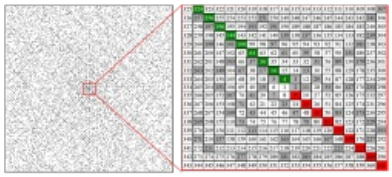
Простые числа — Lurkmore

Простые числа (*OEIS последовательность A000040*) — в математике это такие натуральные числа, которые имеют ровно два делителя: себя и единицу[1]. Встречаются повсеместно, но ИРЛ являются не простыми, а очень даже сложными объектами для технарей и других любителей матана.



Вглядись в них!

Давным-давно в далекой галактике

«Простые числа созданы для того, чтобы их умножать »

— Лев Давидович Ландау

Как и многие другие долгие математические истории, простые числа начались в Древней Греции[2]. Древние греки вообще начали обдумывать аксиоматику и, в частности, пришли к понятию числа. Числам натуральным и рациональным (отношениям натуральных) отводилась важная и б-жественная роль в мироздании, что ещё приведёт к своим трудностям.

Достаточно естественно появилось и сформулированное выше понятие простого числа. Полезность результатов, полученных древними греками, сложно переоценить.

Хозяйке на заметку

Вдумчивый читатель уже заметил, что простые числа также названы последовательностью A000040. В дальнейшем нам ещё не раз встретятся подобные магические обозначения. Это обозначения из энциклопедии целочисленных последовательностей OEIS, в которой можно прочитать подробнее (и заумнее) про матан, связанный с упомянутыми и не только последовательностями. Ну и, кроме того, номера из OEIS постепенно превращаются в стандартный универсальный идентификатор.

Сколько?

Открывши «Начала» Евклида, в 9-й книге, предложении номер 20, анон может невозбранно ознакомиться с доказательством того, что простых чисел бесконечно много.

> Представим, что количество простых чисел конечно. Перемножим их и прибавим единицу. Полученное число не делится ни на одно из конечного набора простых чисел, потому что остаток от деления на любое из них даёт единицу. Значит, число должно делиться на некоторое простое число, не включённое в этот набор. Противоречие.

Сложно сказать, кто придумал это доказательство первым, да не так уж это и важно. Надо только отметить, что уже древние греки задались и другими вопросами, связанными с простыми числами.

К слову, возникает естественное предположение, что число, полученное нами в доказательстве бесконечности множества простых чисел — само простое. Увы, но это не всегда так. Простая калькуляция показывает, что уже число *(спойлер:* $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1$*)* будет составным. Более того, неизвестно, бесконечно ли много простых чисел такого вида. Та же самая ситуация и с числами, которые получаются вычитанием единицы из последовательного произведения простых чисел.

Основная теорема арифметики

> О природе хвалебных отзывов я по природной скромности умолчу, а ругают меня за то, <…>
> что я проявил редкостное невежество, причислив единицу к простым числам

— В. В. Ткачук, «Математика — абитуриенту»

Что же сподвигло греков изучать простые числа? Дело в том, что любое натуральное число, большее единицы, может быть разложено, причём единственным образом (с точностью до перестановки сомножителей и единицы), в произведение простых чисел.

Четкая формулировка этой теоремы справедливости ради впервые встречается у Гаусса, но, судя по тексту всё тех же «Начал», греки это утверждение интуитивно понимали.

В известном смысле именно из этой теоремы растут ноги почти всей дискретной математики и, конечно, криптографии.

