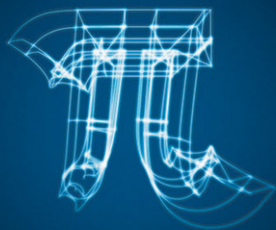


И Э Н С Т Ю А Р Т



ВЕЛИЧАЙШИЕ МАТЕМАТИЧЕСКИЕ ЗАДАЧИ

Выдающийся и наиболее продуктивный
среди британских популяризаторов
математической науки *The Guardian*



Династия



Иэн Стюарт

Величайшие математические задачи

Текст предоставлен правообладателем

http://www.litres.ru/pages/biblio_book/?art=15210871

*Величайшие математические задачи / Иэн Стюарт: Альпина нон-фикшн; Москва; 2015
ISBN 978-5-9614-3705-8*

Аннотация

Закономерности простых чисел и теорема Ферма, гипотеза Пуанкаре и сферическая симметрия Кеплера, загадка числа π и орбитальный хаос в небесной механике. Многие из нас лишь краем уха слышали о таинственных и непостижимых загадках современной математики. Между тем, как ни парадоксально, фундаментальная цель этой науки – раскрывать внутреннюю простоту самых сложных вопросов. Английский математик и популяризатор науки, профессор Иэн Стюарт, помогает читателю преодолеть психологический барьер. Увлекательно и доступно он рассказывает о самых трудных задачах, над которыми бились и продолжают биться величайшие умы, об истоках таких проблем, о том, почему они так важны и какое место занимают в общем контексте математики и естественных наук. Эта книга – проводник в удивительный и загадочный мир чисел, теорем и гипотез, на передний край математической науки, которая новыми методами пытается разрешить задачи, поставленные перед ней тысячелетия назад.

Содержание

Предисловие	5
1. Великие задачи	7
2. Территория простых чисел. Проблема Гольдбаха	18
Конец ознакомительного фрагмента.	26
Комментарии	

Иэн Стюарт

Величайшие математические задачи

Переводчик *Наталья Лисова*

Редактор *Наталья Нарциссова*

Руководитель проекта *И. Серёгина*

Корректоры *Е. Аксёнова, М. Миловидова*

Компьютерная верстка *А. Фоминов*

Дизайн обложки *О. Сидоренко*

© Joat Enterprises, 2013

© Издание на русском языке, перевод, оформление. ООО «Альпина нон-фикшн», 2014

Все права защищены. Никакая часть электронного экземпляра этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами, включая размещение в сети Интернет и в корпоративных сетях, для частного и публичного использования без письменного разрешения владельца авторских прав.

* * *



Династия

Фонд некоммерческих программ «**Династия**» основан в 2002 г. Дмитрием Борисовичем Зиминим, почетным президентом компании «Вымпелком».

Приоритетные направления деятельности Фонда – поддержка фундаментальной науки и образования в России, популяризация науки и просвещение.

В рамках программы по популяризации науки Фондом запущено несколько проектов.

В их числе – сайт elementy.ru, ставший одним из ведущих в русскоязычном Интернете тематических ресурсов, а также проект «Библиотека «Династии» – издание современных научно-популярных книг, тщательно отобранных экспертами-учеными.

Книга, которую вы держите в руках, выпущена в рамках этого проекта.

Более подробную информацию о Фонде «Династия» вы найдете по адресу www.dynastyfdn.ru.

* * *

Мы должны знать – мы будем знать!

Давид Гильберт,

*речь о математических проблемах, произнесенная в 1930 г.
по случаю присвоения Гильберту звания Почетного гражданина
Кёнигсберга*

Предисловие

Математика – обширная, непрерывно растущая и столь же непрерывно меняющаяся область знания. Среди бесчисленных вопросов, которыми задаются математики и на которые они по большей части находят ответы, есть немало и таких, которые стоят особняком и возвышаются над всеми прочими, словно горные пики – над предгорьями. Это действительно сложные проблемы, и любой математик отдал бы правую руку за возможность первым найти решение одной из таких масштабных задач. Некоторые из них оставались нерешенными десятилетиями, иные – столетиями, а есть и такие, что не поддавались усилиям математиков несколько тысячелетий. И до сих пор существуют проблемы, которые ученым только предстоит разрешить. Так, последняя теорема Ферма оставалась для математиков камнем преткновения 350 лет, пока Эндрю Уайлс не доказал ее, потратив на эту работу семь лет жизни. Гипотеза Пуанкаре была неприступна больше 100 лет, пока эксцентричный гений Григорий Перельман не нашел доказательство и не превратил ее в теорему (отказавшись при этом от всяких академических почестей и премии в миллион долларов за эту работу). А гипотеза Римана и сегодня, через 150 лет после того, как была сформулирована, остается нерешенной.

Книга «Великие математические задачи» рассказывает о некоторых крупнейших математических проблемах, работа над которыми открывала перед научной мыслью совершенно новые направления и возможности. Читатель познакомится с истоками этих задач, узнает, почему они так важны и какое место занимают в общем контексте математики и естественных наук. В книге представлены как решенные, так и нерешенные задачи из самых разных периодов истории математики. По существу, рассказ охватывает две с лишним тысячи лет развития науки, однако основное внимание в книге сосредоточено на вопросах, которые либо до сих пор остаются нерешенными, либо были решены относительно недавно, в последние полвека.

Фундаментальная цель математики – раскрывать внутреннюю простоту сложных на первый взгляд вопросов. Это заявление может показаться неочевидным и даже странным, поскольку математическое представление о «простоте» опирается на множество сложных технических концепций. Но важная особенность этой книги заключается именно в том, что акцент в ней сделан на глубинную простоту, а сложности мы стараемся обойти стороной или объясняем простыми словами.

Математика – более молодая и многообразная наука, чем многие думают. По приблизительным оценкам в мире сегодня живет около 100 000 математиков-исследователей, которые каждый год выпускают более *двух миллионов* страниц новых математических изысканий. Это не «новые числа», поисками которых математики не занимаются вообще. И не «новые величины», подобные уже известным, только больше, хотя мы действительно иногда работаем с достаточно большими величинами. Так, про одно недавнее алгебраическое исследование, проведенное командой из 25 математиков, какой-то шутник сказал: «Расчет размером с Манхэттен». Но и это не совсем верно – ребята поскромничали. Размером с Манхэттен у них был *ответ*, а расчет занимал гораздо больше места. Впечатляет, не правда ли? Но главное в математических исследованиях все-таки качество, а не размер и даже не количество. Расчет размером с Манхэттен, о котором шла речь, котируется в обоих отношениях, поскольку дает важную информацию о группе симметрии, играющей существенную роль в математике и, судя по всему, в квантовой физике. Блестящие математические рассуждения и выводы могут уложиться в одну строчку – а могут занять целую энциклопедию. Все зависит от существа и сложности задачи.

При мысли о математике на ум в первую очередь приходят страницы, заполненные малопонятными значками и формулами. Однако те два миллиона страниц, о которых мы говорили, содержат по большей части слова, а не специальные символы. Слова необходимы для объяснения существа проблемы, описания хода мысли и смысла вычислений, и, кроме того, без них невозможно объяснить, какое место все это занимает в постоянно строящемся здании математики. Как заметил на границе XVIII и XIX вв. великий Карл Гаусс, главное в математике – «идеи, а не символы». Тем не менее обычно математические идеи излагаются языком символов. И многие исследовательские работы содержат больше символов, чем слов. Четкости, которую обеспечивают формулы, не всегда можно достичь словами.

Тем не менее нередко математические идеи можно объяснить словами, оставив в стороне большую часть специальных символов. И именно этот принцип лег в основу книги, которую вы держите в руках. Она рассказывает, чем занимаются математики, как они думают и почему предмет их исследований интересен и важен для всего человечества. Она показывает также (и это очень важно), как сегодняшние математики справляются с вызовами своих предшественников, как одна за другой великие загадки прошлого уступают мощным методикам настоящего, тем самым изменяя и математику, и естественные науки будущего. Математика по праву относится к величайшим достижениям человечества, и ее важнейшие задачи – решенные и нерешенные – уже не одну тысячу лет направляют и стимулируют творческие силы человека.

Ковентри, июнь 2012 г.

1. Великие задачи

Телепередачи о математике попадают редко, а хорошие и того реже. Одной из наиболее удачных среди них, причем не только по содержанию, но и по степени увлекательности и вовлеченности зрителей, стала программа о Великой теореме Ферма, которую в 1996 г. снял для научно-популярной серии *Horizon* британской корпорации ВВС Джон Линч. Саймон Сингх, который также участвовал в создании этой программы, превратил рассказанную в ней историю в захватывающую книгу-бестселлер. На своем сайте он рассказал, что поразительный успех передачи стал для всех сюрпризом.

«В нашей программе целых 50 минут математики рассказывают о математике. Не сказать, чтобы это был надежный рецепт создания телевизионного блокбастера, но наша передача взбудоражила зрителей и привлекла внимание критиков. Она получила премию BAFTA как лучшая документальная программа, Приз Италии, другие международные награды и была номинирована на Emmy. Это доказывает, что математика может быть не менее захватывающей темой, чем любая другая».

