

Введение

Математика удивительна. С одной стороны, предметом ее непосредственного исследования являются исключительно абстрактные понятия, продукты человеческого разума, отсутствующие как таковые в окружающем нас мире. Действительно, доводилось ли кому-либо видеть своими глазами число (не три дерева и не три яблока, а само число 3) или плоскость (не плоский объект, а саму плоскость), не говоря уже об уравнении, функции, интеграле или множестве? А ничем иным математика как будто и не занимается... С другой стороны, математические понятия удивительнейшим образом оказываются пригодными для исследования окружающего мира. Многие абстрактные математические объекты, возникшие, казалось бы, исключительно исходя из внутренних потребностей самой математики, неожиданно проявляются в таких сферах, о которых творцы этих понятий не могли даже и помыслить. К примеру, мог ли догадаться в 16 веке Джероламо Кардано, вводя комплексные числа в связи с естественными запросами теории алгебраических уравнений, что через сотни лет они найдут приложения в гидродинамике или квантовой механике? Едва ли Эйлер, Якоби или Кэли, разрабатывающие основы теории матриц, руководствуясь, главным образом, логикой развития линейной алгебры, могли предвидеть матричную механику Гейзенберга. Эллиптическая геометрия Римана появилась как естественное логическое дополнение к уже известным геометриям Евклида и Лобачевского и никак не предвещала общую теорию относительности. Но, может быть, наиболее удивительный пример такого рода дает едва ли не самая древняя, самая сложная и самая абстрактная математическая дисциплина – теория чисел. Речь идет о простых числах, которые были введены примерно две с половиной тысячи лет назад, и нашли неожиданное практическое применение совсем недавно. В данной работе в популярной форме рассказывается о развитии теории простых чисел и ее приложении к криптографии.

1. Развитие теории простых чисел

Возникновение теории чисел принято связывать с именем великого греческого мыслителя **Пифагора**. Жил он в шестом веке до нашей эры и был современником Конфуция и Лао Цзы, Будды и Заратуштры, а также ряда библейских пророков. Будучи, главным образом, философом, Пифагор искал естественную связь между окружающей действительностью, воспринимаемой органами чувств, и человеческим разумом, познающим мир. Согласно Пифагору, таким связующим звеном и является *число*. Действительно, с одной стороны, число есть вполне абстрактное понятие, являющееся продуктом нашего мозга. Но, с другой стороны, всё, происходящее в мире, может быть в той или иной степени измерено, а значит, представлено в числах. Главная мысль Пифагора: в мире царит гармония, и выражена эта гармония – в числах. А отсюда следовало, что для того чтобы прикоснуться к этой гармонии, нужно изучать числа.

Конечно, с числами люди сталкивались в повседневной жизни задолго до Пифагора. Однако смотрели на них исключительно как на средство решения тех или иных практических задач. Пифагор же провозгласил, что числа, будучи основой всего сущего, должны быть непосредственной целью исследования. Возможно, это и стало началом всей математики...

Первые шаги, связанные с исследованием любого класса объектов, обычно направлены на выявление присущих им специфических свойств. Стоило взглянуть на числа, как на непосредственный предмет исследования, как выяснилось, что они в чем-то различаются между собой.



Пифагор
6 в. до н.э.

Сразу же бросается в глаза то естественное обстоятельство, что их можно сравнивать между собой: 5 больше, чем 2, но меньше, чем 10. Собственно, на этом и основано их практическое применение... Существенно более глубоким свойством оказывается возможность разложения чисел на более простые (меньшие по значению) сомножители. Понятно, что любое число делится без остатка само на себя и на единицу. Однако подавляющее большинство чисел имеют и качественно иные представления, например, $8 = 2 \cdot 4$ или $15 = 3 \cdot 5$. Таким образом, все числа (речь, понятно, идет о натуральных числах: 1, 2, 3, ...) можно разбить на два класса. *Простые числа* допускают только тривиальное представление, а *составные числа* разлагаются в произведение простых сомножителей. Упомянутые выше числа 8 и 15 естественно оказываются составными. Простыми числами являются 2, 3, 5, 7, 11, 13, 17 и т.д. Число 1 играет особую роль, к простым числам относить его не принято.