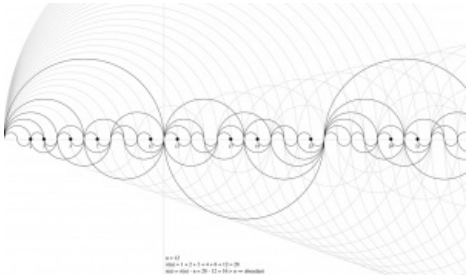
Эта теорема породила, кстати, достаточно забавную дисциплину математической спецолимпиады, а именно, считать единицу составным или простым числом? Ну, в самом деле, если единица — простое число, то разложение на простые множители неединственно, так как *(спойлер:* $1 \cdot 1$*)* $= 1$. А если единица не простое число, то вроде как составное, но это уж какой-то бред, потому что она делится нацело только на единицу и себя. Поэтому у многих авторов получается костыль: множество натуральных чисел разбивается на простые числа, составные и единицу. Ну, а некоторые причисляют-таки единицу к

простым числам и запиливают соответствующий костыль в формулировку основной теоремы арифметики. Nuff said.

Решето Эратосфена

Следующий вполне логичный и важный вопрос о поиске простых чисел был изучен, по всей видимости, в Александрийской библиотеке Эратосфеном Киренским.

Метод прост как пробка: выписываем все числа. Дальше берём двойку и вычеркиваем все остальные чётные числа как заведомо непростые. Следующее невычеркнутое число — это тройка. Запоминаем и вычеркиваем все остальные числа, которые делятся на 3. Следующее ещё невычеркнутое число — снова простое, это пятерка. Вычёркиваем всё, что делится на 5 и т. д... В результате остаются только подряд идущие числа, они и будут простыми. Win. Способ хорош, и ничего более разумного для перечисления всех-всех-всех простых чисел человечество не придумало. Современные способы поиска больших простых чисел в основном сводятся к поиску простых чисел определенного вида.



Решето Эратосфена можно изобразить, например, так

Кстати, Эратосфен много чем ещё отметился. В частности, он первым вычислил радиус Земли. Причём достаточно точно, хоть и непонятно, сколько именно он насчитал, так как считал он в древнегреческих единицах длины, а они несколько различались в зависимости от местности и времени. Однако, исходя из того, что известно, ошибка Эратосфена была достаточно невелика.

Кроме того, сей древнегреческий муж ещё занимался грамматикой, астрономией, филологией и внёс значимый вклад в развитие Александрийской библиотеки. Себя он позиционировал как... филолога.

Классическая эпоха

После заката эпохи античности наступили времена высокой духовности и религиозности, также известные как тёмные века. Никаких особо интересных достижений, связанных с простыми числами, в те времена не зафиксировано, так что мы сразу перенесёмся на полторы тысячи лет вперёд, в конец XVI века. Многие вопросы, зачастую не имеющие ответов и поныне, были заданы именно тогда. В целом направлений для размышлений было два. Первое — нельзя ли придумать какую-нибудь формулу, которая задавала бы исключительно (и лучше бы все) простые числа. Второе — как они распределены среди натуральных, так как довольно быстро стало понятно, что это распределение не совсем случайно. Многое за 500 лет человечество узнало, но далеко не всё. Вот краткое описание основных достижений.

Марен Мерсенн

Марен Мерсенн смотрит на тебя как на последовательность A000668

Монах-католик и кратер на Луне: математик, писатель писем латынью Паскалю, Ферма и другим видным учёным тех времён, однокашник и дружок Декарта, изучатель телескопов, колебания струн и, что для нас наиболее актуально, изобретатель так называемых чисел Мерсенна.

Надо отметить, что Мерсенн был в своём роде первым сам себе научным журналом. Дело в том, что в те времена учёные, сидящие в разных странах, практически не общались друг с другом. А вот Мерсенн сидел у себя в келье и регулярно строчил письма своим знакомым, среди которых были лучшие умы тех времён. В этих письмах он не только высказывал своё ИМХО относительно погоды, но и делился информацией о том, кто, что и как изобрёл и открыл, осуществляя тем самым в одно лицо функцию научной коммуникации, которую теперь выполняют журналы. Тех писем он настрочил аж на 17 томов. Чтобы был понятен масштаб, почти всё, что мы знаем о работах, например, Ферма, мы знаем из его переписки с Мерсенном.

