;$$
$$S_5 = (7^2 - 2) mod 31 = (49 - 2) mod 31 = 47 mod 31 = 0. \quad (5)$$

В результате мы получили, что пятый член последовательности равен нулю, следовательно, доказали, что 31 – простое число Мерсенна.

С каждым новым таким числом количество знаков в них растет. Последнее, пятьдесят второе, обнаруженное число содержит в себе 41 024 320 цифр. Это значит, что проверка следующих чисел по алгоритму требует значительных вычислительных ресурсов и еще большего количества времени.

Для решения этой проблемы используется *метод распределенных вычислений*. Наиболее широко он применяется международным проектом GIMPS (Great Internet Mersenne Prime Search), созданным для централизованного поиска простых чисел Мерсенна в 1996 году. Данный метод заключается в распределении подзадач между компьютерами, что позволяет избежать создания суперкомпьютеров и значительно ускоряет обработку данных. Другими словами, пока одни компьютеры выполняют проверку числа тестом Люка-Лемера, другие занимаются факторизацией, поиском делителей (факторов) исследуемого числа для анализа его структуры. Более того, такой метод позволяет каждому желающему внести свой вклад вне зависимости от мощности конкретного компьютера.

Практическое применение.

Известно, что простые числа Мерсенна широко применяются, когда существует потребность в генерации числовых последовательностей, в частности, длинных, таких как секретные коды в сферах экономики и кибербезопасности.

Рассмотрим пример создания такой уникальной последовательности.

Выберем несколько случайных простых чисел Мерсенна в качестве основы для генерируемого кода. Возьмем 7, 31 и 127.

Следующим шагом могут быть любые математические операции над выбранными числами, такие как сложение и умножение. Проведем их: $31 \times 127 - 7 = 3930$.

Для повышения сложности допускается добавления прочих символов, например, букв латинского алфавита. Теперь код выглядит следующим образом: V7D – 3930.

Был рассмотрен простейший случай использования простых чисел Мерсенна, однако при работе с банковскими системами и коммуникациями могут использоваться гораздо более сложные комбинации.

Ключевым преимуществом изучаемых чисел в области шифрования является удобство для компьютерных вычислений, так как каждое из них в двоичной системе представляет собой ряд единиц. Например, число 31 будет иметь вид 11111.

Это и другие свойства простых чисел Мерсенна используются в криптографии с открытым ключом. Её суть заключается в существовании двух ключей: открытого и закрытого. Первым может пользоваться только владелец, а второй применяется всеми пользователями для шифрования или проверки цифровой подписи.

Наиболее широко распространен алгоритм RSA. В нем произведение двух простых чисел Мерсенна дает модуль

$$p = n_1 \times n_2 \quad (5)$$

который используется в открытом и закрытом ключах.

Например, пусть $n_1 = 2^{17} - 1 = 131071$ и $n_2 = 2^{19} - 1 = 524287$.

Вычисляем модуль $p = n_1 \times n_2 = 131071 \times 524287 = 68718952449$.

Далее необходимо выбрать число e, взаимно простое с функцией Эйлера $\varphi(n) = (p_1 - 1)(p_2 - 1) = 131070 \times 52426 = 68717451520$. Возьмем часто используемое $e = 65537$.

Для вычисления закрытого ключа необходимо взять такое d, что

$$d \times e \equiv 1 mod \varphi(n). \quad (6)$$

Выполняем подстановку: $d \times 65537 = 1 mod 68717451520$.

В результате вычислений получаем $d = 27551547937$.

Сформированные ключи будут иметь следующий вид:

Открытый ключ $(e, p) = (65537, 68718952449)$.

Закрытый ключ $(d, p) = (27551547937, 68718952449)$.

Владелец открытого ключа может зашифровать сообщение s:

$$c = s^e mod p. \quad (7)$$

Только тот, у кого есть закрытый ключ может его расшифровать:

$$s = c^d mod p. \quad (8)$$

Метод Диффи-Хеллмана – еще один криптографический алгоритм, позволяющий найти практическое применение простым числам Мерсенна. С его помощью пользователи имеют возможность создать общий секретный ключ. Особенно это может быть актуально, если до этого между пользователями не осуществлялся обмен информацией.