Первым делом хотелось бы узнать, как много имеется простых чисел? Ответ на этот вопрос дается **Евклидом**, жившем в третьем веке до нашей эры в Александрии. В его знаменитых "*Началах*" приводятся следующие рассуждения. Предположим, что существует лишь конечное множество простых чисел, исчерпывающиеся значениями $p_1, p_2, \dots, p_k$. Тогда число

$$p = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$$

никак не может делиться без остатка на выше указанные числа, поскольку непременно имеет единицу в качестве такового остатка. Отсюда следует, что число p само является простым, а значит, предположение о том, что все простые числа перечислены в указанном выше перечне, не соответствует действительности. Тем самым множество простых чисел оказывается бесконечным. С Евклидом связана также и *основная теорема арифметики*, согласно которой любое натуральное число (кроме 1) однозначно разлагается в произведение простых чисел, например, $12 = 2 \cdot 2 \cdot 3$, а $35 = 5 \cdot 7$.

Следующей и существенно более сложной проблемой было нахождение алгоритма построения простых чисел. Такой способ дал **Эратосфен**, живший на рубеже 3 и 2 веков до нашей эры в той же Александрии и прославившийся своими измерениями длины дуги земного меридиана. Эратосфен предложил *метод решета*, позволяющий найти все простые числа, не превосходящие данного числа n , и состоящий в следующем. На первом шаге процесса записываются подряд все числа, начиная с 2 и кончая n . Выбирается первое число из списка, т.е. 2, являющееся первым простым числом. На втором шаге отсеиваются все числа, кратные 2, т.е. все четные числа. Выбирается ближайшее к 2 из оставшихся чисел, т.е. 3. Оно оказывается вторым простым числом. На третьем шаге отсеиваются все числа, которые делятся на 3. Ближайшее, к 3 из оставшихся чисел, т.е. 5 будет третьим простым числом и т.д. В табл. 1 приведена схема построения простых чисел согласно решету Эратосфена для $n = 20$. Очевидно, уже после третьего шага здесь остаются только простые числа: 2, 3, 5, 7, 11, 13, 17, 19.



Евклид
4 в. до н.э.



Эратосфен
3 в. до н.э.

Табл. 1. Решето Эратосфена. Построение простых чисел не более 20.

шаг 1	2	3	<u>4</u>	5	<u>6</u>	7	<u>8</u>	9	<u>10</u>	11	<u>12</u>	13	<u>14</u>	15	<u>16</u>	17	<u>18</u>	19	<u>20</u>
шаг 2	2	3		5		7		<u>9</u>		11		13		<u>15</u>		17		19	
шаг 3	2	3		5		7				11		13				17		19	

Значительный вклад в теорию чисел внес великий французский математик **Пьер Ферма**, живший в 17 веке. Помимо знаменитой *теоремы Ферма* (уравнение $x^n + y^n = z^n$, для любого $n > 2$ не имеет решения в целых числах), доказанной совсем недавно, ему принадлежит также *малая теорема Ферма*, согласно которой, если числа a и p не имеют общих делителей (кроме, естественно, единицы), а число p простое, то значение a^{p-1} при делении на p имеет остаток 1; утверждение о том, что любое простое число вида $4n+1$ представляет собой сумму двух квадратов и многие другие результаты. Ферма принадлежит также идея *генератора простых чисел*, т.е. такой функции $f = f(n)$ целочисленного аргумента, которая при любом n имеет значением исключительно простые числа. В частности, он выдвинул гипотезу о том, что таковой может оказаться функция $f(n) = 2^{2^n} + 1$.



Пьер Ферма
1601 – 1665

За свою жизнь Ферма, профессиональный юрист, занимающийся математикой в свободное от основной работы время, не опубликовал ни одного труда. Подавляющее большинство его утверждений были приведены без какого-либо доказательства. И лишь через сто лет нашелся математик, сумевший обосновать практически все результаты Ферма, исключая его основную теорему, но и для нее им было дано доказательство для значения $n = 3$. Это был крупнейший математик 18 века **Леонард Эйлер**. Помимо всего прочего, он установил, что предложенная Ферма функция может принимать не только простые значения (простые значения указанной функции называют *числами Ферма*). Самому же Эйлеру удалось подобрать удивительно простую функцию $f(n) = n^2 + n + 41$, которая принимает простые значения при $n = 0, \dots, 39$. Однако справедливо равенство $40^2 + 40 + 41 = 41^2$. Среди других результатов отметим *тождество Эйлера*:



Леонард Эйлер
1707 – 1783

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - 1/p^s},$$

включающее числовой параметр s . Особенностью данного равенства является то обстоятельство, что в левой его части находится сумма по всем натуральным числам, в то время как в правую часть входит произведение по всем простым числам. В этой связи выражение, входящее в его левую часть и называемое *дзета-функцией* (от параметра s), играет большую роль в теории простых чисел. Действительно, любое свойство дзета-функции, непосредственным образом не опирающееся на понятие простого числа, посредством тождества Эйлера дает информацию о простых числах. В частности, при $s = 1$ выражение в левой части этого выражения (т.е. значение дзета-функции в единице) представляет собой *гармонический ряд*, который, как известно, расходится. Отсюда уже следует бесконечность множества простых чисел, поскольку в противном случае выражение в левой части тождества Эйлера конечно и никак не может служить суммой расходящегося ряда.