Я думаю, что успех телепрограммы и книги был обусловлен несколькими причинами, которые имеют немаловажное значение и для моего рассказа. Но чтобы не слишком разбрасываться, я буду говорить только о документальном фильме.

Последняя теорема Ферма – одна из величайших математических проблем, но возникла она из невинного на первый взгляд замечания, сделанного одним из ведущих математиков XVII в. на полях классического учебника. Постепенно проблема приобрела известность, поскольку никто не мог ни доказать, ни опровергнуть утверждение, содержащееся в оставленной Пьером Ферма заметке на полях. Несмотря на усилия, предпринимавшиеся множеством необычайно умных людей, такое положение вещей сохранялось более 300 лет, поэтому когда в 1995 г. британскому математику Эндрю Уайлсу удалось наконец справиться с этой проблемой, масштаб его достижения был очевиден каждому. Не нужно было даже знать, в чем заключается проблема, не говоря уже о ее решении. В какой-то мере достижение Уайлса – то же самое, что покорение Эвереста.

Помимо научного значения, успешное доказательство теоремы Ферма связано с интереснейшей жизненной историей. В 10 лет Эндрю Уайлс так заинтересовался этой проблемой, что решил стать математиком и обязательно решить ее. Он выполнил первую часть плана и даже выбрал своей специализацией теорию чисел – обширную область математики, к которой относится и Великая теорема Ферма. Однако чем больше он узнавал о математике, тем труднее казалось выполнить задуманное. Теорема Ферма – загадочная диковинка, обособленный вопрос из разряда тех, которые умеет задавать любой специалист по теории чисел (ведь для этого не нужно никаких доказательств). Она не укладывается ни в одну систему мощных доказательных средств. Великий Гаусс в письме к Генриху Ольберсу попросту отмахнулся от нее, заметив, что эта проблема «мне не особенно интересна, поскольку легко можно сформулировать множество подобных утверждений, которые никто не может ни доказать, ни опровергнуть». Уайлс решил, что его детская мечта неосуществима, и отложил теорему Ферма в долгий ящик. Однако затем, будто по волшебству, другие математики совершили прорывное открытие, неожиданно связавшее теорему со стержневой темой теории чисел, причем именно той, которой и занимался Уайлс. Гаусс, как оказалось, в свое время недооценил значение этой проблемы, что для него вообще-то было нехарактерно; он не подозревал, что она может быть связана с глубокой, но на первый взгляд достаточно далекой областью математики.

Теперь, когда связь была установлена, Уайлс мог работать над загадкой Ферма и одновременно проводить значимые исследования в рамках современной теории чисел. Даже если с доказательством Великой теоремы ничего бы не получилось, все, что удалось открыть в ходе исследований, было бы достойно публикации. Так что старые наработки были извлечены на свет божий, и Уайлс начал всерьез обдумывать проблему. Через семь лет усердных трудов (а работал он втайне от ученого сообщества, что для математиков совсем не характерно) Уайлс пришел к выводу, что решение найдено. На престижной конференции по теории чисел он прочел серию лекций под невнятным названием, которое никого не обмануло. Новость разлетелась и произвела сенсацию, причем не только в академических кругах, но и в средствах массовой информации. Теорема Ферма доказана!

Полученное Уайлсом доказательство, полное оригинальных идей, оказалось красивым и элегантным. К несчастью, специалисты вскоре обнаружили в его логике серьезный пробел. Как это ни печально, при решении великих (и обычно очень известных) математических задач такое происходит сплошь и рядом, и, как правило, для очередного доказательства такой поворот событий оказывается роковым. Однако на этот раз судьба была благосклонна: при помощи бывшего своего ученика Ричарда Тейлора Уайлсу удалось ликвидировать пробел, исправить доказательство и завершить работу. Эмоциональное напряжение этого момента очень хорошо видно на экране: пожалуй, это единственный случай, когда ученый-математик расплакался перед камерой при одном только воспоминании о тех драматических событиях и последовавшем за ними триумфе.

Вы, наверное, заметили, что я так и не рассказал вам, в чем, собственно, *заключается* Великая теорема Ферма. Я сделал (или, вернее, не сделал) это намеренно: о самой теореме речь пойдет в свое время. Ведь успех телепередачи с сутью теоремы почти не связан. Мало того, математики никогда не придавали особого значения тому, верна ли теорема, которую Ферма небрежно набросал на полях книги, или нет. От ответа на этот вопрос ничего особенно важного не зависит. Откуда же такой интерес к нему? Все очень просто. Огромное значение может иметь именно то, что все математическое сообщество было не в состоянии *найти* этот ответ. И дело вовсе не в самоуважении: это означало, что в существующих математических теориях не хватает чего-то принципиально важного. К тому же теорема очень просто формулируется, и это добавляет загадочности всей ситуации. Как может что-то настолько на первый взгляд простое оказаться таким сложным?

Математиков не слишком заботил ответ на вопрос, поставленный Ферма, зато глубоко заботил тот факт, что они ответа не знают. К тому же им хотелось найти метод решения этой проблемы, поскольку он, по идее, должен был пролить свет не только на вопрос Ферма, но и на множество других вопросов. Опять же так нередко случается с математическими загадками: методы, использованные для их решения, часто важнее результатов. Разумеется, иногда результат тоже важен – все зависит от его следствий.

Доказательство Уайлса слишком сложно для телепередачи, разобраться в нем могут только специалисты. В нем есть математическая красота и интрига, как мы убедимся в свое время, но любая попытка объяснить что-то подобное по телевизору привела бы к немедленной потере интереса у большей части аудитории. Поэтому программа разумно сосредоточилась на более личном вопросе: каково это – решить математическую проблему, известную своей сложностью и влекущую за собой целый шлейф исторических ассоциаций? Телезрителям показали, что существует небольшая, но увлеченная группа математиков, разбросанных по всему миру, что все они глубоко погружены в предмет своих исследований, общаются друг с другом, следят за последними разработками и вообще посвящают значительную часть жизни продвижению математических знаний. Создатели фильма очень живо показали эмоциональную вовлеченность и социальное единство этих людей. Это не разумные автоматы, а реальные люди, любящие свое дело. В этом и заключается главный посыл фильма.

Мы можем сформулировать три основные причины успеха этой программы: серьезная и известная проблема, герой с увлекательной, по-человечески интересной историей и группа поддержки – целая каста эмоционально вовлеченных в процесс людей. Но я подозреваю, что существует и четвертая причина, не столь явная. Люди, не связанные с математикой, по многим объективным причинам редко слышат о новых достижениях в этой области, да и не так уж сильно интересуются этим. В газетах лишь изредка упоминается что-нибудь связанное с математикой, а если и упоминается, то лишь приводятся какие-то отрывочные или тривиальные факты. Наконец, действия и достижения математиков где-то там за кулисами не оказывают, на первый взгляд, никакого влияния на повседневную жизнь. А школьная математика зачастую предстает перед учащимися как уже закрытая книга, где на каждый вопрос есть готовый ответ. Школьникам обычно кажется, что ничего нового в математике днем с огнем не сыщешь.

Если смотреть под таким углом зрения, то главное в достижении Уайлса – не то, что Великая теорема Ферма была доказана, а то, что наконец-то *в математике свершилось хоть что-то новое*. Поскольку на поиск доказательства теоремы у ученых ушло больше 300 лет, многие зрители восприняли открытие Уайлса как первое существенное достижение в математике за весь этот период. Я не говорю, что все *действительно* именно так и решили. Понятно, что подобная позиция рассыпалась бы в прах при первом же очевидном вопросе вроде: «Почему правительство тратит немалые деньги на финансирование университетских математических исследований?» Но на подсознательном уровне все сочли, что это именно так, не задаваясь вопросами и не размышляя. Поэтому достижение Уайлса приобрело в глазах нематематиков еще большие масштабы.

Одна из целей этой книги – наглядно продемонстрировать всем, в том числе и неспециалистам, что математика сейчас на подъеме, а новые открытия в ней – совсем не редкость. Вы почти ничего об этом не слышите просто потому, что большая часть математических работ слишком сложна для неспециалистов, а средства массовой информации с опаской относятся к интеллектуалам и боятся публиковать что-либо сложнее «Х-фактора». Кроме того, практическое приложение математики обычно скрыто от глаз потребителя, причем зачастую намеренно, чтобы не волновать его. «Что? Работа моего айфона построена на математических формулах? Но у меня же по математике всегда была пара! Как я буду входить в “Фейсбук”?»

Исторически новые достижения в математике часто следуют за открытиями в других областях знания. Исаак Ньютон, разработав законы механики и всемирного тяготения, которые описывают движение планет, не избавился разом от всех проблем в понимании устройства Солнечной системы. Наоборот, после этого перед математиками встал ряд новых вопросов: да, конечно, мы знаем законы, но что они подразумевают? В поисках ответов Ньютон придумал дифференциальное (интегральное) исчисление, но и у нового метода обнаружились ограничения. Зачастую он вместо ответа на вопрос просто дает иную его формулировку. Так, с его помощью некоторые задачи можно легко записать в виде специальной формулы, известной как дифференциальное уравнение. *Решение* этого уравнения и есть искомый ответ. Но это решение еще надо найти. Тем не менее дифференциальное исчисление послужило мощным стартом. Оно показало, что ответ в принципе возможен, и снабдило ученых эффективным методом его поиска. До сих пор, хотя прошло уже больше 300 лет, этот метод помогает математикам совершать крупные открытия.