Для реализации этого алгоритма пользователи выбирают большое простое число n и небольшое число, основание g, а также собственные секретные числа a и b для генерации общего ключа.

Пусть $n = M_{13} = 8191$ и $g = 2$. Сторона 1 выбирает $a_1 = 6$, а сторона 2 — $a_2 = 15$.

Открытые ключи вычисляются по следующей формуле:

$$A = g^a mod n \quad (9)$$

После обмена получившимися значениями участники создают ключ, который будет известен обоим.

Сторона 1 вычисляет общий ключ, используя A_2 и своё секретное число a_1:

$$K = A_2^{a_1} mod n \quad (10)$$

Сторона 2 делает то же самое с использованиемA_1 и своего секретного числа a_2:

$$K = A_1^{a_2} mod n \quad (11)$$

Благодаря свойству $(g^a)^b \equiv (g^b)^a mod n$, обе стороны получают одинаковый общий ключ K.

Несмотря на простоту и эффективность использования простых чисел Мерсенна в шифровании, они имеют по крайней мере один существенный недостаток. В силу их небольшого количества и редкости на числовой прямой, существует относительно ограниченное количество возможных комбинаций, пригодных для использования в криптографии, поэтому их нельзя считать универсальными в применении.

Значение в математике.

Простые числа Мерсенна – ключевой элемент в исследовании свойств чисел. Их изучение вдохновляет ученых на развитие новых вычислительных методов и поиск математических закономерностей, таких как связь с совершенными числами. Более того, благодаря открытию чисел Мерсенна, был разработан алгоритм Люка-Лемера, который в последствии стал фундаментом для их поиска.

Как было упомянуто, все простые числа Мерсенна представлены в двоичной системе в виде единиц. Такая структура позволяет в разумные сроки обрабатывать даже самые крупные значения, в частности, в рамках криптографических вычислений.

Тем не менее, есть ряд вопросов по теме, на которые математики пока не могут ответить. Остаётся неизвестным, бесконечна ли последовательность чисел Мерсенна, а также существует ли

закономерность их роста. Помимо этого, в настоящее время проводятся исследования относительно связи простых чисел Мерсенна с другими типами простых чисел, таких как числа Ферма, имеющих вид $2^{2^n}+1$. Существует предположение, что тот факт, что каждое простое число Мерсенна связано с совершенным, обязательно четным, может являться ключом к разгадке существования нечетного совершенного числа.

Список использованных источников:

1. Простые числа Мерсенна [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/prostye-chisla-mersenna/viewer. – Дата доступа: 30.03.2025.

2. О простых числах в информационной безопасности [Электронный ресурс]. – URL: http://textovod.com/unique/link?url=https%3A%2F%2Fnsportal.ru%2Fap%2Flibrary%2Fdrugoe%2F2013%2F08%2F07%2Fo-prostykh-chislakh-v-informatsionnoy-bezopasnosti&key=83215977e9311b1ea15cbe4a20703915. – Дата доступа: 30.03.2025.

3. Первые шаги в мир больших чисел: простые числа [Электронный ресурс] / Хабр. – URL: https://habr.com/ru/articles/853816/. – Дата доступа: 30.03.2025.

UDC 511.17

MERSENNE PRIMES

Bondarovets V.V., Domankova V.V., students gr.473901

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Lobanok L.V. – Senior Lecturer at the Department of Higher Mathematics

Annotation. The article is devoted to Mersenne primes. It examines their exponential nature and their unique relationship to perfect numbers. The main methods of their search and practical directions of application of the object of research are considered separately, with specific examples. The importance of Mersenne primes in mathematical science is highlighted.

Keywords. Primes, perfect numbers, exponential nature of the Luc-Lemaire test, distributed computing, cryptography.