Среди научных результатов в рамках данной статьи нас интересует одна гипотеза, выдвинутая Мареном, а именно: он предположил, что числа вида $2^n - 1$, как правило, являются простыми. Из не вполне ясных соображений Мерсенн мамой клялся, что при n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257 соответствующие числа Мерсенна будут простыми, а все остальные числа Мерсенна до n = 257 совершенно точно будут составными. Впрочем, выяснилось, что инфометр у святого отца барахлил. Некоторые из не включенных в этот список чисел оказались простыми, а некоторые включенные — составными. Фейл? Не совсем. Гипотеза Мерсенна оказалась крайне продуктивной, именно последовательность из его чисел по сей день исправно поставляет самые большие простые числа. Недавно очередной рекорд был поставлен Кёртисом Купером, выяснившим, что число Мерсенна для n, равного 74 207 281, является простым.

Впрочем, до сих пор неизвестно, бесконечно ли множество простых чисел Мерсенна. Может, ты, анон, найдёшь ответ?

Иван Михеевич Первушин недоволен твоими познаниями в математике и слове б-жьем

Иронично, что одним из тех, кто насрал в компот Мерсенну, был простой русский священник Иван Михеевич Первушин, который выяснил, что при $n = 61$ число Мерсенна таки простое, хоть и не было включено в изначальный список. Кроме шуток, Иван Михеевич сделал серьёзную работу и неспроста был избран в Петербургскую и Неаполитанскую академии. А 61-е число Мерсенна ныне известно как число Первушина.

Стоит отметить довольно забавную историю, связанную с числом Мерсенна для $n = 67$. Доказательство того, что это число составное, уже было известно, однако не было известно, на какие же простые сомножители оно раскладывается. Фрэнк Коул вручную (sic!) вычислил разложение на простые множители (ни компьютеров, ни калькуляторов в те времена не было). Во время своего доклада, длившегося час, он молча вышел к доске, после чего… взял и вычислил, так и не сказав ни слова во время доклада, что $2^{67} - 1 = 193\,707\,721 \cdot 761\,838\,257\,287$. Кстати, Коул был правда неплохим математиком, а не каменножопым вычислителем, и отметился ещё и в теории простых групп и других разделах математики.

Пьер Ферма

Мало какой научпоп может обойтись без упоминания Пьера де Ферма, юриста из Тулузы. Про самый эпичный математический срач, связанный с Ферма, уже написано на Уютненьком. Нас же интересует другая гипотеза великого дилетанта.

Гипотеза была в следующем: среди чисел вида $2^{2^n} + 1$ бесконечно много простых. Увы, но до сих пор неизвестно ни одного простого числа Ферма начиная с $n = 5$. Причём, чтобы получить ответ уже для $n = 5$, потребовалось применить целого Леонарда Эйлера. Среди прочего на этой же ниве отметился и уже упомянутый Первушин, который доказал, что не являются простыми несколько чисел Ферма. За сие сельский священник был поощрён: «Академия наук в поощрение трудов П. исхлопотала у святейшего синода высылки ему математических книг на 190 руб»!

А что ты сделал для поиска простых чисел в последовательности A000215?

Остается только подчеркнуть, что поиск простых чисел Ферма до сих пор не привёл ни к каким определённым результатам. Так что современное состояние этого вопроса состоит в писькомере на тему, у кого круче комп, а значит, кто может проверить на простоту самое большое число. На данный момент (результат 2014 года) самое большое точно составное число Ферма при $n = 3\,329\,780$.

Многочлены и простые числа

Вообще, сказанное выше демонстрирует одно из самых популярных направлений мысли XVIII—XIX веков. Это идея описания всего и вся при помощи формул. Математики понимали, что простые числа распределены не совсем случайно, а значит, их наверняка можно описать каким-то разумным способом. Наиболее логичным было предположение о том, что какой-нибудь не слишком сложный многочлен (или другое выражение такого же сорта) при подстановке разных чисел будет давать исключительно простые числа. Может быть, не все, может быть, не по порядку, но зато исключительно простые. Именно эту идею и пытались реализовать Ферма и Мерсенн.