По мере того как росла сумма математических знаний человечества, все большую роль в мотивации новых исследований стал играть еще один фактор: внутренние запросы самой математики. Если, к примеру, вы умеете решать алгебраические уравнения первой, второй, третьей и четвертой степеней, вам не нужно обладать очень уж богатым воображением,

чтобы задаться вопросом об уравнениях пятой степени. (По существу, степень уравнения есть мера его сложности, но чтобы задать очевидный вопрос, не обязательно даже знать, что это такое.) Если решение не дается – как, собственно, и было, – то этот факт *сам по себе* заставляет математиков еще более усердно искать его, и при этом неважно, будет ли вождь-ленный результат иметь какую-либо практическую пользу.

Я не утверждаю, что практическое приложение не имеет значения. Но если какая-то конкретная математическая составляющая раз за разом возникает в вопросах, скажем, физики волн – океанских волн, вибраций, звука, света, – то понятно, что исследовать ее закономерности было бы полезно. Не обязательно знать заранее, какое приложение найдет новая идея: тема волн фигурирует во многих важных областях, так что серьезные результаты непременно где-нибудь пригодятся. В данном случае этим «где-нибудь» стали радио, телевидение и радары. Если кто-то придумает новый подход к тепловым потокам и без всякого математического обоснования предложит новый блестящий метод, то, безусловно, будет очень полезно разобраться во всем этом *как в чисто математической задаче*. И даже если вам нет никакого дела до тепловых потоков, результат обязательно пригодится где-то еще. Фурье-анализ, разработанный в ходе исследования именно этой области, оказался, возможно, самой полезной математической идеей всех времен. Это, по существу, основа современных телекоммуникаций: он обеспечивает работу цифровых камер, помогает реставрировать старые кинофильмы и звукозаписи, а его современное расширение использует ФБР для хранения отпечатков пальцев.

За несколько тысячелетий подобная взаимосвязь между практическим применением математики и ее внутренней структурой привела к тому, что они тесно переплелись и стали почти неотделимы друг от друга. Тем не менее математика делится на две области: чистую и прикладную. Это деление помогает оценить место математических открытий в структуре человеческого знания, однако оно довольно условно. В лучшем случае так можно различить два конца одного непрерывного спектра математических стилей и методов. В худшем – такая классификация вводит нас в заблуждение относительно того, что именно приносит пользу и что служит источником идей. Как и в других областях науки, силу математике придает сочетание абстрактных рассуждений и вдохновения, почерпнутого из внешнего мира. Говоря попросту, они питают друг друга. Разделить математику на две составляющие не просто невозможно – это бессмысленно.

Большинство по-настоящему важных математических задач – великих задач, которым посвящена эта книга, – возникли внутри математического поля в процессе своеобразной интеллектуальной медитации. Причина проста: это сугубо *математические* задачи. Математика часто представляется набором изолированных областей, в каждой из которых господствуют собственные методы: это алгебра, геометрия, тригонометрия, математический анализ, комбинаторика, теория вероятностей. Ее обычно так и преподают, и не без причины: четкое разделение тем помогает учащимся разложить по полочкам учебный материал в своей голове. И действительно, такое деление – вполне разумный способ понять в первом приближении структуру математической науки, особенно классической, давно устоявшейся. Однако на переднем крае исследований это четкое деление часто рушится. И дело не только в том, что границы между основными областями математики размыты, – в реальности их просто нет.

Каждый математик-исследователь знает, что в любой момент внезапно и непредсказуемо может оказаться, что проблема, над которой он работает, требует свежих идей из какой-то совершенно посторонней, на первый взгляд, области. Более того, новые исследования часто захватывают сразу несколько областей. К примеру, мои исследования сосредоточены по большей части на формировании структур в динамических системах – системах, которые изменяются во времени по определенным правилам. Типичный пример – движение живот-

ных. Лошадь при движении рысью раз за разом повторяет одну и ту же последовательность движений ног, и в этих движениях есть четкая закономерность: копыта ударяют по земле попеременно, диагональными парами. Иными словами, лошадь ставит сначала левую переднюю и правую заднюю ноги, затем правую переднюю и левую заднюю. О чем же эта задача? О паттернах, и тогда решать ее надо методами теории групп – алгебры симметрий? Или это задача из динамики – и тогда к решению нужно привлекать ньютоновские дифференциальные уравнения?

Ответ таков: эта задача по определению относится к обеим названным областям. Причем это не пересечение областей, где мог бы находиться материал, общий для обеих, – они почти не пересекаются. Нет, это новая «область», охватывающая два традиционных раздела математики. Она как мост через реку, разделяющую две страны, связывает их, но не принадлежит ни одной. Но этот мост – не узкая полоса дороги: по размерам его можно сравнить с каждой из соединяемых стран. И, что еще важнее, используемые здесь методы не ограничиваются теми, что используются на прилежащих территориях. Фактически в моих исследованиях пригодились знания во всех областях математики, которые я когда-либо изучал. Так, курс по теории Галуа, который я слушал в Кембридже студентом, был посвящен решению (или, точнее, анализу причин, по которым мы не можем их решить) алгебраических уравнений пятой степени. В курсе по теории графов говорилось о сетях, т. е. о точках, соединенных линиями. Я не занимался динамическими системами, поскольку защищал докторскую по алгебре, но с годами познакомился с основными понятиями по этой теме – от статических состояний до хаоса. Итак, теория Галуа, теория графов, динамические системы: три отдельные области. По крайней мере я считал их таковыми до 2011 г., когда меня вдруг заинтересовал вопрос распознавания хаотической динамики в сети динамических систем, и тогда необходимым для исследования оказалось все то, что я узнал 45 лет назад на курсе по теории Галуа.

Итак, математика не похожа на политическую карту мира, где страны разделяются четкими границами и аккуратно окрашиваются каждая в свой цвет: розовый, зеленый или голубой. Она скорее напоминает естественный ландшафт, где никогда нельзя сказать наверняка, где заканчивается долина и начинаются предгорья, где лес переходит в лесостепь, кустарниковые заросли и настоящие степи, где озера впадают в окружающий ландшафт свои водяные зеркала, а реки связывают заснеженные горные склоны с далеким океаном. Но этот вечно меняющийся математический ландшафт состоит не из скал, воды и растений, а из идей, и соединяет все вместе не география, а логика. К тому же это динамичный ландшафт: он изменяется с появлением новых идей, с каждым новым открытием, с изобретением каждого нового метода. Важные концепции с множеством приложений подобны горным пикам, универсальные методики – широким рекам, несущим путешественников через плодородные равнины. Чем четче вырисовывается ландшафт, тем проще разглядеть на нем непокоренные еще вершины или неисследованные местности, которые часто воздвигают перед путником неожиданные и нежеланные препятствия. Со временем некоторые из этих пиков и препятствий становятся знаковыми. Это и есть великие проблемы математики.

Что делает математическую задачу великой? Интеллектуальная глубина в сочетании с простотой и элегантностью. Плюс к тому она должна быть *сложной*. Кто угодно может взобраться на холмик, но Эверест – совсем другое дело. Сформулировать великую задачу обычно нетрудно, хотя условия могут быть как элементарными, так и очень специальными и понятными только профессионалу. Если Великая теорема Ферма и проблема четырех красок без особых пояснений понятны всякому, кто знаком со школьной математикой, то, к примеру, гипотезу Ходжа или теорию Янга – Миллса даже сформулировать невозможно без привлечения глубоких концепций с переднего края науки (в конце концов, последняя

имеет непосредственное отношение к квантовой теории поля). Тем не менее для специалиста в соответствующей области формулировки этих проблем звучат просто и естественно. Для их изложения не нужны многие страницы непонятного текста. И, наконец, существуют задачи, для детального понимания которых требуется уровень хотя бы университетского курса математики. Но более общий уровень понимания существа проблемы – откуда она взялась, почему важна, что можно было бы сделать, имея ее решение, – как правило, доступен любому интересующемуся, и именно это я попытаюсь вам объяснить. Правда, гипотеза Ходжа – крепкий орешек в этом отношении, поскольку она очень технична и очень абстрактна. Однако это одна из семи математических задач тысячелетия, за решение которых Институт Клэя предлагает приз в 1 млн долларов, и потому о ней непременно стоит рассказать.

Великие задачи несут в себе громадный творческий потенциал: они помогают создавать новую математику. В 1900 г. на Международном конгрессе математиков в Париже Давид Гильберт прочел лекцию, в которой перечислил 23 важнейшие математические проблемы. Он не включил в свой список Великую теорему Ферма, но упомянул ее во вступительном слове. Надо отметить, что, когда выдающийся математик перечисляет великие, по его мнению, проблемы, остальные математики относятся к этому очень серьезно. Понятно, что ни одна задача не оказалась бы в этом списке, не будь она важной и сложной. Для человека естественно отвечать на вызов и преодолевать препятствия. С тех самых пор решение одной из гильбертовых проблем стало отличным способом завоевать себе математические «золотые шпоры». Многие из этих задач слишком специальные, чтобы включать их в эту книгу, другие представляют собой скорее программу, направление исследований, чем конкретные задачи, а некоторые мы рассмотрим позже по отдельности. Но сам список тоже заслуживает упоминания, и я включил его с кратким комментарием в примечаниях^[1].