Значительный вклад в теорию простых чисел внес немецкий математик **Петер Лежен Дирихле**, живший в первой половине 19 века. Помимо доказательства теоремы Ферма для $n = 5$ он установил, что если первый член a и разность b арифметической прогрессии не имеют общих делителей, то она содержит бесконечно много простых чисел, т.е. среди элементов последовательности $\{p_k\}$, где $p_k = a + bk$, простые числа встречаются бесконечно часто. К примеру, при $a = 2$, $b = 3$ имеем набор



Петер Лежен Дирихле
1805 – 1859

2, 5, 8, 11, 14, 17, 20, 23, 26, 31, 34, 37, 40, 43, 46, 49, 52, 61, ...

где жирным шрифтом выделены простые числа. Таким, образом, простых чисел не просто бесконечно много. Их уже бесконечно много даже в одной единственной приведенной выше арифметической последовательности. А подобных последовательностей самих по себе бесконечно много. Другой заслугой Дирихле является определение *асимптотических законов* изменения теоретико-числовых функций (функций натурального аргумента с натуральными значениями). В частности, под асимптотическим законом функции f понимается такая более простая функция g , для которой при неограниченном возрастании аргумента их отношение стремится к единице, т.е. $f(n)/g(n) \rightarrow 1$ при $n \rightarrow \infty$.

После Дирихле центральной проблемой теорией простых чисел становится нахождение асимптотического закона *распределения простых чисел*, т.е. функции $\pi = \pi(n)$, характеризующей число простых чисел, не превосходящих данного числа n . Первые идеи в этом направлении были высказаны ранее **Карлом Фридрихом Гауссом** и **Адриеном Мари Лежандром**, которые предположили (фактически, на базе эмпирического анализа), что распределение простых чисел носит логарифмический характер. Более строгий результат был получен выдающимся русским математиком **Пафнутием Львовичем Чебышевым**, которой установил следующее соотношение

$$A \frac{n}{\ln n} \leq \pi(n) \leq B \frac{n}{\ln n},$$

называемое *неравенством Чебышева*, где $A > \ln 2 / 2$, $B < 2 \ln 2$.

Согласно этому результату искомая функция π растёт практически так же, как и четко описанная функция $g(n) = n / \ln n$ (см. табл. 2).



Пафнутий Чебышев
1821 – 1894

Табл. 2. Соотношение между функциями π и $g(n) = n / \ln n$.

n	π	$g(n) = n / \ln n$
3	2	2.7
5	3	3.1
10	4	4.3
20	8	6.7
30	10	8.8
50	15	12.8
70	19	16.5
100	26	21.7

Кроме того, Чебышев дал обоснование *постулату Бертрана*, утверждающему о том, что между числами n и $2n-2$ при $n > 3$ есть простое число (см. табл. 3).

Табл. 3. Постулат Бертрана (наличие простых чисел между n и $2n-2$ при $n > 3$).

n	$2n-2$	простые
4	6	5
5	8	7
6	10	7
7	12	11
8	14	11, 13
9	16	11, 13

Существенный прорыв в исследовании закона распределения простых чисел связан с учеником Дирихле, **Бернхардом Риманом**. Внесший колоссальный вклад в геометрию, математический анализ, математическую физику, будучи одним из основоположников топологии, Риман написал одну небольшую статью по теории чисел, которая до сих пор будоражит умы ведущих математиков. Решающим шагом здесь было рассмотрение дзета-функции с комплексным значением аргумента (у Эйлера аргумент был действительным). Последствия оказались настолько значительными, что указанную функцию с тех пор стали называть *дзета-функцией Римана*. Установив ряд особенностей этой функции, Риман далее приводит без доказательства



Бернхард Риман
1826–1866

несколько ее удивительных свойств, имеющих чрезвычайно большое значение для понимания природы простых чисел. Больше статей в этой области он не написал.