Полевые испытания Эйлера показали, что многочлен $n^2 - n + 41$ — почти хороший. Для первых сорока натуральных чисел получаются простые значения. Но увы, последователи Эйлера доказали, что среди многочленов от одной переменной не бывает так, чтобы все значения многочлена были простыми. Некий итог в поиске точных формул для перечисления всех простых чисел поставил в конце XX века Матиясевич. Ответ оказался не очень приятный. Да, такие многочлены существуют, но вот выглядят они, скажем так, не очень. Сам Матиясевич привёл в качестве примера многочлен степени 15 905. Позже были предъявлены и примеры попроще, например многочлен степени 25, от 26 переменных…

Разумеется, и по сей день известно про формулы для простых чисел далеко не всё. Так, неизвестно, какая наименьшая степень для многочлена, «перечисляющего» простые числа, не ясно также, и каково минимальное необходимое число переменных.

Отметим напоследок, что, несмотря на очень высокую теоретическую ценность, практическая польза таких формул, увы, невелика.

Проблема Гольдбаха

Возьмем два множества натуральных чисел A и B и всевозможные попарные суммы $A + B$ из этих множеств. Насколько большое множество мы получим? Несложно привести примеры, когда будет получено множество всех натуральных чисел (значит, множества достаточно жирные) и когда нет (множества мелковаты или неудачно распределены). Именно с этой конструкцией связана самая знаменитая, оставшаяся неразрешенной до сих пор проблема теории чисел, то есть проблема Гольдбаха.

В переписке Кристиана Гольдбаха (тогда ещё работавшего в рідном Кенигсбергском университете, а в будущем перебравшегося на работу в Министерство иностранных дел той ещё Российской Империи) с Эйлером (также перебравшегося в Петербург на ПМЖ) было высказано две гипотезы: тернарная проблема Гольдбаха о том, что любое нечётное число может быть представлено в виде суммы не более чем трёх простых чисел, а также бинарная проблема, гласящая, что любое чётное число может быть представлено в виде суммы двух простых чисел.

Довольно долго никаких значимых продвижений в решении обеих проблем Гольдбаха не наблюдалось, пока наконец на проблему не набижали советские математики. Сначала в 1930 году Шнирельман доказал, что для некоторой константы k любое натуральное число может быть представлено в виде суммы не более чем k простых. После доработки напильником эта константа была доведена до 67. Fail? Как бы не так. Этот результат вселил уверенность, что проблема Гольдбаха в принципе разрешима.

Мощный ход в 1937 сделал Иван Матвеевич Виноградов, который доказал справедливость тернарной проблемы Гольдбаха для всех натуральных чисел, больших некоторой константы. Win? Теоретически да, но есть нюанс. Константа, до которой нужно перебрать, оказалась не просто большой, а пиздец какой большой, а именно сопоставимой с числом атомов во Вселенной… Ясное дело, что ни о каком переборе речь идти не могла. Многие допиливали и уточняли доказательство, заметно уменьшив константу, но так и не сделали её обозримой.

В результате тернарную проблему окончательно доковырял несколько иным методом перуанец Хельфготт в 2013 году.

Многие из результатов, полученных в ходе доказательства, позволяют сделать определенные выводы и в отношении бинарной проблемы, но окончательно она до сих пор не сделана. Sad but true.

Кристиан Гольдбах смотрит на тебя как на нечётное число

Кристиан Гольдбах смотрит на тебя как на нечётное число

Леонард Эйлер посмотрел бы на тебя как на говно, но на этом портрете он уже слеп

Леонард Эйлер посмотрел бы на тебя как на говно, но на этом портрете он уже слеп

Шнирельман невысокого мнения о тебе

Распределение простых чисел

Ещё одно направление размышлений о простых числах такое. С одной стороны, среди натуральных чисел бывают сколь угодно длинные промежутки, на которых нет ни одного простого числа (это задача для 7-го класса). С другой стороны, иногда простые числа бывают очень близко друг к другу. Нет ли какого-нибудь способа узнать, насколько часто встречаются простые числа?