Именно это делает великие математические задачи великими. Проблема редко заключается в том, чтобы найти ответ. Математики очень четко представляют себе, какими должны быть ответы буквально всех великих задач, – или представляли, если на сегодняшний день решение уже известно. В самом деле, ожидаемый ответ часто заключен уже в формулировку вопроса. Гипотеза представляет собой правдоподобную догадку, предположение, основанное на совокупности данных. Как правило, хорошо изученные гипотезы со временем находят подтверждение, хотя так происходит не всегда. А в случае теоремы Ферма слово «теорема» употребляется (или, точнее, употреблялось) неверно – у теоремы обязательно должно быть доказательство, а его-то, пока не появился Уайлс, и не хватало.

Доказательство – вот то, чего требуют великие задачи и что делает их такими сложными. Любой человек, обладающий определенными знаниями, способен провести несколько вычислений, заметить явную закономерность и кратко сформулировать ее суть. Но математики требуют большего: они настаивают на полном, логически безупречном доказательстве. Или, если гипотеза не подтверждается, на столь же полном опровержении. Вообще же невозможно оценить всю чарующую привлекательность великой задачи, не понимая до конца жизненно важную роль доказательства в любом математическом предприятии. Обоснованное предположение может сделать кто угодно, трудно лишь доказать его истинность. Или ложность.

Концепция математического доказательства менялась с течением времени, причем требования к логике, как правило, становились все строже. Многочисленные высокоинтеллектуальные философские дискуссии о природе доказательства поднимали важные вопросы. Предлагались и внедрялись точные определения понятия «доказательство». Сегодня мы учим студентов, что доказательство начинается с набора некоторых явных допущений, известных как аксиомы. Аксиомы – это, так сказать, правила игры. В принципе возможны и другие аксиомы, но они относятся к другим играм. Первым такой подход предложил древ-

негреческий математик Евклид, но и сегодня он вполне применим. Доказательство на основе принятых аксиом представляет собой серию шагов, каждый из которых является логическим следствием либо аксиом, либо уже доказанных утверждений, либо того и другого. По существу, математика исследует логический лабиринт, перекрестками в котором служат утверждения, а проходами – достоверные умозаключения. Доказательство – путь через лабиринт, который начинается с аксиом. Утверждение, на котором он заканчивается, и есть то, что требовалось доказать.

Однако такое правильное и «причесанное» представление о доказательстве – еще не вся история и даже не самая главная ее часть. Это все равно что сказать: симфония – последовательность музыкальных нот, которая подчиняется законам гармонии. Определение верно, но где же творчество? Такое определение ничего не говорит нам не только о том, как искать доказательство, но и о том, как проверить его, когда оно предложено кем-то другим. Это определение ничего не говорит нам о том, какие места в лабиринте важнее других. Не говорит и о том, какие проходы в нем элегантны, а какие безобразны, какие значительны, а какие бесполезны. Это всего лишь формальное, механическое описание процесса, у которого немало и других аспектов, в частности человеческое измерение. Доказательства ищут люди, и математические исследования – отнюдь не воплощение пошаговой логики.

Формальный подход к определению доказательства может породить доказательства почти нечитаемые, поскольку основные усилия придется бросить на копание в мелочах и «расставление точек над логическими *i*», в то время как решающий вывод будет буквально бросаться в глаза. Поэтому практикующие математики спрямляют путь и оставляют за бортом все рутинные или очевидные шаги. На пропуски обычно указывают фразы вроде «несложно показать, что...» или «из стандартных расчетов следует, что...» Зато ни один математик не пройдет – по крайней мере сознательно – мимо логической трудности и не попытается сделать вид, что ее нет. Более того, компетентный математик постарается обратить особое внимание на слабые с точки зрения логики звенья цепочки рассуждений и потратит большую часть времени и усилий на то, чтобы укрепить их и сделать достаточно надежными. Дело в том, что на практике доказательство – это математическая история с собственным сюжетом. У нее есть завязка, кульминация и развязка. В ней часто можно обнаружить боковые сюжетные ходы, которые вырастают из основного ствола, но ведут каждый к своему результату. Британский математик Кристофер Зиман однажды заметил, что любая теорема – это своего рода интеллектуальная точка покоя, где можно сделать остановку, перевести дыхание и ощутить некоторую определенность. Побочная сюжетная линия помогает свести концы с концами в основном сюжете. Доказательство напоминает литературный сюжет и в других отношениях: в них часто имеются один или несколько главных героев – конечно, это не люди, а идеи, – сложные взаимоотношения которых ведут к развязке и финалу.

Как явствует из формального определения, доказательство начинается с неких четких предположений, движется шаг за шагом от одного логического вывода к другому и заканчивается выводом о том, что вы, собственно, хотели доказать. Но доказательство – не просто список последовательных умозаключений, и логика в нем – не единственный критерий. Доказательство – это рассказ, который выслушивают и разбирают по косточкам люди, посвятившие большую часть жизни искусству прочтения таких историй и поиска в них ошибок и противоречий. Основная цель этих людей – доказать, что автор доказательства *не прав*. Эти люди обладают поразительной способностью замечать слабые места и без усталости долбить в них, пока вся конструкция не рухнет, подняв облако пыли. Вообще, если какой-нибудь математик заявляет, что ему удалось решить крупную проблему (одну из великих, например, или что-нибудь попроще, но тоже достойное), остальные математики не спешат кри-

чать «Ура!» и открывать шампанское. Профессиональный инстинкт велит им прежде всего постараться опровергнуть предложенное доказательство.

Так или иначе, доказательство – это единственный надежный инструмент, при помощи которого математики могут убедиться в собственной правоте. Предвидя реакцию математического сообщества, исследователи тратят огромные усилия на проверку собственных выводов и поиск противоречий в них. Так проще. Если же история успешно выдерживает критический анализ коллег, сообщество вскоре приходит к выводу, что она верна, и в этот момент создатель доказательства получает заслуженные похвалы и награды. Во всяком случае, обычно бывает именно так, хотя непосредственным участникам событий это может видаться иначе. Когда ты вовлечен во что-то, то воспринимаешь все не так, как сторонний наблюдатель.

Как математики решают задачи? Этот вопрос почти не изучался. Современные образовательные исследования на базе когнитивистики в основном ограничиваются изучением образования от начальной до высшей школы. Есть исследования, посвященные преподаванию математики в вузах, но их не так уж много. Кроме того, есть большая разница между освоением и преподаванием математики и новыми исследованиями в этой области. Многие из нас умеют играть на каком-нибудь музыкальном инструменте, но мало кто способен сочинить симфонический концерт или хотя бы написать популярную песенку.

Когда речь заходит о творчестве на высочайшем уровне, почти все, что мы знаем – или думаем, что знаем, – мы получаем путем самоанализа. Мы просим математиков объяснить ход их мыслей и пытаемся выделить в этих описаниях общие принципы. Одной из первых серьезных попыток понять, как думают математики, можно считать книгу Жака Адамара «Исследование психологии процесса изобретения в области математики»¹, вышедшую в 1945 г. Адамар расспросил ведущих математиков и физиков своего времени и попросил описать, как они думают в процессе работы над сложной задачей. И тут выявилась важная и даже необходимая роль того, что за неимением лучшего термина следует назвать интуицией. Их мысли направляло нечто подсознательное. Самые плодотворные их идеи и озарения не приходили постепенно, в результате логической пошаговой проработки, а возникали неожиданно, и весь процесс развивался скачкообразно.

Одно из самых подробных описаний этого на первый взгляд нелогичного подхода к логическим вопросам дал французский математик Анри Пуанкаре – один из ведущих ученых конца XIX – начала XX в. Пуанкаре отметил едва ли не во всех областях математической науки, внес радикальные изменения во многие из них и основал несколько новых ее разделов. В последующих главах мы не раз будем возвращаться к его работам. Кроме того, Пуанкаре писал научно-популярные книги, и, возможно, именно огромный опыт и широта кругозора помогли ему глубже понять процесс собственного мышления. Во всяком случае, он был твердо убежден, что осознанная логика – лишь часть творческого процесса. Да, бывают моменты, когда без нее не обойтись: к примеру, без логики невозможно понять, в чем именно состоит проблема, как невозможно и проверить полученный ответ. Но в промежутке, считал Пуанкаре, его мозг нередко работал над задачей самостоятельно, ничего не сообщая хозяину, причем работал так, что хозяин был просто не в состоянии постичь его методы.

Его описание творческого процесса различает три ключевых этапа: подготовка, вынашивание и озарение. Подготовка представляет собой сознательные логические усилия, направленные на то, чтобы увидеть проблему, точно сформулировать ее и попробовать решить традиционными методами. Этот этап, когда подсознание получает задание и мате-

¹ Адамар Ж. Исследование психологии процесса изобретения в области математики. – М.: Советское радио, 1970.

риал для работы, Пуанкаре считал очень важным. Вынашивание происходит, когда вы прекращаете думать о задаче, отвлекаетесь от нее и занимаетесь чем-то другим. А подсознание тем временем начинает перебирать и комбинировать идеи, часто довольно дикие, и продолжается это до тех пор, пока вдали не забрезжит свет. Если повезет, результатом станет озарение: подсознание даст вам сигнал, и в вашем мозгу как будто вспыхнет лампочка – возникнет готовый ответ.