Риман умер в расцвете творческих сил в возрасте 39 лет. Осталась лишь запись в его бумагах: *"Эти свойства дзета-функции выводятся из одного из ее выражений, которое я не сумел достаточно упростить, чтобы опубликовать"*. И дальше лучше всего процитировать известного французского математика **Жака Адамара**, внесшего значительный вклад в данную теорию. *"Мы и сейчас не имеем ни малейшего понятия о том, что могло бы представлять собой это выражение! Что же касается свойств, простой формулировкой которых он ограничился, то мне потребовалось десятка три лет, чтобы я смог их доказать – все, кроме одного"*. В 1890 году Парижская академия наук учредила премию за обоснование асимптотического закона распределения простых чисел. Эту премию получили упоминавшийся выше Адамар, а также бельгийский математик **Шарль Ла Валле Пуссен**. Среди доказанных ими утверждений Римана следует отметить соотношение

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{n / \log n} = 1,$$

говорящее о том, что с ростом n функция $\pi = \pi(n)$ (количество простых чисел, не превосходящих n) возрастает так же, как отношение $n / \ln n$, задающее тем самым асимптотический закон распределения простых чисел. Неравенство Чебышева оказывается лишь приближенной формой указанного условия.

Однако оставалось не доказанным еще одно из утверждений Римана. Речь идет о тех значениях комплексного числа s , в которых дзета-функция обращается в нуль. Достаточно легко показывается, что таковыми являются все отрицательные четные значения, т.е. $s = -2, -4, -6, \dots$. Но существует и нетривиальные нули этой функции, которые особо важны для понимания закона распределения простых чисел. Согласно Риману все такие значения s имеют вид $\frac{1}{2} + it$, где i есть мнимая единица, а t – действительное число. Таким образом, все *нетривиальные нули дзета-функции* имеют число $\frac{1}{2}$ в качестве своей действительной части. Если верить процитированной выше фразе Римана, то это совершенно не тривиальное утверждение является следствием некоего загадочного выражения, которое Риман получил, но не рискнул опубликовать без предварительного упрощения. А затем, как мы знаем, Риман умер сравнительно молодым, так и не успев опубликовать больше ни одной статьи в области теории чисел. История теоремы Ферма повторяется...

Как развивались события дальше? В 1900 году **Давид Гильберт** сформулировал 23 важнейшие математические проблемы 20 века. Среди них достойное место занимает проблема нетривиальных нулей дзета-функции Римана. **Герман Минковский**, основоположник геометрической теории чисел, выпуклого анализа и геометрии Минковского назвал гипотезу Римана важнейшей проблемой всей математики.

Шел двадцатый век... Одна за другой решались знаменитые проблемы Гильберта. Под конец века была, наконец, доказана великая теорема Ферма. В 2000 году были

сформулированы математические проблемы тысячелетия (Millennium Prize Problems), за решение любой из которых Математический институт Клея (США) готов выделить премию в размере одного миллиона долларов. В их число вошла и гипотеза Римана, единственная из списка Гильберта, перешедшая из разряда проблем 20 века в ряд проблем нового тысячелетия. В настоящее время она остается, по-видимому, самой известной из пока не решенных математических проблем.

Итак, мы дали краткий исторический обзор развития одного из абстрактнейших математических направлений – теории простых чисел. И кто бы мог подумать, что это направление во второй половине двадцатого века найдет серьезное практическое применение. Дело дошло до того, что многие крупнейшие специалисты по теории чисел неожиданно нашли чрезвычайно высоко оплачиваемые и глубоко засекреченные должности в военных ведомствах и богатейших компаниях ведущих мировых держав. И здесь мы должны обратиться к одному из важнейших разделов информатики – к криптографии.

2. Простые числа и криптография

С проблемой защиты информации люди столкнулись в глубокой древности. При передаче важного сообщения на расстояние хотелось бы иметь уверенность в том, что информация эта будет в полной степени понята адресатом, но никак не посторонними лицами. Всегда приходилось считаться с возможностью того, что переданное послание будет перехвачено тем, кому его никак нельзя раскрывать. От умения тайно передавать свое сообщение и раскрывать секретные замыслы противника зачастую зависела судьба государства. В связи с этим постоянно совершенствовались применяемые шифры, что приводило к необходимости использовать более эффективные методы дешифровки, что, в свою очередь, стимулировало появление еще более изощренных принципов шифрования. Постепенно стало ясно, что серьезное решение указанных проблем является уделом высоко квалифицированных математиков. Так, над принципами составления шифров и методами чтения зашифрованных текстов работали, к примеру, **Джероламо Кардано** и **Франсуа Виет**, стоявшие у истоков математики нового времени. В двадцатом веке значительный вклад в это направление внесли **Алан Тьюринг** и **Клод Шеннон** – основоположники теоретической информатики. С появлением современных компьютеров проблема защиты информации стала особенно актуальной. Постепенно сформировалась *криптология*, относящаяся к классу информационных наук, и состоящая из *криптографии*, занимающейся способами преобразования информации с целью ее защиты от незаконных пользователей, и *криптоанализа*, целью которого является разработка методов вскрытия шифров.

Шифрование текста осуществляется с помощью некоторого способа преобразования информации, т.е. *ключа*. Для чтения зашифрованной информации надо выполнить соответствующее обратное преобразование. Однако здесь следует иметь в виду то обстоятельство, что разработка секретного ключа и шифровка с его помощью имеющегося сообщения еще не решает всех проблем. Если речь идет об однократном сообщении, то таковое может быть передано с помощью *одноразового ключа*, заранее известного получателю информации и, как показал Шеннон, практически не поддающегося вскрытию. Необходимость многократной пересылки сообщений значительных размеров существенно повышает вероятность перехвата информации с ее последующей дешифровкой. В этой связи возникает необходимость в периодической смене ключа. Однако в этих условиях особо остро встает вопрос о том, как передать получателю информации новый ключ. При использовании *симметричной криптосистемы*, когда для шифрования и дешифрования информации применяется один и тот же ключ, необходимо иметь чрезвычайно надежный канал связи для передачи партнеру теперь уже самого ключа. Сообщение о смене ключа само по себе должно передаваться, видимо, с помощью особого сверхсекретного ключа. А если (при длительной переписке) возникнет необходимость и в смене последнего?

Во избежание выше указанных трудностей в 1976 г. американские математики **Уитфилд Диффи** и **Мартин Хеллман** выдвинули концепцию *асимметричной криптосистемы*. В этом случае процедуры шифрования и дешифрования осуществляется с помощью различных ключей, причем шифровка осуществляется с помощью *открытого ключа*, а чтение зашифрованного сообщения – с помощью *секретного ключа*. При этом получатель информации сам разрабатывает оба ключа, причем ключ для шифрования передается партнеру совершенно открыто. С его помощью можно закодировать сообщение, но никак не прочесть его. Перехват противником открытого ключа не наносит серьезного ущерба, поскольку расшифровать полученную информацию может только обладатель секретного ключа, который вообще никому не передается. Открытый и секретный ключи, естественно, связаны между собой, а иначе они не могли бы быть использованы для работы с одним и тем же сообщением. Однако их связь должна быть столь изощренной, чтобы знание одного из них практически не могло бы раскрыть второй. Асимметричные криптосистемы отличаются высокой надежностью. Но их еще предстояло разработать...

В 1977 г. американцы **Рональд Ривест**, **Ади Шамир** и **Леонард Адлеман** разрабатывают асимметричную *криптосистему RSA*, названную по первым буквам ее авторов (Rivest, Shamir, Adleman) и получившую вскоре повсеместное распространение. В ее основу были положены свойства простых чисел.

Итак, у нас есть некоторый текст, подлежащий шифровке. Любой символ из текста (буква, цифра, знак препинания, какой-либо специальный символ) может быть стандартным образом закодирован в виде некоторого числа (так, в компьютере каждый символ имеет свою стандартную кодировку). Записывая эти числа подряд одно за другим, мы можем представить данное сообщение в виде некоторого достаточно большого (обычно, чрезвычайно большого) числа s , которое, собственно и подлежит кодированию. Процесс шифровки текста предполагает выполнение над ним некоторой кодирующей процедуры E (*encoding*), в результате чего получается другое число $t = E(s)$. Расшифровка закодированного текста подразумевает восстановление по закодированному тексту t исходного текста s , т.е. выполнении обратного преобразования D (*decoding*), такого, что $s = D(t)$.

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 $\varphi(n) = (p-1) \cdot (q-1)$. Затем определяется число d таким образом, чтобы величина $d \cdot e - 1$ делилась бы без остатка на $\varphi(n)$. 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 $s = D(t)$.

Попробуем воспользоваться указанной методикой для шифровки и дешифровки достаточно короткого сообщения на примере чрезвычайно простых ключей. Определим простые числа $p = 3, q = 7$, которым соответствует произведение $n = p \cdot q = 21$. Вычисляем значение $\varphi(n) = (p-1) \cdot (q-1) = 2 \cdot 6 = 12$. Выбираем, к примеру, число $e = 23$, не имеющее общих делителей с величиной $\varphi(n) = 12$. Теперь предстоит определить число d так, чтобы разность $d \cdot e - 1$ делилась бы без остатка на $\varphi(n)$, а значит, имело бы вид $12k$, где k есть некоторое натуральное число. Таким образом, искомое целое число d должно быть таким, чтобы выполнялось равенство $23d = 12k + 1$ для некоторого значения k . В силу относительной малости рассматриваемых чисел эту задачу можно без труда решить простым перебором параметров, т.е. рассматривая наборы чисел вида $23d$ и

$12k+1$ до тех пор, пока в указанных наборах не появится одно и то же число. К числам первого класса относятся значения 23, 46, 69, 93, 115, 138, 161, 184, 207, 230, 253,..., а к числам второго класса – 13, 25, 37, 49, 61, 73, 85, 97, 109, 121, 133, 145, 157, 169, 181, 193, 205, 217, 229, 241, 253,... Мы видим, что число 253 появляется сразу в обоих списках, будучи, с одной стороны, равным произведению $23 \cdot 11$, а, с другой стороны – величине $12 \cdot 21 + 1$. Таким образом, в качестве d выбирается значение 11. Итак, в нашем случае получается открытый ключ (23,21), и секретный ключ (11,21).

Рассмотрим некоторое сообщение (число), которое подлежит шифровке, например, $S = 10051602$. Поскольку оно превосходит величину $n = 21$ (размер ключа, как правило, много меньше длины передаваемого сообщения), то мы разбиваем величину S на части (пары) 10, 05, 16, 02, каждая из которых кодируется самостоятельно. Результат шифрования приводится в табл. 4. Здесь в первом столбце s приводятся перечисленные выше части данного сообщения (например, в последней строке – значение 02). Второй столбец дает результат s^e возведения данного числа s в степень e , определяемую открытым ключом (в последней строке имеем $2^{23} = 8388608$). Третий столбец включает в себя целую часть $[s^e/n]$ результата деления числа s^e на n , т.е. вычисляется величина s^e/n , из которой отбрасывается все дробные значения (в частности, в последней строке имеем величину $[2^{23}/21] = 399457$). Четвертый столбец дает результат умножения найденного на предшествующем шаге значения $[s^e/n]$ на величину n (в последней строке – значение 8388597). Наконец, в пятом столбце получается закодированное значение t , представляющее собой разность между значениями s^e из второго столбца и тем, что получено в четвертом столбце, т.е. остаток от деления величины s^e на n (в последней строке получаем $t = 11$). Итогом шифровки оказываются значения 19, 17, 04, 11. Таким образом, зашифрованное сообщение принимает вид 19170411.

Табл. 4. Процедура кодирования сообщения.

s	s^e	$[s^e/n]$	$[s^e/n] \cdot n$	$t = s^e - [s^e/n] \cdot n$
10	100000000000000000000000	4761904761904761904761	999999999999999999981	19
05	11920928955078125	567663283575148	11920928955078108	17
16	4951760157141521099596496896	235798102721024814266499852	4951760157141521099596496892	04
02	8388608	399457	8388597	11

Для дешифровки числа 19170411 оно также разбивается на части: 19, 17, 04, 11. Сама по себе эта процедура аналогична предыдущей, но с заменой открытого ключа на секретный (см. табл. 5). Очевидно, в результате получается исходный текст.

Табл. 5. Процедура расшифровки сообщения.

t	t^d	$[t^d/n]$	$[t^d/n] \cdot n$	$s = t^d - [t^d/n] \cdot n$
19	116490258898219	5547155185629	116490258898209	10
17	34271896307633	1631995062268	34271896307628	05
04	4194304	199728	4194288	16
11	285311670611	13586270029	285311670609	02

В чем "хитрость" этой, как будто, не очень замысловатой процедуры? Какую роль здесь играет теория простых чисел, которые присутствуют в ней не столь уж явно (числа p и q , не используемые непосредственно при кодировании и расшифровке)? Итак, открытый код, т.е. числа n (произведение этих самых простых чисел) и e в секрете не держатся, т.е. вполне доступны противнику. Единственно, чего тот не может знать, так это числа d , входящего в состав секретного ключа. Противник смог бы расшифровать послание, если бы ему удалось разложить данное число n на простые сомножители p и q (при известных значениях e , p и q искомый параметр d находится без труда). Таким образом, для успешного вскрытия ключа нужно (всего-то!) уметь разлагать числа на сомножители. Казалось бы, несложная задачка, особенно если на вооружении имеются мощнейшие компьютеры. Однако на практике число n (совершенно открытое) содержит сотни значащих цифр. В нашем же примере $n = 21$, т.е.

значащих цифр только две. Заодно обратим внимание на то, сколь огромные числа появляются в процессии шифровки и дешифровки коротенького сообщения с чрезвычайно простым ключом (результаты возведения двузначного числа в двузначную степень). А что будет, если нам придется иметь дело с большим текстом и реальным ключом? Ситуация такова, что самые мощные современные компьютеры оказываются не пригодными для того, чтобы разложить очень большие числа (на сотни значащих цифр) на простые сомножители за разумное время. Информация же устаревает достаточно быстро, и сегодняшний секрет через год, а то и через месяц (а порой и через день) секретом уже не является. Так что криптосистемой *RSA* успешно пользуются и в настоящее время.

А все дело в том, что в распределении простых чисел нет явно выраженной закономерности. Поэтому-то специалисты в теории простых чисел с недавних пор пользуются известным спросом в секретных организациях. Именно они (а кто же кроме них?) находят все новые и новые большие простые числа для постоянного обновления списка возможных ключей и стараются выявить все новые закономерности в распределении простых чисел, которые смогли бы упростить задачу криптоанализа, т.е. сократить время, необходимое для взлома секретного ключа. Так, один из наиболее абстрактных разделов математики, до недавних пор служивший пристанищем горстки узких специалистов, стал делом государственной важности и высочайшей секретности.

Такова математика.

Post Scriptum

Не будучи специалистом в области криптографии (как, впрочем, и в теории чисел), в процессе подготовки данной статьи я заглянул в Интернет в поисках необходимой литературы. И практически сразу наткнулся на броские заголовки: "*Математики несут угрозу электронной коммерции*", "*Математики стоят на пороге уничтожения криптографии*" и т.п. Меня естественно заинтересовало, что же такое еще натворили эти математики, тем более что всё это как будто имело прямое отношение к обсуждаемой тематике. Как выяснилось, американский математик французского происхождения **Луи де Бранж** (Louis de Branges) объявил о том, что он доказал гипотезу Римана – ту самую, о которой шла речь выше. Свое доказательство де Бранж разместил в Интернете (для желающих см. www.math.purdue.edu/~branges). И что же теперь?

Сразу возникают два естественных вопроса. Действительно ли де Бранж получил указанный результат? Столь ли уж катастрофическими для криптографии могут быть последствия обоснования гипотезы Римана?

Итак, найдена ли разгадка наиболее знаменитой на сегодняшний день из математических тайн? Уже в значительной степени поутих тот ажиотаж, который был лет десять назад, когда англичанин **Эндрю Уайлс** доказал-таки теорему Ферма. Еще на слуху обоснование российским математиком **Григорием Перельманом** гипотезы Пуанкаре, тоже, кстати, из списка Проблем тысячелетия (стоимостью в миллион долларов, от которого сам Перельман почему-то отказался). И вот теперь гипотеза Римана... Не слишком ли много ярких событий за короткий срок, в то время как за предшествующий полувековой период в математике как будто и не происходило радикальный сдвигов?

Так доказал или нет? Работу Уайлса (объемом порядка ста страниц) долго изучала группа авторитетных специалистов. И нашла таки пробел в доказательстве, вследствие чего Уайлс еще год проводил уточнение результатов, пока не добился безупречного результата. Перельман установил свое утверждение еще в 2004 году, но лишь через два года после тщательной проверки его работы получил признание математической общественности. А по поводу работы де Бранжа специалисты еще не вынесли своего решения. И все же...

В пользу де Бранжа говорят ряд обстоятельств. Прежде всего, он далеко не дилетант. Это формулировка теоремы Ферма доступна пониманию пятиклассника. А чтобы понять гипотезу Римана нужно, как минимум, разбираться в теории бесконечных рядов и

функций комплексного переменного. Де Бранж – достаточно авторитетный специалист в области теории чисел, работающий непосредственно над данной проблемой уже не одно десятилетие. Свою силу он уже однажды показал, решив *проблему Бибераха* – задачу достаточно серьезную, хотя и определенно меньшего ранга. Однако есть и доводы против.

Де Бранжу уже случалось делать ошибочные утверждения (в том числе и в области гипотезы Римана). Его результат не был опубликован в солидном издании, а был лишь выставлен в Интернете, где имеет возможность выставляться любой желающий. Ему уже около семидесяти лет, хотя серьезная математика – это удел молодых. Наконец, приведенное доказательство получило известность еще в апреле 2006 года, и до сих пор никто из крупных специалистов по этому поводу, как будто, не высказался (а речь идет о миллионе долларов!). На эти доводы, впрочем, можно и возразить. Ошибаться доводилось и величайшим гениям. Лежандр доказал теорему Ферма для $n = 5$ (наряду с Дирихле), когда ему было за 70, да и Уайлс с Перельманом получили свои результаты не в самые юные годы. А Перельман, кстати, также не стал публиковать свое доказательство и выставил его в Интернете (время такое!). Ну а специалисты, возможно, еще просто не успели разобраться. Подождем же их решения и не будем спешить с выводами...

А вот по поводу того, насколько серьезными будут последствия обоснования гипотезы Римана для криптографии, сказать что-то можно. Сам по себе факт доказательства данного утверждения для криптографии, видимо, решительно ничего не меняет (оставим сенсационные заголовки на совести у их авторов). Никто, как будто, и не сомневался в том, что нетривиальные нули дзета-функции располагаются именно там, где указал Риман. Ну, предположим, что де Бранж (или кто другой) это строго обосновал. Это что-то меняет? Мы что, в результате получаем эффективный способ описания всего множества простых чисел? Гипотеза Римана при всей ее важности ничего такого не дает. Другое дело, что в процессе доказательства данного результата могли бы быть обнаружены какие-то важные свойства простых чисел, которые можно было бы использовать для взлома шифров. Однако даже сам де Бранж, допуская ранее поспешные выводы, ничего подобного не говорит. Так что, по-видимому, спецслужбы могут спокойно заниматься своим делом. Едва ли им грозят серьезные неприятности, тем более что история криптографии никак не завершилась разработкой системы *RSA*. Впрочем, надо иметь в виду, что в случае реального прорыва в области теории простых чисел и обнаружении каких-то качественно новых закономерностей в их распределении ситуация может серьезно измениться, и соответствующим органам будет над чем задуматься.

В заключении отмечу ряд нерешенных проблем из теории простых чисел. Еще древнегреческие математики обнаружили, что некоторые простые числа появляются парами, отличаясь друг от друга на двойку (они называются *близнецами*), например, 5 и 7, 11 и 13, 17 и 19. До сих пор не известно, конечно или бесконечно множество близнецов. С 18 века остается открытой *проблема Гольдбаха*, согласно которой любое четное число больше двух представимо в виде суммы двух простых чисел, например, $8 = 3 + 5$, $12 = 5 + 7$, $50 = 13 + 37$. Не известно, бесконечно ли множество простых чисел Ферма. Хорошо бы отыскать и генератор простых чисел, т.е. функции целочисленного аргумента, принимающей только простые значения. Словом, желающие могут попробовать свои силы...

Комментарии к литературе

Для предварительного ознакомления с теорией чисел можно рекомендовать небольшую книгу Е. П. Ожиговой [6]. Систематическое изложение теории простых чисел излагается, например, в книгах [3], [4], [10]. В книге С. Сингха [9] в увлекательной форме рассказывается об истории доказательства теоремы Ферма и о других проблемах теории чисел. Краткое изложение основ криптографии дается в статье В. В. Яценко [13]. Теоретические и прикладные аспекты криптографии описываются, например, в [1], [2], [5], [8], [11] (см. также сборник статей К. Шеннона [12]). История развития методов шифровки

и дешифровки информации излагается в книге [14], к сожалению, еще не переведенной на русский язык.

Литература

1. Аграновский А. В., Хади Р. А. Практическая криптография. – М.: Солон-Р, 2002.
2. Бабаш А. В., Шанкин Г. П. Криптография. – М.: Солон-Р, 2002.
3. Ингам А.Э. Распределение простых чисел. – М.: URSS 2005.
4. Карацуба А.А. Основы аналитической теории чисел. – М.: Наука, 1983.
5. Нил Коблиц, Курс теории чисел и криптографии. – М.: ТВП, 2001.
6. Ожигова Е. П. Что такое числа. – М.: УРСС, 2004.
7. Прахар К. Распределения простых чисел. – М.: Мир, 1967.
8. Ростовцев А.Г., Маховенко Е.Б. Введение в криптографию с открытым ключом. СПб, Мир и Семья, 2001.
9. Сингх. С. Великая теорема Ферма. – М., МЦНМО, 2000.
10. Чандрасекхаран К. Введение в аналитическую теорию чисел. – М., Мир, 1974.
11. Чмора А. Современная прикладная криптография. – М., Гелиос, 2002.
12. Шеннон К. Работы по теории информации и кибернетике. – М., ИЛ, 1963.
13. Яценко В. В. Основные понятия криптографии // Математическое просвещение. – 1998, сер. 3, вып. 2, с. 53-70.
14. Kahn D. Codebreakers. The story of Secret Writing. – New York: Macmillan, 1967.

S. Serovajsky

Prime numbers: from Pythagoras to cryptography

The subject of this popular paper is the short history of the development of prime numbers theory. It is a very abstract theory during two and a half thousand years. But it became a very important as the real practical mean in the second part of 20 century in connection of requirement of cryptography. The well-known cryptographic system RSA with using of the prime number properties is described.

Знаменит ответ [Гильберта](#) на вопрос о том, каковы будут его действия, если он по какой-либо причине проспит пятьсот лет и вдруг проснется. Математик ответил, что самым первым делом он спросит была ли доказана гипотеза Римана.