Проблема близнецов

Если начать изучать последовательность простых чисел, то видно, что иногда (и не так уж и редко) попадаются простые числа, между которыми расстояние равно двум, например 11 и 13, 17 и 19. Такие числа называются близнецами. Самые большие найденные на данный момент близняшки — это $2\,996\,863\,034\,895 \cdot 2^{1\,290\,000} \pm 1$.

Печаль в том, что по сей день неизвестно, конечно ли множество пар близнецов. Хочется верить, что нет. Самый сильный результат по этому поводу принадлежит одному китайцу (подробности тут). Вкратце доказано, что существует бесконечно много пар простых чисел, расстояние между которыми не превышает всего лишь 70 миллионов. Уже через месяц

Пятиминутка жидоборчества

Иван Матвеевич, кстати, был весьма интересной личностью. Будучи правда блестящим и выдающимся математиком, а также директором математического института, он был ещё и дичайшим, лютым антисемитом и жидоборцем. Впрочем, с этим связаны и определенные лулзы. Так, когда пришло распоряжение уволить академика Шафаревича, по словам очевидцев, сидевших под кроватью, произошёл примерно такой диалог с «компетентными органами»:

> — Нужно уволить Шафаревича!
>
> — Я проверил, он не еврей. —

после опубликования эта оценка была снижена с 70 миллионов более, чем на порядок - до 4 982 086, а через год (в апреле 2014) ее удалось свести к значению 246.

Впрочем, как и в случае с упомянутой выше работой Шнирельмана, посвященной проблеме Гольдьбаха, даже такая, мягко говоря, грубая оценка — это уже хорошо. Внушает оптимизм, что окончательный ответ и в этой проблеме будет получен в обозримом будущем.

Постулат Бертрана

Достаточно быстро (ещё Эйлеру) стало понятно, что простые числа распределены не так уж и редко. Так что, если отвлечься от близнецов и совсем уж «соседних» простых чисел, сосредоточившись на их распределении в среднем, станет ясно, что какой-то ответ рано или поздно появится.

Самый первый результат от дедушки Эйлера состоял в том, что количество простых чисел среди натуральных растёт медленнее, чем линейная функция.

Вскоре возникла гипотеза, высказанная Бертраном, о том, что между числами n и $2n$ есть хотя бы одно простое. Доказал это утверждение Пафнутий Львович Чебышёв (кстати, первый научный руководитель этой вашей Софьи Ковалевской). Интересно отметить, что самое простое доказательство этой теоремы ещё лет через 50 придумал Эрдёш.

Вообще, в классической теории чисел шаг вправо, шаг влево — нерешенная проблема. Вот и с постулатом Бертрана та же хуйня. Неизвестно до сих пор, верно ли, что между любыми двумя соседними квадратами чисел — n^2 и $(n + 1)^2$ — есть хотя бы одно простое число (гипотеза Лежандра).

Распределение

Как уже было сказано, Эйлер доказал, что количество простых чисел $\pi(n)$, не превышающих n, растёт медленнее, чем линейная функция. Так что довольно быстро математики стали подозревать, что где-то тут зарыт логарифм. Первым заподозрил что-то такое Гаусс, потом Лежандр и Вега.

Однако точно сформулировал гипотезу и почти (установил очень и очень узкий коридор, в котором может быть колебание) доказал Пафнутий наш Львович Чебышёв. Гипотеза была, что $\pi(x) \approx x/\ln(x)$. Чуть позже Риман связал эту самую функцию со своей дзета-функцией (о которой пара слов будет сказана ниже), и, наконец, в 1896 году Адамар и Валле-Пуссен окончательно доказывают теорему о распределении простых чисел.