Такое творчество подобно хождению по натянутому канату. С одной стороны, вы не можете решить сложную проблему, пока не познакомитесь как следует с областью, к которой она относится, а также с множеством других тем, которые могут пригодиться, а могут и не пригодиться в работе, просто на всякий случай. С другой стороны, если, изучая все нужные области математики, вы обратитесь к стандартному, уже много раз безрезультатно опробованному пути, то, возможно, уже не сумеете выбраться из наезженной колеи и ничего нового не откроете. Фокус в том, чтобы много знать и сознательно собирать свои знания воедино, работать над этим неделю за неделей... а затем отложить проблему в сторону. Тогда за дело возьмется интуитивная часть вашего сознания: она отсмотрит все идеи, повертит их так и эдак, оценит, где «холодно», а где «горячо», и сообщит вам, если что-нибудь найдет. Произойти это может в любой момент: Пуанкаре однажды понял, как нужно решать задачу, мучившую его несколько месяцев, выходя из автобуса. Шриниваса Рамануджан, индийский математик-самоучка, создававший замечательные формулы, часто видел новые идеи во сне. А Архимед, согласно легенде, нашел способ определить содержание золота в сплаве, принимая ванну.

Пуанкаре особо указал, что без первоначального периода подготовки успеха не достичь. Подсознанию, настаивал он, необходимо дать как можно больше пищи для размышления, в противном случае удачные идеи, которые в конечном итоге могут привести к решению, просто не возникнут. Вдохновения без трудового пота не бывает. Кроме того, Пуанкаре наверняка знал – ведь об этом знает любой математик-исследователь, – что одного такого трехэтапного процесса редко бывает достаточно. Решение серьезной задачи, как правило, требует нескольких озарений. Этап вынашивания одной идеи может быть прерван вспомогательным процессом подготовки, вынашивания и озарения какой-то другой задачи, решение которой оказалось необходимым для работы над первой, основной идеей. Решение любой стоящей задачи, великой или не слишком, обычно включает в себя множество таких последовательностей, заключенных одна в другой, как замысловатые фракталы Бенуа Мандельброта. Вы решаете задачу, разбивая ее на подзадачи. Вы убеждаете себя, что если удастся решить эти подзадачи, то затем из полученных результатов можно будет собрать решение задачи в целом. Иногда они решаются, иногда приходится возвращаться к началу пути. Иногда подзадача сама рассыпается на несколько кусочков. Даже уследить за происходящим и удержать в голове общую картину порой очень и очень непросто.

Я назвал работу подсознания «интуицией». «Интуиция» – одно из удобных, но вводящих в заблуждение слов, таких как «инстинкт», которые широко используются, хотя и не имеют четкого значения. Подобными словами называют нечто непонятное, присутствие чего тем не менее отрицать невозможно. Математическая интуиция – это способность разума чувствовать форму и структуру и распознавать закономерности, которые мы не в состоянии уловить на сознательном уровне. Интуиция не обладает кристальной чистотой осознанной логики, зато способна привлечь наше внимание к вещам, которые мы никогда не стали бы рассматривать сознательно. Нейробиологи еще только начинают понимать, как человеческий мозг справляется с гораздо более простыми задачами. Понятно, однако, что интуиция, как бы она ни работала, существует благодаря структуре мозга и его взаимодействию с внешним миром.

Зачастую главное, чем помогает в работе интуиция, – она подсказывает, где у задачи слабые места, где к ней можно подступиться с максимальными шансами на успех. Математическое доказательство подобно сражению или, если вы предпочитаете менее воинственные сравнения, шахматной партии. Как только потенциально слабое место выявлено, исследователь бросает в бой (т. е. на его изучение) все свои возможности исследователя, весь математический аппарат, которым владеет. Как Архимед нуждался в точке опоры, чтобы перевернуть Землю, так и математик-исследователь нуждается в рычагах воздействия на задачу. Одна-единственная ключевая идея может раскрыть ее, сделать доступной для стандартных методов. Ну а после этого довести решение задачи до конца – дело техники.

Мой любимый пример рычагов такого рода – задачка, которая не имеет особого математического смысла, но помогает объяснить важный момент. Предположим, у вас есть шахматная доска из 64 клеток и набор костяшек домино, каждая из которых по размеру точно закрывает две соседние клетки доски. Очевидно, 32 костяшек достаточно, чтобы закрыть всю доску. Но теперь представьте, что из доски удалили две противоположных по диагонали угловых клетки, как показано на рис. 1. Можно ли закрыть оставшиеся 62 клетки при помощи 31 костяшки? Попробовав, вы поймете, что ничего не получается. С другой стороны, явных причин, по которым это задание можно было бы счесть невыполнимым, вроде бы тоже не видно. Но ровно до тех пор, пока вы не сообразите, что каждая костяшка домино, как их ни раскладывая, должна закрывать одну черную и одну белую клетку доски. Вот ваш рычаг, и теперь остается только применить его. Он подразумевает, что любая площадь, закрытая костяшками домино, содержит равное число черных и белых клеток. Но противоположные по диагонали клетки – одного цвета (в данном случае – белые), так что при их удалении возникает фигура, в которой черных клеток на две больше, чем белых. А никакую фигуру такого рода полностью закрыть костяшками невозможно. Наблюдение о том, что *любая* костяшка домино обязательно закрывает две клетки разного цвета, и есть слабое место этой головоломки. Поняв это, вы получаете точку, к которой можно приложить логический рычаг – и нажать. Если бы вы были средневековым бароном и осаждали замок, это стало бы для вас слабым местом замковой стены – местом, где следует сосредоточить огонь требушетов или начать делать подкоп.

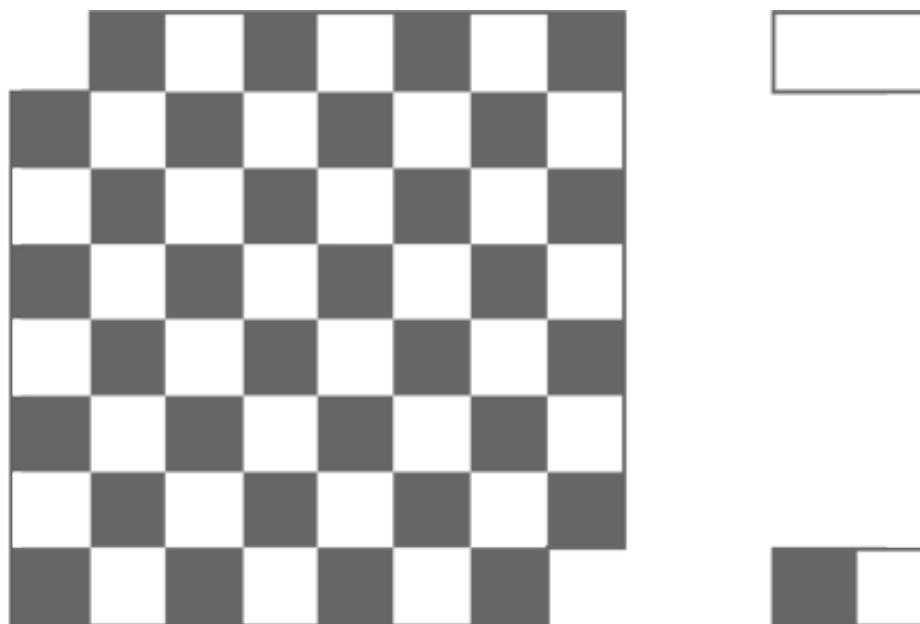


Рис. 1. Сможете ли вы закрыть обрезанную с двух углов доску костяшками домино, каждая из которых закрывает ровно две клетки (вверху справа)? Если вы раскрасите костяшку (внизу справа) и сосчитаете, сколько на доске черных и белых клеток, ответ станет очевиден

Однако в одном существенном моменте математические исследования отличаются от сражения. Любая территория, которую вам однажды удалось оккупировать, остается вашей навсегда, и после этого вы можете сосредоточить усилия на чем-то ином. Но доказанная теорема никуда не исчезает. И именно благодаря этому математики достигают прогресса в решении задачи, даже если дойти до конца им не удастся. Однажды установленный факт становится доступен всем, и воспользоваться им может кто угодно и совершенно в любом контексте. Нередко отправной точкой новой атаки на древнюю как мир проблему становится незамеченное ранее сокровище, затерявшееся в целой куче разнообразных фактов. И это одна из причин, по которым любые новые математические расчеты ценны сами по себе, даже если польза от них не видна сразу. Это еще один кусок завоеванной территории, еще одно оружие в арсенале. Возможно, его время еще придет – но этого не случится, если его посчитают «бесполезным» и забудут или просто не дадут увидеть свет, потому что не поймут, какой в нем *смысл*.

