DOI: 10.17117/na.2015.12.02.451

<http://ucom.ru/doc/na.2015.12.02.451.pdf>

Поступила (Received): 01.12.2015

Нугманов Д.Т., Перминов П.В., Шабля Ю.В., Кручинин Д.В. Простые числа в современном мире

Nugmanov D.T., Perminov P.V., Shablya Yu.V., Kruchinin D.V.
Primes in the modern world

Данная работа посвящена простым числам, истории их открытия и развития, а также проблемам, связанным с ними. Значительное внимание уделяется актуальной на сегодняшний день проблеме поиска простых чисел. Данная проблема мало изучена и требует дальнейших исследований

Ключевые слова: простые числа, тест на простоту, криптография

This work is devoted to prime numbers, the history of their discovery and development, and problems associated with them. Considerable attention is paid to a problem of finding prime numbers. This problem is poorly understood and requires further research

Key words: primes, primality test, cryptography

Нугманов Данияр Тахирович

Студент

Томский государственный университет систем управления и радиоэлектроники

г. Томск, ул. Красноармейская, 146

Nugmanov Daniyar Tahirovich

Student

Tomsk state university of control systems and radioelectronics

Tomsk, Krasnoarmeyskaya st., 146

Перминов Петр Витальевич

Студент

Томский государственный университет систем управления и радиоэлектроники

г. Томск, ул. Красноармейская, 146

Perminov Peter Vitalievich

Student

Tomsk state university of control systems and radioelectronics

Tomsk, Krasnoarmeyskaya st., 146

Шабля Юрий Васильевич

Аспирант

Томский государственный университет систем управления и радиоэлектроники

г. Томск, ул. Красноармейская, 146

Shablya Yuriy Vasilievich

Graduate

Tomsk state university of control systems and radioelectronics

Tomsk, Krasnoarmeyskaya st., 146

Кручинин Дмитрий Владимирович

Младший научный сотрудник

Томский государственный университет систем управления и радиоэлектроники

г. Томск, ул. Красноармейская, 146

Kruchinin Dmitry Vladimirovich

Jr. Researcher

Tomsk state university of control systems and radioelectronics

Tomsk, Krasnoarmeyskaya st., 146

Введение

Простые числа – это целые натуральные (положительные) числа больше единицы, которые имеют ровно 2 натуральных делителя (только 1 и самого

себя), т.е. не делится ни на одно другое число, кроме самого себя и единицы. Все остальные числа, кроме единицы, называются составными. Простые числа обладают рядом свойств, например: множество простых чисел бесконечно (т. е. среди простых чисел нет наибольшего); среди простых делителей составного числа есть хотя бы один, квадрат которого меньше или равен данному составному числу.

История открытия простых чисел

Сложно сказать, когда люди впервые задумались о простых числах, ученые предполагают, что это произошло более двадцати тысяч лет назад. Но именно Пифагор предложил число, как первоначало, как связующий элемент между окружающей действительностью, воспринимаемой органами чувств, и человеческим разумом. Пифагор и его ученики изучали вопрос о делимости чисел. Эратосфен в III в. до н. э. предложил первый метод поиска, который позволял найти все простые числа в любом числовом отрезке. Метод был назван «решетом Эратосфена», алгоритм данного метода заключается в нахождении всех простых чисел не больше заданного числа n . Следуя методу Эратосфена, нужно выполнить следующие шаги:

1. Выписать подряд все целые числа от двух до n (2, 3, 4, ..., n).
2. Пусть переменная p изначально равна двум – первому простому числу.
3. Зачеркнуть в списке числа от $2p$ до n считая шагами по p (это будут числа кратные p : $2p, 3p, 4p, \dots$).
4. Найти первое незачеркнутое число в списке, большее чем p , и присвоить значению переменной p это число.
5. Повторять шаги 3 и 4, пока возможно.

Теперь все незачеркнутые числа в списке – это все простые числа от 2 до n .

Следуя этому методу, выясняется, что постепенно простые числа встречаются все реже и реже, но уже тогда ученым было понятно, что простых чисел бесконечно много. Доказательства приводятся в «Началах» Евклида [1]. Пьер Ферма (1601–1665), занимаясь арифметикой целых чисел, вывел критерий, определяющий простоту числа – «Малая теорема Ферма» (была открыта в 1640 году). Теорема утверждает что: «Если P – простое число, a – целое число, то $a^P - a$ делится на P .»

Бернхард Риман выдвинул теорию о том, что распределение простых чисел – а это центральная проблема теории чисел – зависит от того, где дзета-функция обращается в нуль. У нее есть так называемые тривиальные нули – в четных отрицательных числах ($-2, -4, -6, \dots$). Задача состоит в том, чтобы описать все остальные нули дзета-функции.

Также простыми числами занимались знаменитые ученые, такие как: Леонард Эйлер (1707–1783), Петер Лежен Дирихле (1805–1859), Пафнутий Чебышев (1821–1894). Все их работы берут свое начало с арифметики древних ученых. Каждый из них доказывал и усовершенствовал теоремы ученых предшественников, стараясь упростить алгоритм нахождения простых чисел, но при этом находить новые, более крупные простые числа.

На сегодняшний день применяются теоремы Е.М. Райта, теоремы Мерсенна и Ферма, метод под названием «скатерть Улама», тест Рабина-Миллера и другие.

В связи с тем, что используемые методы проверки простоты вероятностные, поиск надежного и быстрого теста на простоту остается актуальной задачей.

Простые числа в Криптографии

Наиболее широкое применение простые числа нашли в криптографии, для создания открытого ключа, который защищает персональные данные, которые хранятся на всевозможной электронно-цифровой технике. Для получения надежного и трудно дешифруемого ключа и сохранения информации используются простые числа, имеющие в своем составе более трех сотен цифр. Наиболее яркий пример использования простых чисел в криптографии – это асимметричная криптосистема RSA, созданная в 1977 и названная по первым буквам ее авторов (Рональд Ривест, Ади Шамир и Леонард Адлеман) и получившую вскоре повсеместное распространение. В ее основу были положены свойства простых чисел. Система RSA, прежде всего, предполагает выбор некоторого числа $n=p \cdot q$, где p, q – простые числа. Кроме того, выбирается число e , не имеющее общих делителей с величиной $\phi(n)=(p-1) \cdot (q-1)$. Затем определяется число d таким образом, чтобы величина $d \cdot e - 1$ делилась бы без остатка на $\phi(n)$. Пара (e, n) представляет собой открытый ключ, а (d, n) – секретный ключ. Для получения зашифрованного текста исходное число s (имеющийся текст) возводится в степень e и результат делится на n . То, что получится в остатке от этого деления и есть зашифрованный текст (число) $t=E(s)$. Обратная процедура аналогична. Число t (зашифрованное сообщение) возводится в степень d и результат вновь делится на n . Остаток от этого деления и есть расшифрованный текст, т.е. исходное сообщение $s = D(t)$ [2,3].

Также простые числа могут быть использованы при построении генераторов псевдослучайных чисел или хэш-функций (вихрь Мерсенна).

Заключение

К сожалению, на сегодняшний день вопрос простых чисел является основным нерешенным вопросом целочисленной арифметики, и исследования в данной области имеют высокую научную ценность.

Проблема заключается в определении, является ли заданное натуральное число простым. Решение данной проблемы принято делить на следующие три основные задачи:

- построение простых чисел (на данный момент актуально при построении огромных простых чисел, применяемых в некоторых криптографических системах);
- проверка натуральных чисел на простоту (поиск наиболее эффективного и точного метода тестирования числа на простоту);
- факторизация чисел (разложение числа на простые множители).

Поиск новых подходов определения простоты числа является актуальной задачей, решение которой имеет большее техническое и экономическое значение и позволит улучшить работу современных криптографических систем.

Список используемых источников:

1. Евклид. Начала, кн. VII-X. М.-Л.: ГИТТЛ, 1949. 510 с.
2. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. М.: МЦНМО, 2002. 104 с.
3. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2003. 328 с.

© 2015, Нугманов Д.Т., Перминов П.В.,
Шабля Ю.В., Кручинин Д.В.
Простые числа в современном мире

© 2015, Nugmanov D.T., Perminov P.V.,
Shablya Yu.V., Kruchinin D.V.
Primes in the modern world