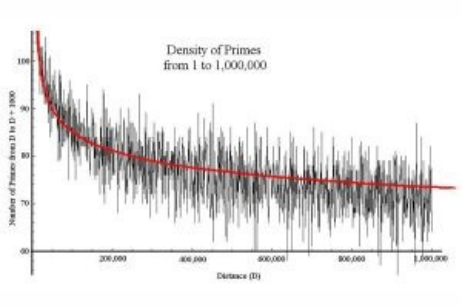
Таким образом, глобальные свойства распределения простых чисел были окончательно получены. Впрочем, масса вопросов о подробностях того, как они распределены, до сей поры осталась без ответа. В том числе и проблема близнецов, проблема Лежандра и многое другое.

Гипотеза Римана

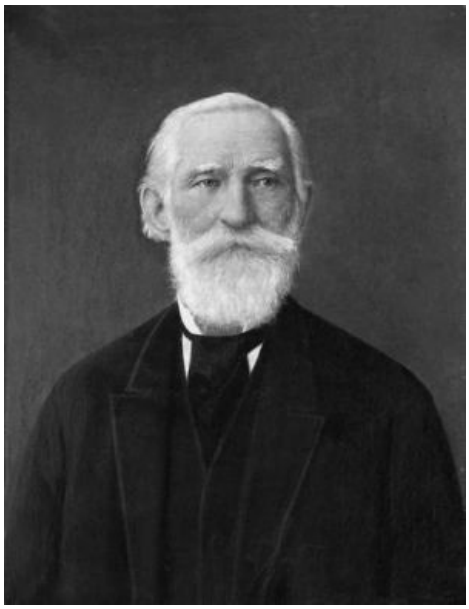
Тесно связана с распределением простых чисел и такая очень известная математическая конструкция, как дзета-функция Римана, которую в своё время придумал Эйлер и активно изучал Чебышёв. За определением этой функции и её свойствами марш в Вику. Мы же отметим, что тот, кто докажет, что все нетривиальные нули этой функции имеют действительную часть, равную 0,5, будет ба-а-альшой молодец. И даже получит лям баксов от института Клея за решение проблемы тысячелетия.

> Уволить его надо, какая разница еврей он, или нет? Он враг советской власти! — Да нет, что вы! Я тщательно всё проверил, он точно не еврей! — !!!???

В общем, Шафаревича так и не уволили. Также злые языки утверждают, что своим главным административным достижением Виноградов считал «очистку математического института от евреев». Впрочем, не исключено, что истории про антисемитизм Виноградова сильно преувеличены.



Красная линия — та самая асимптотика



Пафнутий Львович смотрит на тебя как-то недовольно, свирепо и в то же время грустно и с недоумением

Между прочим, Львович был действительно крутым учёным. Он отметился в теории вероятностей, механике, анализе, геометрии… Сделал массу изобретений. Однажды Пафнутия Львовича попросили прочитать лекцию для ткачих о математическом взгляде на вопросы раскройки тканей. Львович согласился. Собрался полный зал. Пафнутий Львович взял в руки мел и вышел к доске: «Будем для простоты считать, что человек имеет форму шара…» Зал быстро опустел.

А разгадка проста: распределение нетривиальных нулей дзета-функции связано с распределением простых чисел. Кроме того, на гипотезе Римана основано некоторое количество (используемых) методов в криптографии. Подробнее про эти связи можно почитать тут.

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - p^{-s}}$$

Первое равенство — это определение дзета-функции Римана, а второе равенство — утверждение, доказанное Эйлером

Наши дни

«Криптография бывает двух типов: криптография, которая помешает читать ваши файлы вашей младшей сестре, и криптография, которая помешает читать ваши файлы людям из правительства. »

— Брюс Шнайер, «Прикладная криптография» (Applied Cryptography), 2-е издание.