2. Территория простых чисел. Проблема Гольдбаха

Некоторые великие задачи встречаются и в начальном курсе математики, хотя мы этого не замечаем. Вскоре после того, как ребенок осваивает умножение, он знакомится с концепцией простого числа. Известно, что некоторые числа могут быть получены при перемножении двух меньших чисел, к примеру: $6 = 2 \times 3$. Другие, такие как 5, невозможно разложить подобным образом на сомножители. Максимум, что можно сделать, это записать $5 = 1 \times 5$, но в этом выражении нет двух *меньших* чисел. Числа, которые можно разбить на сомножители, называют составными, а те, что разложить невозможно, – простыми. Простые числа кажутся такой несложной темой! Если вы уже умеете перемножать натуральные числа, то способны разобраться и в том, что представляет собой простое число. Простые числа – первичные строительные кирпичики для всех натуральных чисел, и обнаружить их можно в самых разных разделах математики. Но в них есть тайна, и, на первый взгляд, они раскиданы среди положительных целых чисел почти случайным образом. Нет никаких сомнений: простые числа – настоящая загадка. Возможно, это естественное следствие их определения – ведь определяются они не через какое-либо присущее им свойство, а напротив – через свойство, которое у них отсутствует. С другой стороны, для математики это фундаментальное понятие, поэтому мы не можем просто так в ужасе поднять руки и сдаться. Нам необходимо с ними освоиться и каким-то образом вызвать их потаенные секреты.

Некоторые свойства простых чисел очевидны. За исключением самого маленького из них, двойки, все они нечетные. Сумма цифр простого числа, за исключением тройки, не может быть кратна трем. Они, за исключением пятерки, не могут заканчиваться на цифру 5. Если же число не подпадает под эти правила – и под несколько других, более тонких, – то невозможно посмотреть на него и сразу сказать, простое это число или нет. Да, существуют формулы для простых чисел, но это в значительной степени обман. Эти формулы не дают никакой полезной новой информации о простых числах; это просто хитрый способ зашифровать определение «простоты» в виде формулы. Простые числа – как люди: каждое из них – личность, и они не подчиняются общим правилам.

За тысячелетия математики сумели постепенно расширить свои знания о простых числах. Время от времени и сегодня решаются новые серьезные проблемы, с ними связанные. Однако многие вопросы по-прежнему остаются нерешенными. Некоторые из них фундаментальны и легко формулируются, другие понятны немногим. В этой главе говорится о том, что мы знаем и чего не знаем об этих раздражающих своей неприступностью, но все же фундаментальных числах. Начинается она с установления некоторых базовых понятий: в частности, концепции разложения на простые множители – как представить заданное число в виде произведения простых чисел. Даже этот знакомый процесс заводит нас на глубину сразу же, как только мы начинаем задавать вопросы о по-настоящему эффективных методах поиска простых множителей конкретного числа. Как ни удивительно, определить, является ли данное число простым, относительно несложно, но если число составное, то отыскать его простые множители часто намного труднее.

Разобравшись в основах, перейдем к самой известной из нерешенных задач, связанных с простыми числами, – к проблеме Гольдбаха, которой уже 250 лет. В последнее время в работе над ней достигнут колоссальный прогресс, но полностью она пока не решена. А несколько других задач представят нам примеры того, что еще предстоит сделать в этой важной, но трудно поддающейся исследованию области математики.

Простые числа и разложение на множители знакомы нам из школьного курса арифметики, однако большинство интересных свойств простых чисел на этом уровне не рассматривают и никаких доказательств не представляют. Тому есть веские причины: доказатель-

ства даже самых очевидных, на первый взгляд, свойств удивительно сложны. Вместо этого школьников учат некоторым простым методикам работы с простыми числами, акцентируя внимание на вычислениях, где цифры относительно невелики. В результате наши первые впечатления от встречи с простыми числами, как правило, обманчивы.

Древние греки были знакомы с некоторыми базовыми свойствами простых чисел и знали, как их доказать. Простые числа и сомножители – основная тема Книги VII евклидовых «Начал», классического труда, посвященного геометрии. В этой книге имеется, в частности, геометрическое представление арифметических действий – деления и умножения. Греки предпочитали работать не с числами как таковыми, а с длинами линий (отрезков), но их результаты несложно переформулировать на языке чисел. Так, Предложение 16 Книги VII доказывает, что при перемножении двух чисел результат не зависит от того, в каком порядке берутся эти числа. Иными словами, $ab = ba$, фундаментальный закон алгебры.

В школьной арифметике простые делители используют для поиска наибольшего общего делителя двух чисел. К примеру, чтобы найти наибольший общий делитель чисел 135 и 630, мы раскладываем их на простые множители:

$$135 = 3 \times 3 \times 3 \times 5; 630 = 2 \times 3 \times 3 \times 5 \times 7.$$

Затем берем все простые числа, которые присутствуют в обоих разложениях, в наибольшей общей степени; получаем $3^3 \times 5$. Перемножаем, получаем 45. Это и есть наибольший общий делитель. Из этой процедуры создается впечатление, что без разложения на простые множители невозможно найти наибольший общий делитель. На самом деле с точки зрения логики все наоборот. Предложение 2 Книги VII «Начал» представляет метод поиска наибольшего общего делителя двух натуральных чисел без разложения их на простые множители. Метод состоит в последовательном вычитании меньшего числа из большего, а затем остатка из меньшего числа и т. д. до тех пор, пока есть остаток. Для тех же чисел 135 и 630 – это достаточно типичный случай для небольших чисел – процесс выглядит так. Вычитаем 135 из 630 столько раз, сколько сможем:

$$630 - 135 = 495;$$

$$495 - 135 = 360;$$

$$360 - 135 = 225;$$

$$225 - 135 = 90.$$

Поскольку $90 < 135$, переходим к той же процедуре с участием чисел 90 и 135:

$$135 - 90 = 45.$$

Поскольку $45 < 90$, продолжаем то же с числами 45 и 90:

$$90 - 45 = 45;$$

$$45 - 45 = 0.$$

Таким образом, наибольший общий делитель чисел 135 и 630 равен 45.

Эта процедура работает потому, что на каждой стадии происходит замена первоначальной пары чисел более простой парой (одно из чисел уменьшается), которая тем не менее имеет тот же наибольший общий делитель. В конце концов, одно из чисел делится на второе нацело, без остатка, и процесс поиска на этом завершается. В наше время подробное описание вычислительного метода, при помощи которого можно гарантированно найти ответ той или иной задачи, называют алгоритмом. Поэтому и процедура из «Начал» Евклида известна сегодня как евклидов алгоритм. Логически эта процедура первична по отношению к процедуре разложения на простые множители. В самом деле, Евклид использует ее для доказательства основных свойств простых делителей. В современных университетских курсах математики алгоритм Евклида используется с той же целью.

Описанная процедура целиком опирается на евклидово Предложение 30 и была бы невозможна без него. В современных терминах речь в нем идет о том, что если произведение двух чисел – то, что мы получаем при их перемножении – делится на некое простое число, то на это же число должен делиться один из сомножителей. Предложение 32 заключается в том, что любое число либо само является простым, либо имеет простой делитель. Объединив оба утверждения, несложно сделать вывод, что любое число есть результат перемножения простых множителей и что их набор единственный, если не брать во внимание порядок записи. К примеру,

$$60 = 2 \times 2 \times 3 \times 5 = 2 \times 3 \times 2 \times 5 = 5 \times 3 \times 2 \times 2$$

и т. д., но единственный реальный способ получить 60 состоит в том, чтобы взять множители из первого разложения и переставить их местами. Не существует, к примеру, разложения, в котором $60 = 7 \times \text{что-нибудь}$. Существование какого-нибудь разложения следует из Предложения 32. Если число простое – стоп. Если нет, находим простой делитель, делим на него, получая меньшее число, и повторяем процедуру. Уникальность набора делителей следует из Предложения 30. Так, если бы разложение $60 = 7 \times \text{что-нибудь}$ существовало, то одно из чисел 2, 3 и 5 должно было бы тоже делиться на 7, но этого не происходит.

Здесь я должен прояснить один небольшой, но важный момент: исключительный статус числа 1. Согласно приведенному выше определению, оно простое: если мы попытаемся разбить его на множители, максимум, что мы получим, будет $1 = 1 \times 1$, где нет меньших чисел. Однако позже, с развитием теории, такая интерпретация вызывает проблемы, поэтому в последние век-два математики добавили в определение простого числа дополнительное ограничение. Число 1 настолько отличается от всех остальных чисел, что его следует рассматривать как исключение, – это не простое число, но и не составное. Это третья разновидность числа – единица. Одна из причин, по которым мы называем 1 особым случаем, а не относим ее к настоящим простым числам, заключается в том, что если мы согласимся с простотой единицы, то единственность набора множителей нарушится. Вообще-то $1 \times 1 = 1$ – уже нарушение, а уж $1 \times 1 \times 1 \times 1 \times 1 \times 1 \times 1 \times 1 \times 1 = 1$ ни в какие ворота не лезет. Можно было бы изменить определение единственности и сказать «единственный, без учета дополнительных единичных множителей», но это был бы всего лишь другой способ признать, что 1 – число особое.

Много позже, в Предложении 20 Книги IX, Евклид доказывает еще один ключевой факт: «Простых чисел существует больше, чем их насчитывается в любом множестве простых чисел». Иными словами, множество простых чисел бесконечно. Это чудесная теорема и изящное доказательство, но ее появление вызвало множество проблем. Если простые числа уходят в бесконечность, но, судя по всему, расположены без всякой системы, то как можно сказать, на что они похожи?

Мы вынуждены обратиться к этому вопросу потому, что не можем оставить в стороне простые числа – очень существенную деталь математического ландшафта. Особенно часто они встречаются (и особенно полезны) в теории чисел – разделе математики, изучающем свойства целых чисел. Звучит, может быть, достаточно элементарно, но на самом деле теория чисел – один из самых глубоких и сложных разделов математики. Позже мы увидим тому множество свидетельств. В 1801 г. Гаусс, ведущий специалист того времени по теории чисел (а также, по мнению некоторых ученых, один из ведущих математиков всех времен, а может быть, и величайший из них), написал продвинутый учебник по этой теории – «Арифметические исследования» (*Disquisitiones Arithmeticae*). В нем среди множества сложных тем Гаусс указал, что не следует терять из виду два весьма фундаментальных вопроса: «Известно,

что задача отличения простых чисел от составных и разложения последних на простые множители является одной из важнейших и полезнейших в арифметике».

В школе, как правило, учат ровно одному способу поиска простых делителей числа. Заключается он в том, чтобы пробовать по очереди все потенциальные делители, пока не найдется такой, на который число разделится нацело. Если вы не нашли ни одного делителя к тому моменту, как добрались до корня квадратного из первоначального числа – точнее, до наибольшего целого числа, меньшего или равного этому корню, – то число это простое. В противном случае вы найдете множитель, разделите на него и продолжите с новым числом с того же места. Эффективнее всего пробовать только простые делители, но для этого необходим список простых чисел. Поиск останавливается на корне квадратном из числа, потому что наименьший делитель любого составного числа не превосходит корень квадратный из этого числа. Однако для больших чисел эта процедура безнадежно неэффективна. К примеру, если взять число

$$1\,080\,813\,321\,843\,836\,712\,253,$$

то на простые множители оно раскладывается следующим образом:

$$13\,929\,010\,429 \times 77\,594\,408\,257,$$

и, чтобы добраться до меньшего из двух множителей, вам придется опробовать каждое из первых $624\,401\,249$ простых чисел. Конечно, при помощи компьютера это несложно сделать, но если взять для начала число из 100 цифр, которое – так уж случилось – раскладывается на два множителя по 50 цифр в каждом, то систематический перебор последовательных простых чисел продлится до конца Вселенной и вряд ли успеет дать результат.

Нет, вообще-то современные компьютеры, как правило, умеют раскладывать числа из 100 цифр на простые множители. Моему компу требуется меньше секунды, чтобы найти простые множители числа $10^{99} + 1$ (выглядит это число как 1000 ... 001 с 98 нулями). Это число – результат перемножения 13 простых чисел (одно из них повторяется дважды), наименьшее из которых – 7, а наибольшее – 141 122 524 877 886 182 282 233 539 317 796 144 938 305 111 168 717.

Однако если я попрошу компьютер разложить на множители число $10^{199} + 1$, в котором 200 цифр, то жужжать он будет долго, но результата так и не выдаст. Хотя, конечно, даже разложение числа из 100 цифр производит сильное впечатление. В чем тут секрет? В более эффективном по сравнению с последовательным перебором потенциальных простых делителей алгоритме поиска.

Мы сегодня знаем о первой из названных Гауссом задач (проверка числа на простоту) гораздо больше, чем знал он сам, и гораздо меньше, чем хотелось бы, о второй (разложение на простые множители). Здравый смысл говорит о том, что проверка на простоту намного проще разложения на простые множители. Как правило, это удивляет нематематиков, – ведь в школе учат проверять число на простоту тем же методом, что и искать его простые множители: перебором всех возможных делителей. Но, оказывается, существуют хитрые способы доказать простоту числа и без этого. Эти же методы позволяют доказать, что число составное, без нахождения каких бы то ни было его делителей. Достаточно показать, что это число не проходит тест на простоту.

Прапрадедушкой всех современных тестов на простоту может считаться теорема Ферма (чтобы не путать со знаменитой Великой теоремой, о которой речь пойдет в главе 7, ее иногда называют Малой теоремой Ферма). Эта теорема основана на модулярной арифметике, которую иногда называют еще «часовой арифметикой», поскольку числа в ней спирально накладываются друг на друга, как время на циферблате часов. Выберем число – для 12-часовых аналоговых часов это число 12 – и назовем его модулем. Теперь в любых

арифметических вычислениях с неотрицательными целыми числами мы договоримся заменять любое число, кратное 12, нулем. К примеру, $5 \times 5 = 25$, но 24 – это дважды 12, поэтому вычтем из результата 24. Получим $5 \times 5 = 1$ по модулю 12. Модулярная арифметика очень красива, поскольку почти все обычные арифметические законы в ней тоже работают. Основная разница заключается в том, что мы не всегда можем разделить одно число на другое, даже если это не нуль. Модулярная арифметика полезна также тем, что обеспечивает удобный и аккуратный способ разбираться с вопросами делимости: какие числа делятся на те или иные модули без остатка и чему равен остаток, если это не так. Модулярную арифметику предложил Гаусс в «Арифметических исследованиях», и сегодня она широко используется не только в математике, но и в информатике, физике, инженерном деле.

Малая теорема Ферма утверждает, что если взять простой модуль p и любое число a , не кратное p , то степень $(p - 1)$ числа a будет равна 1 по модулю p . Пусть, к примеру, $p = 17$ и $a = 3$. Тогда теорема предсказывает, что остаток от деления 3^{16} на 17 будет равен 1. Проверим:

$$3^{16} = 43\,046\,721 = 2\,532\,160 \times 17 + 1.$$

Ни один человек, находящийся в своем уме, не захочет проводить подобные расчеты для, скажем, 100-значных простых чисел. К счастью, существует хитрый и быстрый способ сделать это. Смысл в том, что ответ не равен единице, если модуль, с которого мы начали, является составным числом. Так что теорема Ферма – надежная основа для эффективного теста, который обеспечивает необходимое условие простоты числа.

К несчастью, одного этого теста недостаточно. Известно, что его проходят и многие составные числа, известные как числа Кармайкла. Самое маленькое из них 561, и в 2003 г. Ред Элфорд, Эндрю Гранвиль и Карл Померанс доказали, к всеобщему изумлению, что таких чисел бесконечно много. Изумление математического сообщества вызвал тот факт, что авторам удалось найти доказательство; сам по себе результат особого удивления не вызвал. Фактически было доказано, что для каждого числа x существует по крайней мере $x^{2/7}$ чисел Кармайкла, меньших или равных x , если x достаточно велико.

Однако более сложные варианты теоремы Ферма действительно можно превратить в тесты на простоту, такие как опубликованный в 1976 г. Гэри Миллером. К несчастью, доказательство достоверности теста Миллера опирается на одну из нерешенных великих математических задач – обобщенную гипотезу Римана (глава 9). В 1980 г. Майкл Рабин превратил тест Миллера в вероятностный, т. е. такой, который может иногда давать неверный ответ. Исключения, если они существуют, встречаются очень редко, но тем не менее доказать, что их нет, невозможно.

Наиболее эффективным детерминированным (т. е. дающим гарантированный результат) тестом на сегодняшний день является тест Адлемана – Померанса – Румели, названный в честь своих создателей – Леонарда Адлемана, Карла Померанса и Роберта Румели. В нем используются концепции теории чисел, куда более сложные, чем теорема Ферма, но примерно того же характера.

Я до сих пор помню письмо одного математика-любителя, предложившего вариант испытания делением. Давайте пробовать все возможные делители, предлагал этот энтузиаст, но начинать с корня квадратного из числа и двигаться, наоборот, вниз. Иногда этот метод действительно позволяет быстрее получить результат, чем при проверке делителей в обычном порядке, но с ростом чисел он, естественно, встречается с теми же проблемами, что и обычный метод. Если применить предложенный вариант к приведенному выше примеру, 22-значному числу 1 080 913 321 843 836 712 253, то квадратный корень из него равен примерно

32 875 725 419. Вам придется перепробовать 794 582 971 простой делитель, прежде чем вы доберетесь до нужного. Это *хуже*, чем искать его обычным путем.

В 1956 г. знаменитый логик Курт Гедель в письме к Джону фон Нейману почти буквально повторил мольбу Гаусса. Он спрашивал, можно ли улучшить метод пробного деления, и если можно, то насколько. Фон Нейман не стал заниматься этим вопросом, но позже другие математики ответили Геделю, открыв практические методы нахождения простых чисел длиной до 100 знаков, а иногда даже больше. Эти методы, самый известный из которых называется методом квадратичного решета, появились около 1980 г. Однако почти все они либо вероятностны, либо неэффективны в следующем смысле.

Как увеличивается компьютерное время, необходимое для вычислений, с ростом объема исходных данных? При тестировании на простоту исходные данные – это не само число, а число знаков в нем. Ключевое различие в этом случае проводится между двумя группами алгоритмов – алгоритмами, принадлежащими и не принадлежащими к классу P . Если время работы алгоритма растет как некая фиксированная степень от размера исходных данных, то алгоритм принадлежит к классу P ; в противном случае – не принадлежит. Грубо говоря, алгоритмы класса P полезны, тогда как те, что не принадлежат к этому классу, непрактичны. Существует, однако, промежуточная полоса своеобразной ничьей земли, где в ход идут другие соображения. Класс P получил название от понятия «полиномиальное время» – именно так замысловато математики говорят о постоянных степенях. Мы еще вернемся к теме эффективных алгоритмов позже, в главе 11.