Всё, о чем мы толковали выше, это пусть и почтенные задачи, но пик интереса к ним остался в прошлом. Дело в том, что, если (когда?) будет доказана бинарная проблема Гольдбаха, это не приблизит человечество к алгоритму представления числа в виде суммы двух простых. То же можно сказать и о других задачах. Знание тонкостей распределения простых чисел интересно и важно с теоретической точки зрения, но едва ли даст нам что-то по-настоящему новое. Передний фронт современных математических интересов ушёл далеко (и ты, дорогой читатель, даже не представляешь себе, НАСКОЛЬКО), а равно и фронт интересов практических, также известных как прикладная математика. Однако интерес к простым числам отнюдь не праздный.

Дело в том, что очень многие криптографические алгоритмы основаны, очень грубо говоря, на том, что если есть очень большое число, которое является произведением двух очень больших простых чисел, то найти это разложение, не зная одного из сомножителей, очень трудно. Поэтому знание очень больших (действительно ОЧЕНЬ БОЛЬШИХ) простых чисел необходимо, чтобы обеспечивать криптостойкость.

Второй очень важный сюжет, тесно связанный с первым, это поиски быстрых алгоритмов проверки числа на простоту. Ну в самом деле, если последняя цифра числа в десятичной записи — чётная, то число заведомо составное. Также легко и быстро проверить, что число кратно трём и т. д. Но есть ли способ проверить, составное ли число, не перебирая все возможные простые сомножители? Над этим вопросом бьются и многое придумали. Например, вероятностный тест, да и много чего ещё. Вот навскидку ещё один тест.

Причина таких специфических интересов проста. Дело в том, что в основе многих криптографических алгоритмов (в частности, цифровой подписи) лежит простая идея. Если есть очень большое число, являющееся произведением двух очень больших простых чисел, то не зная, как это число раскладывается на сомножители, найти такое разложение очень сложно (то есть займёт очень большое время). Зато зная один из сомножителей (если упростить до предела, то это как раз ключ шифра), то очень легко (то есть быстро) и найти второй сомножитель, и проверить, что исходное число делится на это число. Конечно, в реальных алгоритмах всё несколько сложнее, но в конечном счёте всё упирается в то, что дешифровка если и возможна, то за очень продолжительное время.

Мир развивается, и старые, классические задачи отправляются туда же, куда и перфокарты. Нечто похожее происходит и с криптографией. Нынче в моде кодирование при помощи эллиптических кривых и тому подобные штучки. В будущем, наверное, в массы придут квантовые компьютеры и иные вундервафли, про которые мы пока ничего не знаем.

Новые технологии приведут и к новым вопросам, будут среди них, наверное, и вопросы о простых числах. Но вряд ли они заинтересуют тебя.

Сложновато?

Многих удивляет (и уже давно) та удивительная сложность всех вопросов, связанных с простыми числами. Чтобы доказать даже самые простые и давно известные утверждения, требуются определенные усилия. Почти любой вопрос, который можно задать про простые числа, будет либо тривиальным, либо пиздец каким сложным. Отчего же так?

Разумная версия состоит в том, что простые (да и вообще натуральные) числа — очень не геометричный объект. То есть если бы была какая-то их разумная геометрическая интерпретация, более разумная, чем нули дзета-функции, то и решались бы соответствующие задачи гораздо проще. Неспроста многие задачи теории чисел решаются последние лет 70 такими далёкими, на первый взгляд, от теории чисел инструментами, как комплексный анализ, алгебраическая геометрия и прочий зубодробительный матан, в котором разве что Перельман разберётся.

Второй адекватный, но более философский взгляд состоит в том, что простые числа являются антропоморфным объектом, а не естественным. Вот поверхности, многие алгебраические структуры и тому подобное — это естественные объекты, потому что про них «простые» вопросы действительно, как

правило, просты. В отличие от простых чисел. Сон разума рождает чудовищ, одним словом.

И наконец, последнее, что можно сказать о сложности теории чисел, это криптография. Во многом большая часть современных теоретико-числовых задач, в том числе и связанных с простотой, упирается в вычислительные мощности и оптимизацию тех или иных алгоритмов. Но увы, мощь компьютеров не бесконечна, а в оптимизации любых алгоритмов есть предел. И как это ни прискорбно, но решение многих теоретико-числовых задач уже давно упирается именно в вычислительные мощности (так было до недавнего времени с тернарной проблемой Гольдбаха, пока не был найден «обходной путь», так сейчас дела обстоят и с бинарной проблемой Гольдбаха).

Так что, дорогой читатель, никто не помешает тебе поломать голову над какой-нибудь теоретико-числовой задачей, но, если ты хочешь всерьёз заняться математикой и решить какую-нибудь крутую задачу, придётся работать и работать. Тебя ждут боль и страдание. Но, быть может, тебе повезёт! Попробуй!

Что почитать по теме

- Апостолос Доксиадис «Дядюшка Петрос и проблема Гольдбаха» — годнейший, куда более интересный и захватывающий, чем эти ваши «Игры престолов» с «Гарри Поттером», худлит про Теорему Гольдбаха, простые числа и вообще математиков.
- Матиясевич Ю. «Формулы для простых чисел» — хорошая, годная статья Матиясевича о формулах для задания простых чисел.
- Нил Стивенсон «Криптономикон» — в своём роде культовая художественная книга про криптографию.
- «Эллиптическая криптография: теория» — про криптографию эллиптическими кривыми.
- Текст для вдумчивого обмазывания

См. также

- Комплексные числа
- Великая теорема Ферма

Примечания

1. ↑ Более простым языком для школьников, прокуривших уроки математики в туалете: простыми называются числа, которые можно разделить без остатка (это важно) только на единицу и на самих себя. Допустим, 5 делится лишь на 5 (получаем 1) и на 1 (получаем 5). А вот девятку, помимо самой себя и единицы, можно безо всяких дробей в ответе поделить ещё и на тройку. Такие дела.
2. ↑ Потому что всем похуй на арабов^Wегиптян и папирус Ахмеса, конечно же.

Числа

1 Guy 1 Jar 101-й километр 10:10 1111 12309 127.0.0.1 128 bit 13 14/88 1500 рублей 16 рублей 1917 1984 2 Girls 1 Cup 2 в 1 2000 2012 год 228 25-й кадр 265 28 героев-панфиловцев 282 статья 3,5 анонимуса 3,62 3605 3730 40 кг хурмы 410 42 640 килобайт 666 7:40 90% женщин — изнасилованы 95% населения — идиоты 9600 бод и все-все-все DotA In 5 Seconds IT'S OVER NINE THOUSAND! Leet Monkey Dust Nokia 3310 X86 Автомобильные номера Большой Пиздец/Предполагаемые даты БОЧ рВФ 260602 Веб 1.0 Веб 2.0 Великая теорема Ферма Восьмидесятые Вячеслав Мальцев Гет Двести двадцать Девяностые ДЕЕ1991ГР Деление на ноль Десятые Днепропетровские маньяки Жертвы пранка Закон Парето Звёздные войны Золотой миллиард Зона 51 Инфа 100% Йобибайт Квадратура круга Код Матан Миллиард расстрелянных лично Сталиным Мне 20 и я бородат Мытищи Нулевые Плюс 1 Полшестого Правило 34 Правило 63 Правило трёх секунд Проблема 2000 Простые числа Пятисемит Рулетка Семь чудес света Слава роботам Сотни нефти Стопицот Сырно Тёмная башня Теория относительности Три обезьяны Тринадцать миллионов педофилов Число Грэма Число Эрдёша Чуров Чуть более, чем наполовину Эльф 80-го уровня

w:Простые числа