По стандартам класса P метод пробного деления работает из рук вон плохо. На школьном уровне, где для проверки предлагаются двух- или трехзначные числа, с ним все в порядке, но при работе со 100-значными числами он абсолютно безнадежен. В общем, пробное деление никак не укладывается в P -класс. Если быть точным, то время выполнения этого алгоритма для любого n -значного числа приблизительно равняется $10^{n/2}$, а эта величина растет быстрее, чем любая фиксированная степень n . С таким типом роста, известным как экспоненциальный, по-настоящему *трудно* иметь дело, это страшный сон любого, кто занимается вычислениями.

До 1980-х гг. у всех известных алгоритмов проверки на простоту, за исключением вероятностных или тех, надежность которых оставалась недоказанной, время вычислений росло экспоненциально. Однако в 1983 г. был найден алгоритм, очень соблазнительно лежащий на ничьей земле вблизи P -территории: это уже упоминавшийся тест Адлемана – Померанса – Румели. Его улучшенная версия, разработанная Генри Коэном и Хендриком Ленстрой, имела время вычисления n в степени $\log \log n$, где $\log$ – обозначение логарифма. Технически $\log \log n$ может быть сколь угодно большим, поэтому данный алгоритм не относится к P -классу. Однако это не мешает ему быть пригодным к практическому использованию: если n – гуголплекс, т. е. 1 с 10^{100} нулями, то $\log \log n$ равен примерно 230. Старая шутка гласит: «Доказано, что $\log \log n$ стремится к бесконечности, но никто никогда не видел, как он это делает».

Первый тест на простоту, принадлежащий к P -классу, открыли в 2002 г. Маниндра Агравал и его студенты-дипломники Нирадж Каял и Нитин Саксена. В Примечаниях можно прочитать об этом немного подробнее^[2]. Они придумали алгоритм и доказали, что время его выполнения растет пропорционально не более чем n^{12} ; очень скоро эта величина была уменьшена до $n^{7.5}$. Однако, несмотря на то что их алгоритм относится к P -классу и, соответственно, считается «эффективным», его преимущества не проявляются до тех пор, пока n не становится очень и очень большим. По идее этот алгоритм должен побить тест Адлемана – Померанса – Румели, когда *число знаков* в n приблизится к 10^{1000} . Но такое большое число невозможно разместить не только в память компьютера, но и вообще в известной Все-

ленной. Зато теперь мы *точно знаем*, что алгоритмы Р-класса для проверки простоты числа существуют. Ясно, что поиск лучших алгоритмов в этой категории – дело стоящее. Ленстра и Померанс снизили степень с 7,5 до 6. Если еще некоторые предположения о свойствах простых чисел подтвердятся, степень можно будет снизить до 3, что приблизит нас к практическому применению подобных алгоритмов.

Но самое интересное в алгоритме Агравала – Каяла – Саксены – не результат, а метод. Он прост – по крайней мере для математиков – и отличается новизной. В основе его лежит вариант теоремы Ферма, но, вместо того чтобы работать с числами, команда Агравала использовала многочлены. Многочлен, или полином, – это комбинация степеней переменной x , такая, к примеру, как $5x^3 + 4x - 1$. Многочлены можно складывать, вычитать и перемножать, и обычные алгебраические законы на них тоже распространяются. В главе 3 мы поговорим о многочленах подробнее.

По-настоящему великолепная идея: расширить пространство дискурса и перенести проблему в новую область. Это тот самый случай, когда идея проста настолько, что нужно быть гением, чтобы разглядеть ее. Первый намек на нее проскользнул в статье Агравала и его научного консультанта Сомената Бисваса: авторы предложили вероятностный тест на простоту, основанный на аналоге теоремы Ферма в мире полиномов. Агравал был убежден, что вероятностный компонент этого метода может быть устранен. В 2001 г. его студенты пришли к нему с очень важным техническим замечанием. Начав в нем разбираться, команда углубилась в дебри теории чисел, но постепенно, со временем, все замечания удалось свести к единственному препятствию – вопросу существования простого числа p , такого, чтобы число $p - 1$ имело бы достаточно большой простой делитель. Несколько консультаций с коллегами и поиск в Интернете помогли обнаружить теорему, которую Этьен Фуври доказал в 1985 г. при помощи сложных формальных методов. Именно этого команде Агравала не доставало, чтобы доказать работоспособность алгоритма, и последняя деталь головоломки точно встала на место.

В те времена, когда теория чисел пребывала в своей башне из слоновой кости, вся эта история прошла бы незамеченной и никак не повлияла бы на жизнь остального мира. Но в последние 20 лет простые числа приобрели огромный вес в криптографии – науке о шифрах. Шифры важны не только для военных, у коммерческих компаний тоже хватает секретов. Сегодня, в век Интернета, секреты есть у каждого из нас: мы не хотим, чтобы преступники получили доступ к нашим банковским счетам и номерам кредитных карт. Мало того, все чаще в преступных целях используются и другие личные данные, так что хотелось бы уберечь их все, вплоть до клички домашней кошки. Но Интернет невероятно удобен при оплате счетов, страховании машин и заказе всего, что необходимо для поездки на отдых, и всем нам приходится мириться с риском того, что ценная частная информация попадет не в те руки.

Производители компьютеров и интернет-провайдеры пытаются снизить этот риск, предлагая пользователям различные системы шифрования. Надо сказать, что внедрение компьютеров изменило как саму криптографию, так и криптоанализ – искусство взлома шифров. В настоящее время разработано множество новых шифров. Один из самых известных шифров, который в 1978 г. придумали Рональд Ривест, Ади Шамир и Леонард Адлеман, основан на использовании простых чисел. Больших простых чисел, примерно 100-значных. Система Ривеста – Шамира – Адлемана (известная как RSA) используется во многих компьютерных операционных системах, встроена в основные протоколы безопасного интернет-соединения, ею широко пользуются правительства, корпорации и университеты. Конечно, не каждое новое открытие, имеющее отношение к простым числам, может повлиять на безопасность вашего банковского счета, но это добавляет теме интереса. Как только удастся выяснить что-то новое, что помогает связать простые числа и компьютерные вычис-

ления, это привлекает повышенное внимание. Так случилось и с тестом Агравала – Каяла – Саксены, хотя при всей своей математической элегантности и важности непосредственного практического значения он не имеет.

Тем не менее он позволил немного под другим углом рассмотреть общий вопрос криптографии по Ривесту – Шамиру – Адлеману, и результат вызывает некоторые опасения. До сих пор не существует ни одного алгоритма Р-класса для решения второй из названных Гауссом задач – разложения на простые множители. Большинство специалистов сходится во мнении, что такого алгоритма не существует, но в последнее время их уверенность несколько поколебалась. Поскольку где-то за кулисами, совсем рядом, могут скрываться и другие открытия, подобные тесту Агравала – Каяла – Саксены и основанные на таких же простых идеях, как полиномиальная версия теоремы Ферма (и не важно, что пока о них никто даже не подозревает), может оказаться, что системы шифрования, основанные на разложении числа на простые множители, не настолько надежны, как нам хочется верить. Так что пока не стоит раскрывать в Интернете кличку вашей кошки!

Даже элементарная математика простых чисел ведет к выдвижению более сложных концепций. Евклид доказал, что простые числа уходят в бесконечность, так что невозможно просто перечислить их все и успокоиться. Мы не можем также дать простую и практичную алгебраическую формулу для вычисления всех простых чисел подряд, примерно так, как по формуле x^2 вычисляются квадраты чисел. (Простые формулы существуют, но они «мошенничают», встраивая в формулу сами простые числа под разными личинами, и в результате не сообщают нам ничего нового^[3].) Пытаясь познать природу этих неуловимых и странных чисел, мы экспериментируем, ищем в них признаки структурированности и пытаемся доказать, что найденные нами закономерности присутствуют во всех простых числах, какими бы большими они ни были. Можно, к примеру, задаться вопросом о том, как простые числа распределены среди всех целых чисел. Таблицы простых чисел позволяют предположить, что чем дальше, тем таких чисел становится меньше. В табл. 1 показано, сколько простых чисел содержится в разных диапазонах на 1000 последовательных целых чисел.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.

Комментарии

1.

Вот как выглядят на сегодняшний день проблемы Гильберта и их статус:

2.

Алгоритм Агравала – Каяла – Саксены выглядит так:

3.

Примером того, что я имею в виду, может служить формула, где квадратные скобки обозначают наибольшее целое число, меньшее или равное их содержимому. В 1947 г. У. Миллс доказал, что существует действительная константа A , такая, что для любого n вычисленное по этой формуле значение будет простым. Если считать гипотезу Римана верной, то минимальное значение A , удовлетворяющее условию, равно приблизительно 1,306. Однако эта константа определяется при помощи подходящей последовательности простых чисел, а формула – всего лишь символьный способ записи этой последовательности. Подобные формулы, включая некоторые из тех, что представляют все простые числа, представлены также на сайтах: