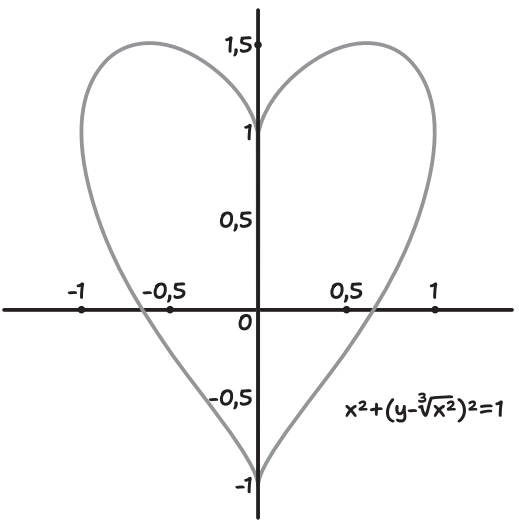
Алексей Савватеев

МАТКУЛЬТ-ПРИВЕТ!

О математике с любовью



ПИТЕР®
Санкт-Петербург • Москва • Минск
2026

ББК 22.1я9
УДК 51
С12

Савватеев Алексей

С12 О математике с любовью. Маткульт-привет! — СПб.: Питер, 2026. — 208 с.: ил. — (Серия «New Science»).

ISBN 978-5-4461-2443-5

Математика — это не просто цифры и формулы, это захватывающее приключение для ума!

И все лекции Алексея Савватеева подтверждают это. Вы думаете, что математика — это скучно? С этой книгой вам скучно не будет. Автор откроет мир удивительных задач, которые заставят ваш мозг работать на полную мощность. Вы увидите забытые школьные примеры в совершенно новом свете.

Здесь нет сухих объяснений и скучных доказательств. Алексей Владимирович показывает, насколько математика может быть изящной и увлекательной. Даже если вы всегда считали себя гуманитарием, эта книга раскроет красоту чисел, логику и изящество интеллектуальных открытий.

Готовы ли вы взглянуть на математику по-новому? Тогда открывайте эту книгу — и приготовьтесь удивляться!

16+ (В соответствии с Федеральным законом от 29 декабря 2010 г. № 436-ФЗ.)

ББК 22.1я9
УДК 51

ISBN 978-5-4461-2443-5

СОДЕРЖАНИЕ

МАТКУЛЬТ-ПРИВЕТСТВЕННОЕ СЛОВО АВТОРА

Дорогие друзья!

Перед вами — очередной математический привет от меня, положенный на бумагу. Содержание лекционных сюжетов, записанное любителями нашей великой и ужасной, самой прекрасной-распрекрасной науки. Несколько наиболее популярных математических зарисовок, которыми я завлекаю слушателей, когда езжу по городам...

«Почему нельзя делить на ноль?», «Почему дважды два четыре?» — вот эти два вопроса выдают полное незнание математики у спрашивающего, и пора положить этому конец! Прочитавший вводные разделы уже никогда подобных вопросов не задаст.

Есть и более содержательные запросы: «Что такое теория игр?», «Кто такие комплексные числа?» (именно компле́ксные, а вовсе не ко́мплексные, как обед, который, правда, тоже, по словам моего учителя, может состоять из действительной и мнимой частей). Для более продвинутых любителей математики будут раскрыты и эти сюжеты, и ряд других, не менее

популярных и захватывающих. Любой читатель, за исключением математиков-профессионалов, найдет в книге что-то интересное, рассчитанное именно на его уровень!

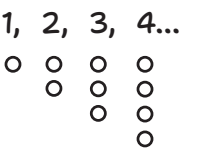
Михаил Бочкарёв (Ростов-на-Дону) и Сергей Полозков (Москва) выступили в роли окончательных редакторов, вылавливая ошибки и опечатки. Спасибо вам огромное, друзья!

Друзья, переворачиваем страницу — и вперед!

Маткульт-вперед!

1. ПОЧЕМУ ДВАЖДЫ ДВА — ЧЕТЫРЕ

Как ни парадоксально, друзья, но то тут, то там меня частенько просят доказать, что два плюс два равно четырем. И что дважды два — тоже четыре.



Мы называем словом «четыре» четвертое число в этом ряду (1, 2, 3, 4, 5...). Можно сказать, натуральные числа создал Бог, но названия-то им придумали мы. Вот они, созданные Творцом условные точки, ну а уж мы вправе добавить к каждой последующей еще одну.

Итак...

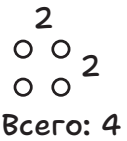
Что же такое «два плюс два»?

Это когда мы к этим имеющимся двум точкам прибавляем еще две

и считаем: первая, вторая, третья, четвертая. Подсчитали — доказали.

1, 2, 3, 4, 5...

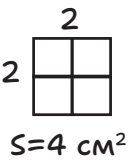
Если говорить про **умножение**, то



> «дважды два» — это нахождение площади квадрата со стороной 2.

Умножить 2 на 2 означает взять два раза по 2. Можем сказать и чуть иначе.

Площадь квадрата со стороной 2 см равна 4 см^2. Пересчитаем: 1, 2, 3, 4 см^2. Вот и все.



Но это доказательство — ссылка на физический опыт. Существует в истории математики такое направление, как «Бурбаки»*, а еще есть подход Германа Вейля**. Что касается математиков из «Бурбаки», то они пытались все на свете аксиоматизиро-

---

* Николя Бурбаки́ (*фр.* Nicolas Bourbaki) — коллективный псевдоним группы французских математиков, созданной в 1935 году. Группа разработала новые принципы подачи математических текстов. Это оказалось непростым для восприятия неподготовленной аудиторией, но зато строгое, формальное изложение исключало любые логические пробелы, а каждая теорема была обоснована и изложена с максимальной точностью. С годами группа создала значительное число терминов и концепций, ставших стандартами в математике.

** Герман Клаус Гуго Вейль [Вайль] (1885–1955) — немецкий математик и физик-теоретик, лауреат премии Лобачевского. Автор философских размышлений о природе математики и ее роли в познании мира.

Николя Бурбаки

Герман Вейль

вать*, и лично я считаю это изначально мертворожденной затеей.

Ну а Вейль, наоборот, говорил, что не нужно пробуксовывать в вопросах, на которые может дать ответ физический опыт. И направлять свое внимание необходимо на интересные и содержательные вещи, которые физический опыт нам сразу даже и не прояснит, и на те, что следует раскрывать постепенно, разворачивая все новые и новые аспекты некоего замысла по поводу устройства нашего мира. Именно это и есть математика! Такова она согласно подходу Германа Вейля.

Моих особо дотошных собеседников интересует и такой вопрос:

— Для чего, собственно, изучать математику?

— **Да чтобы быть умными!**

И это ли не исчерпывающий ответ?!

---

* Аксиоматизировать — сводить к системе простых постулатов.

2. ПОЧЕМУ НЕЛЬЗЯ ДЕЛИТЬ НА НОЛЬ

Деление на ноль

Один из самых частых вопросов, которые задают автору: «Почему делить на ноль нельзя?»

Кстати, этот вопрос еще ничего. Хуже, когда люди допытываются, почему дважды два — четыре? Каждый раз приходится рисовать квадратик «два на два» и показывать: «*Вот вам 1—2, 3—4. Получается, что “четыре” — это и есть “дважды два”*». Но народ не унимается: «*Почему это так называется?*», «*А почему именно так надо делать?*» И начина-а-ется... Но это все не про математику, это про бардак в голове. Впрочем, мы это уже обсудили в первой главе.

А вот «Почему делить на ноль нельзя?» — это про математику. А еще это про физику.

Давайте начнем...

Есть **два принципиально разных подхода**.

Первый — *физический*, а второй можно назвать формальным или *формально-аксиоматическим*.

Начнем с физического подхода, потому что его легче понять большинству людей.

Итак...

Физический подход

Вот вы пришли на какой-то праздник, где много-много детей, и вы этим детям разливаете сверхвкусный сироп. И этого невероятно вкусного сиропа у вас *1 литр*, и его нужно разлить детям (они его потом разбавят, и получится вкуснющий напиток). Учитель говорит: «Та-а-к! Разливать стр-р-рого *по 10 миллилитров*!»

Внимание! **Вопрос:** на сколько детей хватит имеющегося литра сиропа?

Ну, ответ знает любой второклассник (ну, хорошо, второклассник советской школы... Ладно! Любой второклассник

хорошей школы — такие еще остались...). Так вот, он берет *1 литр* и *делит на 10 миллилитров*.

Наш второклассник получает очевидный ответ: *100*.

$$(1 \text{ л}) : (10 \text{ мл}) = 100.$$

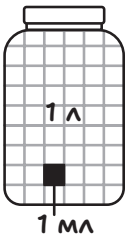
Ответ: 1 литра хватит на 100 школьников.

А потом приходит новое распоряжение, например, от Роспотребнадзора: «*Разливать по 10 миллилитров теперь строго запрещено, это о-очень большая доза! Теперь можно* **только по 1 миллилитру**. *Разливать, а потом все равно водичкой разводить*!»

У нас **новый вопрос**: на сколько детей теперь нам хватит 1 литра сиропа?

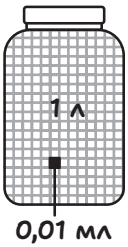
$$(1 \text{ л}) : (1 \text{ мл})$$

Давайте снова спросим у нашего второклассника.



А **ответ** очевиден: «Сиропа хватит на 1000 школьников!» — потому что в 1 литре 1000 миллилитров.

$$(1\ л) : (1\ мл) = 1000.$$



На этом Роспотребнадзор не остановился. Выяснилось, что в больших дозах сироп — это яд, и по новым правилам разрешено давать детям только по 1 капле. И вот мы уже 1 литр делим на одну малюсенькую капельку — примерно на 0,01 миллилитра, и оказывается, что 1 литром можно напоить 100 000 школьников:

$$(1\ л) : (0{,}01\ мл) = 100\ 000.$$

Помните, Христос пять хлебов разделил на несколько тысяч человек, и у нас литра сиропа хватит на 100 000 детей.

* * *

Даже этого разъяснения, полагаю, достаточно, чтобы понять, почему нельзя делить на ноль: да просто потому, что получится бесконечность.

Если вы будете литр делить на все меньшую и меньшую дозу для каждого, в пределе получится то самое деление на ноль: мы делим 1 на 0 и получаем бесконечное число детишек:

$$(1\ л) : (10\ мл) = 100;$$

$$(1\ л) : (1\ мл) = 1000;$$

$$(1\ л) : (0{,}01\ мл) = 100\ 000;$$

$$\ldots$$

$$1\ л : 0 = \infty.$$

Если раздавать по 0 капель, то, естественно, придется раздавать сироп бесконечному количеству детей.

Но *формально бесконечность — это не число*, и фактически измерить его нельзя.

Просто примите утверждение: «**Делить на ноль нельзя!**» Поймите, при делении на ноль все меньших и меньших чисел получаются все большие и большие значения, а это значит, что *в пределе никакого фиксированного значения не получится*.

Все сказанное выше и есть физический подход к объяснению, почему нельзя делить на ноль.

Но я бы не был математиком, если бы не изложил вам...

Формально-аксиоматический подход

Итак, **что такое деление** с точки зрения аксиоматической математики?

Что мы действительно имеем в виду, когда говорим, что a можно разделить на b (что a делится на b):

$$a \vdots b.$$

Когда это происходит?

Ответ такой: по определению, a делится на b тогда и только тогда, когда существует такое c, что при умножении на b оно дает a:

$$a \vdots b \Leftrightarrow \exists c, \text{ такое что } b \cdot c = a.$$

> То есть «разделить» — значит найти такое c, чтобы при умножении его на b получилось a.

Давайте попробуем разделить на 0, скажем, число 1: делится или не делится 1 на 0?

> 1 делится на 0 тогда и только тогда, когда существует число, при умножении которого на 0 получается 1:

$$1 \vdots 0 \Leftrightarrow \exists c, \text{ такое что } c \cdot 0 = 1.$$

Но умножение на 0 — это **аннигиляция**! Это уничтожение. Это значит: «нет *c*», или «*c* умножить на 0 равно 0».

Но ноль единице не равен, поэтому мы не можем поделить единицу на ноль просто формально: не существует такого элемента, который при умножении на ноль давал бы единицу. Таким образом, мы выяснили, что 1 не делится на 0.

$$0 \neq 1;$$
$$c \cdot 0 \neq 1;$$
$$1 \nvdots 0.$$

По тем же причинам это утверждение будет справедливо для любого другого числа, отличного от нуля, например для числа π.

$$\pi \nvdots 0.$$

> **Никакое отличное от нуля число на ноль делиться не может.**

А 0 делится на 0?

Давайте проверим чисто формально: 0 делится на 0? То есть существует ли *c*, при умножении на 0 дающее 0?

Тут у всех должен случиться взрыв мозга... кроме математиков...

Повторим **вопрос**: «Существует ли какое-нибудь число, которое при умножении на 0 дает 0?»

$$c \cdot 0 = 0?$$

Ну да, существует. Вот, например, 1:

$$1 \cdot 0 = 0.$$

Или тот же 0:

$$0 \cdot 0 = 0.$$

и 13 тоже...

$$13 \cdot 0 = 0.$$

При умножении на 0 все они дают 0. Значит, такие числа существуют! При этом мы не спрашивали: «Такое число *единственное* или нет?» Вопрос звучал: «Существует ли?»

Поэтому **чисто формально, алгебраически** (внимание!):

> **0 делится на 0!**

А вот *разделить* 0 на 0 нельзя, потому что «разделить» означает «*найти единственный вариант*», а в данном случае вариант не единственный: **«0 разделить на 0» — это любое число!** Если у нас больше одного результата деления, то мы говорим: «*Нормально разделить нельзя*».

Резюмируем...

Что мы можем сказать про деление на ноль?

Первое: в силу аксиоматического подхода и в силу физического принципа

> **никакое отличное от 0 число на 0 не делится!**

Второе: про «*0 делить на 0*» физический подход вам не скажет ничего, потому что сами физики считают все это абстрактными математическими бреднями. А вот абстрактно-математический подход скажет, что утверждение «*0 делится на 0*» с формальной точки зрения справедливо.

Существует элемент, при умножении на ноль дающий ноль, — берите любой, какой хотите. Но при этом

> разделить 0 на 0, получив какой-то однозначный результат деления, невозможно,

потому что результат получается многозначный.

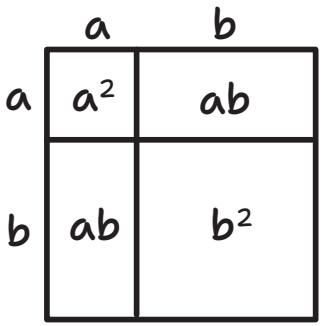
Автор надеется, что вопрос «**Можно ли делить на ноль?**» теперь снят.

3. БИНОМ НЬЮТОНА

Готов рассказать и показать вам, что такое **бином Ньютона** при $n = 3$. То есть как возвести сумму двух слагаемых в третью степень. Ну а случай, когда степень $n = 2$, знаком практически всем, это еще в школе все изучают. Запишем и вспомним:

$$(a + b)^2 = a^2 + 2ab + b^2.$$

Эту формулу легко изобразить на картинке.

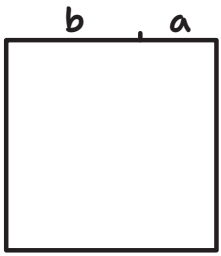


А вот при $n = 3$ речь уже идет о некоей пространственной фигуре, а именно о кубе.

Значит, мы сейчас и рассмотрим этот самый куб, даже немного повскрываем его. Что тут за куб у нас с вами? Голландский сыр! С ним-то мы и поразвлекаемся.

Итак, что такое в данном случае бином Ньютона? Это утверждение о том, из каких слагаемых состоит выражение $(a + b)^3$.

$$(a + b)^3 = ?$$

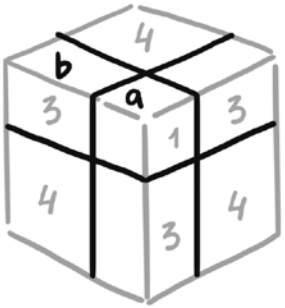


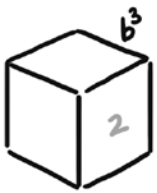
А что такое $(a + b)^3$? Это объем куба со стороной $a + b$. (Как видите, стороны нашего с вами кубика одинаковые.) Пусть вот эта отрезанная часть будет a, ну а рядом останется b. Для наглядности мы сделали нашу a короче, чем b.

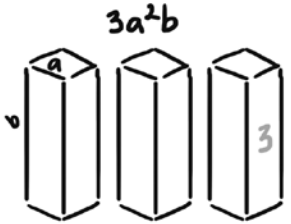
* * *

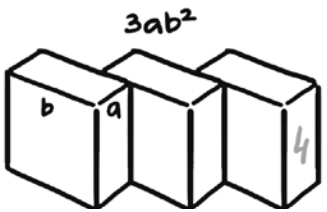
Теперь вспомним одну старую загадку.

Как тремя разрезами разрезать торт на 8 частей? Обычным хозяйкам сложно ответить на этот вопрос, поскольку они









не могут себе представить, что торт пришлось бы разрезать еще и поперек, через середину.

И в самом деле, как это возможно, неужели для этого надо отрезать крем?! Так что такая ситуация — лишь задача для математика, который тремя разрезами в разных плоскостях легко получит 8 кусков торта.

* * *

Ну а мы с вами режем не торт, а сыр. Отделили a от b, повторили такой же вертикальный разрез по соседней грани, а затем сделали третий — горизонтальный — разрез.

Итак, $(a + b)^3$ состоит из восьми слагаемых. Вот они, здесь все. Вот кусок с объемом a^3, а вот самый увесистый b^3 (эх, и повезет же кому-то съесть такой!). Есть 3 одинаковых, судя по объему каждого, a^2b. Ну а эти 3 своими размерами составляют ab^2 каждый.

Так и получается, что

$$(a + b)^3 = a^3 + b^3 + 3a^2b + 3ab^2.$$

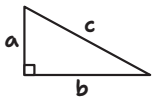
Вот, собственно, и все.

4. ТЕОРЕМА ПИФАГОРА

Сейчас я поделюсь с любителями математики моим любимым доказательством **теоремы Пифагора**.

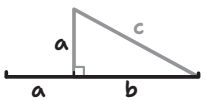
$$c^2 = a^2 + b^2.$$

Итак, есть некий прямоугольный (конечно же!) треугольник со сторонами a, b и c. Назовем его исходным треугольником.



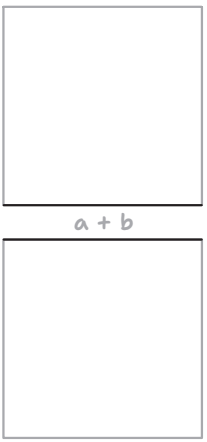
Чтобы доказать: «***c* в квадрате равно сумме *a* в квадрате и *b* в квадрате»**, нужно правильно представлять эти самые квадраты. Для этого я собираюсь начертить квадрат и найти его площадь.

Я делаю следующее: продлеваю сторону b нашего исходного треугольника на длину a:



Доказательство, часть I

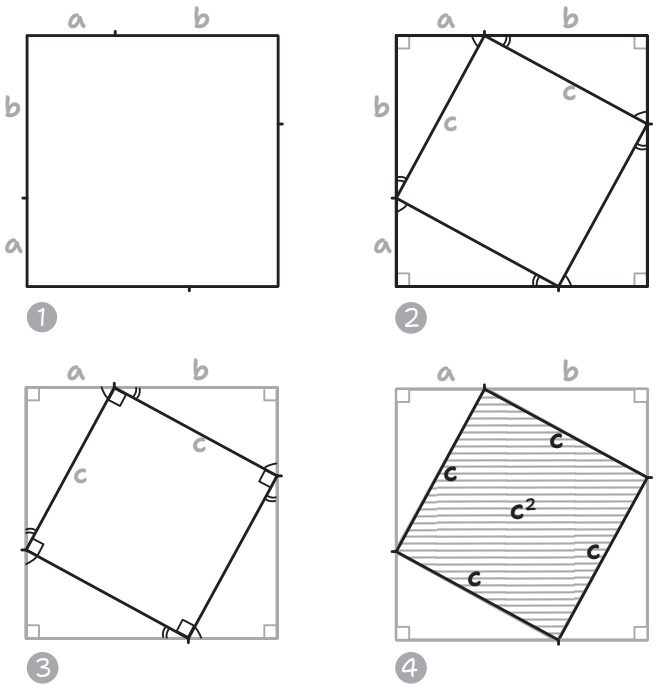
Теперь нарисую соответствующие треугольнику два одинаковых квадрата (да-да, не один, а два!), найду их площади и сравню. Длина каждой стороны получившихся квадратов будет как раз-таки $a + b$.



1. Теперь первый квадрат я размечу так, чтобы в каждом углу уселось по треугольнику: все они представляют собой в точности тот самый, про который я все это пытаюсь доказывать.
2. Вот и продолжим доказывать. Сумма обозначенных мною углов составит 90° (ведь сумма углов любого треугольника на плоскости равна 180°).

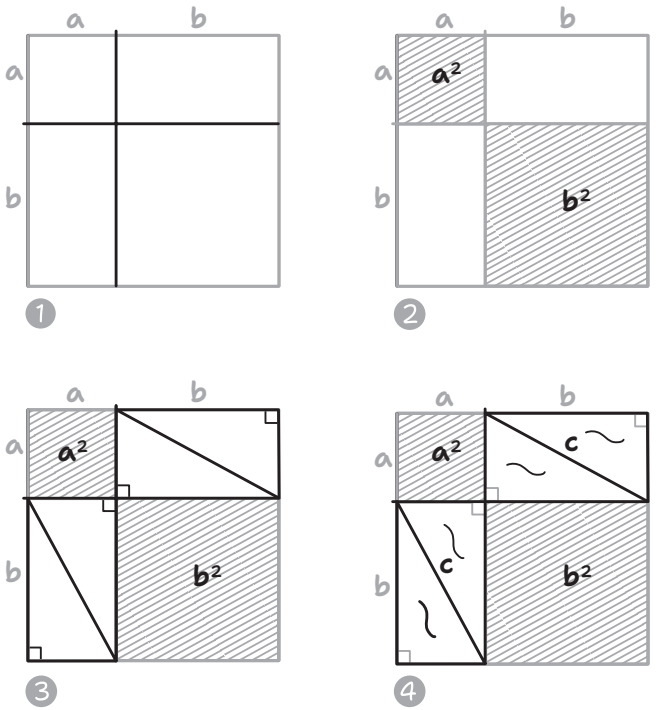
3. Один из углов нашего треугольника прямой, то есть 90°. И поскольку все наши треугольники равны, сумма этих двух углов соседних треугольников тоже будет равна 90°. И угол, оставшийся от развернутого, тоже будет равен 90°.

4. Мы видим получившийся квадрат, каждая сторона которого равна c, и все углы прямые. И площадь его, следовательно, равна c^2. Заштрихуем эту площадь.



Доказательство, часть II

1. Ну а наш второй большой квадрат мы разметим так же, как в разделе «3. Бином Ньютона». Отделим отрезки a и b на его сторонах перпендикулярными линиями.
2. Заштрихуем площадь получившегося квадратика со стороной a. Так же выделим площадь второго квадрата: b^2.
3. Теперь осталось лишь глянуть и сравнить то, что мы отбросили (не заштриховали) в первом и во втором случае.
4. Поможем себе, разрезав каждый из этих «выкинутых» прямоугольников на два треугольника, и увидим, что все эти четыре треугольника совпадают с нашим исходным треугольником.



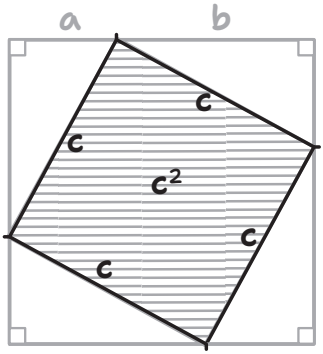
И на квадрате из первой части доказательства (I) мы замечаем то же самое. «За бортом» — четыре исходных треугольника.

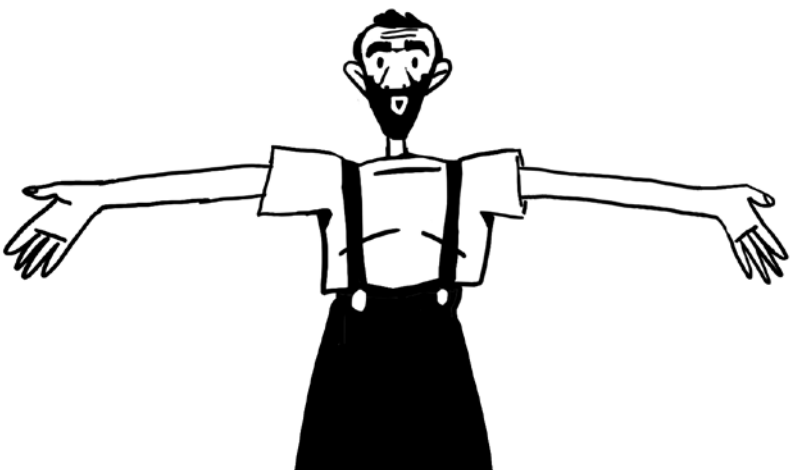
* * *

Иными словами, мы взяли два одинаковых квадрата со стороной $a + b$. Выкинули из каждого из них четыре одинаковых исходных треугольника, но двумя разными способами.

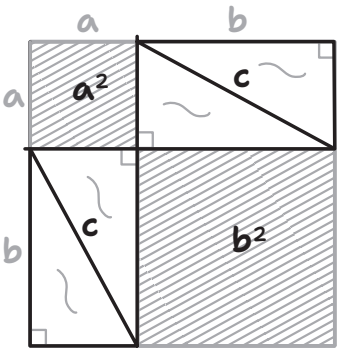
Понятно, что оставшиеся площади — одинаковые.

Площадь квадрата I — c^2.





А квадрат II состоит из квадратов a^2 и b^2.



Поэтому площадь большего квадрата (I) и равна сумме площадей двух оставшихся, меньших, квадратов (II).

$$c^2 = a^2 + b^2.$$

И вот теперь теорема Пифагора полностью доказана!

5. ЗАДАЧА ПРО ЦИКЛИЧЕСКИЙ ПОЕЗД

С **круговой железной дорогой** связана отличная задача.

Представьте, что вас поймал некий царь Дадон и «замуровал» в циклическом поезде. Состоит он из несметного — вам неизвестного! — количества вагонов, и *вы должны ухитриться их сосчитать, находясь внутри этого поезда.*

* * *

Измерить угол поворота тоже не получится — нужного прибора у вас нет. Что же вам дано?

А то, что в каждом вагоне этого циклического поезда есть лампочка и выключатель. Когда вы там очутились, некоторые лампочки были включены, а некоторые выключены. И вы вправе включать и выключать лампочки, сколько хотите.

Условие таково, что, когда вы оповестите Дадона своими криками или звонком по специальному телефону об успешном завершении подсчетов, он тут же вас выпустит (ну а если нет, он вас просто съест). Вот так.

* * *

Ну что, как будем поступать? Для начала подумайте сами, ведь догадаться-то можно. Пейте чаек и размышляйте.

Либо я сейчас расскажу решение.

Итак, *ларчик открывается следующим образом*.

Первым делом **включите лампочку** в том самом вагоне, куда вас впихнули. После этого выберите направление — в какую сторону вы пойдете для обхода поезда. И вот вы переходите в соседний вагон и смотрите, включена ли там лампочка. Если она включена, вы ее **выключаете**. После этого припомните, сколько вагонов вы уже прошли. Всего один? Что ж, пока все понятно.

Затем вы возвращаетесь в предыдущий вагон — *включенная лично вами* лампочка горит. (Но если вдруг ничего не горит, значит, наш циклический поезд состоял, видимо, лишь из одного вагона, и на этом все закончено. Я шучу — скорее всего, будет не так!)

* * *

После этого вы опять идете вперед, в прежнем направлении — до первой включенной лампочки.

И считаете пройденные вагоны. Вот здесь, допустим, свет не горел — идем дальше. В другом вагоне тоже, затем снова темнота, а вот в следующем лампа оказалась включенной!

Как же вам поступить теперь? А вы уже сосчитали, что этот вагон, допустим, — четвертый. И вот эту лампочку вы выключаете, а затем идете обратно, отсчитывая эти четыре вагона уже назад.

Итак, вы снова в том вагоне, с которого начали. И если этот вагон освещен, значит, лампочку вы выключали не в нем. А значит, вы еще не все вагоны обошли.

Ну а если света в нем, первом вашем вагоне, не было, то ясно, что круг вагонов, которые вы подсчитывали, уже замкнулся.

* * *

И дальше, думаю, понятно: раз у нас замкнутая кольцевая дорога, так же как и сам поезд, то при очередном вашем **проходе по всем ранее пройденным вагонам первый вагон с включенной лампочкой будет исходным вагоном, и вы выключите в нем свет.** Потом вы вернетесь назад (конечно же, подсчитывая вагоны), включите вновь свет в вашем первом вагоне, после чего сможете просигналить:

«Э-эй, ты! Дадон! Тут тринадцать вагонов!»

И он ответит:

«Отлично! Выходи на свободу!»

6. КОМПЛЕКСНЫЕ ЧИСЛА

Что же, давайте вспомним, как все это начиналось и развивалось. Математик Кронекер* говорил: «Бог создал натуральные числа, все остальное — дело рук человеческих». И к комплексным числам, к их появлению и роли мы подберемся издалека.

Как появились комплексные числа

Значит, так. Жили-были **натуральные числа**: 1, 2, 3 и так далее до бесконечности

$$\mathbb{N} = \{1, 2, 3, ...\}.$$

(А затем, кстати, в этот ряд встроился и ноль. Для чего? Ну как же, а если у нас ноль крокодилов в комнате? Значит, этот самый ноль обязан существовать и иметь название.)

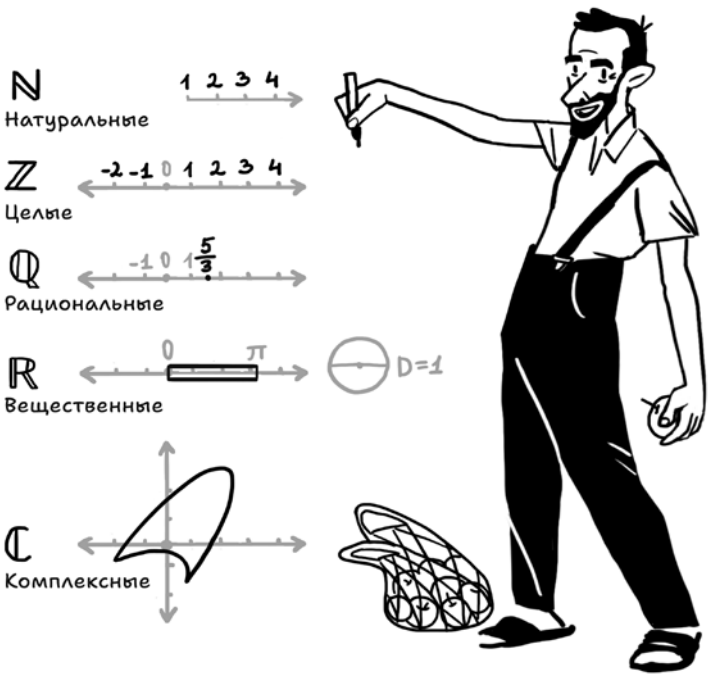
> Ведь натуральные числа используются для подсчета количества предметов. В старом смысле слова это — отличные от нуля положительные числа.

---

* Леопольд Кро́некер (1823–1891) — выдающийся немецкий математик, работавший над теорией чисел, алгеброй и логикой.

Есть еще такое мнение, что **натуральные числа** — это мощности **конечных множеств***. Но пустое множество** — это тоже конечное множество. Значит, его **мощность, равная нулю, должна быть натуральным числом**.

В общем, вне зависимости от того, относить ли 0 к натуральным числам, однажды люди увидели, что уравнение вида, например, $2 + x = 1$ решения в натуральных числах иметь не будет.



* Мощностью конечного множества называют число элементов этого множества.

** Пустое множество — это множество, которое не содержит никаких элементов. Оно обозначается значком $\emptyset$.

> И чтобы решать уравнения вида $2 + x = 1$, нужно изобретать какие-то новые числа.

Допустим, у вас было два яблока, сколько-то добавили, и в итоге вы получили одно яблоко. Сколько же было прибавлено? На самом деле это означает, что одно из яблок вы кому-то задолжали. Вам пришлось его вернуть (его значение «–1»), и осталось у вас лишь одно яблоко.

* * *

Так у нас выстроилась система уже всех целых чисел. Обозначим ее $\mathbb{Z}$. В нее входят 0, 1, –1, 2, –2 и т. д. А вот и всем известная геометрическая интерпретация: числа выстраиваются по обе стороны от 0. Натуральные пошли вправо, а отрицательные целые — влево. Посередине — 0.

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}.$$

Казалось бы, чего лучше? Так ведь хочется иметь возможность делить одно на другое, а это не всегда выходит. 6 на 3 делится, а 5 на 3 не делится. Ну что ж, придумаем $\frac{5}{3}$ — и вставим это вот сюда:

(Этак можно удариться и во все тяжкие, делить без передышки и втиснуть в нашу числовую шкалу все дроби, которые только есть: и со знаком «+», и со знаком «–».)

И вот мы видим, что нам под силу решать любые линейные уравнения, ведь теперь мы имеем дело с системой всех рациональных чисел. Это система всех дробей $\frac{m}{n}$, где m — целое число, а n — натуральное (в старом смысле слова, то есть отличное от 0, положительное число). Математики эту систему чисел обозначают следующим образом:

$$\mathbb{Q} = \left\{ \frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N} \right\}.$$

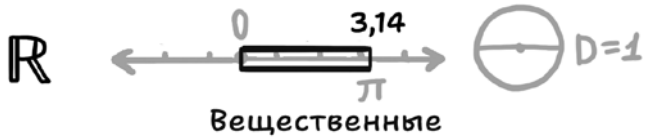
И с такой системой чисел все уже становится очень интересным. Ведь если приглядеться к нашей шкале, то в любом, даже сколь угодно малом по длине, интервальчике всегда есть какая-то дробь.

Что же мы умеем делать с такими числами? Да почти все что угодно! Дроби мы можем складывать и вычитать, умножать и делить (хотя, конечно, бóльшая часть населения Земли этого, к сожалению, делать уже не умеет).

В общем, внутри дробей есть уже все, что только можно душе пожелать, но неугомонные люди знай себе твердят: «Нет, нас интересуют не только дроби, а все **вещественные числа***». Например, на прямой есть $\sqrt{2}$ — решение уравнения $x^2 = 2$, которое дробью не является (впрочем, это тема отдельной беседы).

---

* Вещественные числа (действительные числа) — это числа, которые могут быть представлены точкой на числовой прямой. Они включают в себя как целые, так и дробные числа: отрицательные, положительные, нуль, корни, число π: все десятичные дроби.



Соответственно, появляется необходимость введения системы чисел, полностью заполняющих всю нарисованную ранее числовую прямую.

> Такие числа и называются вещественными: это все числа, которые можно отмерить на числовой прямой.

Например, $\sqrt{2}$ мы можем отмерить как диагональ квадрата, а π — обмерив ниткой окружность нарисованного нами круга с диаметром 1 и приложив эту нитку к нулю на нашей числовой прямой. Второй конец нитки попадет как раз в число π.

То есть все измеримые в физике количества заполняют всю эту числовую прямую.

* * *

Что было дальше? Дальше люди озадачились: «А мы ведь не умеем извлекать корень из –1!»

$$\sqrt{-1} = ?$$

Законный вопрос: «Ну не умеете, и ладно... Зачем вам нужно извлекать корень из “минус единицы”?!» — хочется какого-то внятного объяснения, в чем необходимость.

Например, можно подумать, что кто-то хочет «вообще» решать уравнения вида: **многочлен равен нулю**.

$$f(x) = 0.$$

И первый такой нетривиальный многочлен, который невозможно решить в действительных числах, будет иметь вид:

$$x^2 + 1 = 0,$$

и это то же самое, что извлечь корень из –1, просто сказано более «умным языком» — определить через решение уравнения. В принципе, это хороший подход.

Но у автора есть своя идея, которая кажется более убедительной. **Приступим к этому объяснению!** И снова начнем немного издалека...

* * *

Наверняка каждый из вас неоднократно (хочется надеяться, что с особенной любовью) решал в школе такое уравнение:

$$ax^2 + bx + c = 0.$$

От решения квадратных уравнений никуда не деться, в том числе и в жизненных задачах. Нужно уметь их решать.

Сначала сократим на a:

$$x^2 + \frac{b}{a}x + \frac{c}{a} = 0;$$

затем, возведя в квадрат $x + \frac{b}{2a}$, мы получим следующее выражение:

$$\left(x + \frac{b}{2a}\right)^2 = x^2 + \frac{b}{a}x + \frac{b^2}{4a^2}.$$

Сравнивая правую часть этого выражения с левой частью исходного уравнения, мы видим очевидное сходство. Перегруппируем слагаемые и получим после несложных преобразований (проведите их самостоятельно!) стандартную формулу:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Эта формула — времен Аль-Хорезми*. Этого человека, собственно, мы все должны благодарить за курс алгебры восьмого класса. Возникает **вопрос**: можно ли так же поступить с уравнением следующего вида:

$$ax^3 + bx^2 + cx + d = 0?$$

Вопрос очень интересный. Это уже кубическое уравнение! До XVI века никто не знал, что с ним делать, но тогдашние математики Кардано, Тарталья и ученик их Феррари исхитрились **решить это кубическое уравнение**!

Мухаммад Аль-Хорезми

* Мухáммад ибн Мусá Аль-Хорезмú (ок. 780 — ок. 850), «отец алгебры», — математик, астроном, географ, философ, переводчик и историк. Впервые представил алгебру как самостоятельную науку об общих методах решения линейных и квадратных уравнений, дал классификацию этих уравнений. Разработал подробные тригонометрические таблицы, содержащие функции синуса, косинуса, тангенса и котангенса.

Как же им это удалось?

С помощью манипуляций, подобных описанным выше, и «перенормировки» коэффициентов ученые уже 1000 лет назад научились приводить любое кубическое уравнение к виду:

$$x^3 - 3px - 2q = 0 \qquad (1)$$

(если при x был некий коэффициент β, то здесь мы за p ради удобства обозначили $\beta/3$).

Но что делать дальше, было совершенно непонятно... Поиск ответа занял четыре века! А мы управимся за несколько минут, потому что уже знаем, как надо действовать!

* * *

Гениальнейшая идея то ли Тартальи, то ли Кардано, то ли обоих состояла в том, чтобы **искать решение в виде суммы двух чисел**:

$$x = \alpha + \beta.$$

Суть в том, что помимо неизвестного x следует найти еще два числа — α и β, тоже неизвестные, но которые в сумме дадут x. Иными словами, нужно искать удобный способ представить x в виде суммы α и β, которые так или иначе удалось бы найти с помощью уже известных на тот момент методов. Речь, конечно же, о том, что **надо свести кубическое уравнение к квадратному, и тогда получится его решить**: найдя α и β, удастся найти x.

Мы с вами будем пользоваться свободой выбора чисел, сумма которых составит число x.

Итак, если величина x представлена суммой двух неизвестных чисел $\alpha + \beta$, то чему будет равен ее куб x^3? Воспользуемся формулой бинома Ньютона (немного сокращенной):

$$x^3 = (\alpha + \beta)^3 = \alpha^3 + \beta^3 + 3\alpha\beta(\alpha + \beta).$$

Не забываем, что $\alpha + \beta$ — это x. И если $x = \alpha + \beta$, то

$$x^3 = \alpha^3 + \beta^3 + 3\alpha\beta x. \qquad (2)$$

Вот такая вывелась классная формула!

И теперь мы подставляем (2) в (1), и у нас получается:

$$\alpha^3 + \beta^3 + 3\alpha\beta x - 3px - 2q = 0$$

или

$$(\alpha^3 + \beta^3 - 2q) + 3(\alpha\beta - p)x = 0.$$

Внимание! Если $\alpha^3 + \beta^3 - 2q$ и $3(\alpha\beta - p)x$ будут равны 0 (то есть если мы добьемся равенства нулю содержимого этих двух скобок), то мы решим наше уравнение.

> Иными словами, если мы подберем такие α и β, что содержимое обеих скобок обнулится, то сумма $\alpha + \beta$ и станет решением исходного уравнения.

Это гениальнейший трюк, и совершенно неудивительно, что почти четыре века люди не могли до него додуматься. Ведь по тем временам, когда еще никто толком не умел обращаться с буквами (переменными), такой ход мысли и впрямь представляется очень остроумным (видимо, когда в математику ввели буквы — тогда и догадались).

Итак, **нужно найти α и β, удовлетворяющие двум уравнениям** ($\alpha^3 + \beta^3 = 2q$ и $\alpha\beta = p$), и если это получится, то задача будет решена. Посмотрим, что из этого следует:

$$\begin{cases} \alpha^3 + \beta^3 = 2q \\ \alpha \cdot \beta = p \end{cases} \Rightarrow \begin{cases} \alpha^3 + \beta^3 = 2q \\ \alpha^3 \cdot \beta^3 = p^3 \end{cases}.$$

Если бы мы никогда не слыхали о комплексных числах (а мы как раз в контексте XVI века будто ничего о них и не знаем), то замена $\alpha \cdot \beta = p$ на $\alpha^3 \cdot \beta^3 = p^3$ была бы эквивалентной заменой, ведь операция возведения в куб является взаимно однозначным преобразованием множества вещественных чисел.

Итак, нам нужно найти α и β, решив вот эти уравнения:

$$\begin{cases} \alpha^3 + \beta^3 = 2q \\ \alpha^3 \cdot \beta^3 = p^3 \end{cases}.$$

А это не что иное, как формулы Виета* для уравнения

$$z^2 - 2qz + p^3 = 0.$$

И такое уравнение мы можем решить.

---

* Формулы Виета связывают коэффициенты многочлена с его корнями, ими удобно пользоваться для проверки правильности нахождения корней многочлена, а также для составления многочлена по заданным корням. Неявно присутствуют в работах Франсуа Виéта (1540–1603), французского математика, основоположника символической алгебры.

Корни — z_1 и z_2 (то есть два разных корня) будут иметь следующий вид — и это, соответственно, α^3 и β^3 (по формуле Виета).

$$z_{1,2} = q \pm \sqrt{q^2 - p^3} = \alpha^3, \beta^3.$$

Но если так, то сами α и β — это кубические корни из полученных выражений: в одном случае со знаком «+», в другом — со знаком «–». А x как сумма α и β (вспоминаем: x был «закодирован» как α + β) представляет собой — извлекаем кубические корни! — следующее выражение:

$$x = \alpha + \beta = \sqrt[3]{q + \sqrt{q^2 - p^3}} + \sqrt[3]{q - \sqrt{q^2 - p^3}}. \qquad (3)$$

Получается **формула Кардано** — и да, ничего красивее в алгебре мы, наверное, не встречали! Однако справедливо будет задаться вопросом: «Так при чем же здесь комплексные числа?!»

А вот при чем...

Рассмотрим кубическое уравнение:

$$(x - 1)(x - 2)(x + 3) = 0. \qquad (4)$$

Капитан Очевидность утверждает, что его корни — это 1, 2 и –3. Теперь давайте перепишем уравнение, раскрывая все скобки по правилам:

$$x^3 - 7x + 6 = 0.$$

Если мы сравним с формулой $x^3 - 3px - 2q = 0$, с которой мы уже умеем работать, то увидим, что в нашем случае

$$p = \frac{7}{3},$$
$$q = -3.$$

Похоже на правду!

Подставляем значения в формулу Кардано (3) и получаем:

$$x = \sqrt[3]{q + \sqrt{q^2 - p^3}} + \sqrt[3]{q - \sqrt{q^2 - p^3}} = \\ = \sqrt[3]{-3 + \sqrt{9 - \frac{343}{27}}} + \sqrt[3]{-3 - \sqrt{9 - \frac{343}{27}}} = \ldots \quad (5)$$

А теперь внимание! То, что мы сейчас написали, должно быть равно вот этим трем корням:

$$\{1, 2, -3\}.$$

Или хотя бы одному из них (раз мы умеем решать кубические уравнения)! А лучше всем трем, хотя это и кажется странным.

Так что давайте вернемся к (5) и продолжим разбираться, что здесь вообще происходит:

$$\ldots = \sqrt[3]{-3 + \sqrt{\frac{-100}{27}}} + \sqrt[3]{-3 - \sqrt{\frac{-100}{27}}}.$$

Finita la commedia, как говорится. Чтобы найти корни уравнения (4) (которые мы уже и так прекрасно знаем: 1, 2 и –3), нам придется извлекать квадратный корень из –100. А мы его извлекать не умеем! Вообще.

* * *

Вернемся к вопросу: зачем нужны комплексные числа? Вот вам и ответ:

> затем (хотя и не только!), чтобы решать кубические уравнения, такие как (4), с тремя вещественными корнями.

Иными словами,

> чтобы решить в виде формул кубическое уравнение с тремя вещественными корнями, требуется извлечь корень из отрицательного числа. То есть зайти в область комплексных чисел и, выходя из нее обратно в вещественные, получить решение.

Такая мотивация, побудившая людей искать решение, как извлекать корень из «минус единицы» (помните, мы с нее и начали наши поиски), кажется автору абсолютно убедительной и — внимание! —

> иного способа решать кубические уравнения никто до сих пор не знает

и знать, видимо, не будет, потому что (и это принципиальный момент!) заход в комплексные числа здесь необходим. То есть, чтобы решать уравнение даже с вещественными корнями, нужны комплексные числа. Для квадратных было не так: решения либо существовали, либо не существовали (мы-то знаем, что в комплексных числах решения существуют всегда и даются той же формулой, но здесь ситуация гораздо круче. И вещественные числа никак без комплексных обойтись не могут).

Можно не сомневаться: мы получили неплохую мотивацию для рассмотрения комплексных чисел и можем к ним переходить.

Извлечение корня из отрицательного числа

Итак, чтобы найти $\sqrt{-100}$, явно нужно научиться извлекать корень из -1, потому что с корнем из 100 мы уж потом как-нибудь справимся.

$$\sqrt{-100} = \sqrt{(-1)}\sqrt{100} = 10\sqrt{-1}.$$

Что же такое $\sqrt{-1}$?

Вряд ли мы наглядно представляем, что это такое, ведь среди вещественных чисел такого числа нет, поэтому обозначим значение $\sqrt{-1}$ специальной буковкой i.

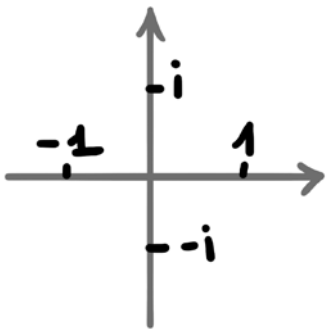
$$i = \sqrt{-1}.$$

Сразу же отметим, что $-i$ тоже будет являться значением $\sqrt{-1}$, потому что при возведении $-i$ в квадрат наше $(-i)^2$ будет равно тому же самому, что i^2 (ведь перемножение двух отрицательных чисел (-1 на -1) дает положительное число).

Теперь надо понять, как это изобразить — ведь нам же хочется «увидеть живьем» комплексные числа!

Ответ таков: если числовую прямую заполняют все вещественные числа, а $\sqrt{-1}$ на ней очевидным образом нет, то это число должно проявиться не на этой прямой, а где-то на плоскости. Давайте выведем на плоскость два числа: и положительное (i), и отрицательное ($-i$).

Это естественная форма **геометрического изображения комплексных чисел**.



Итак, у меня появилось число *i*, которое позволяет извлечь корень из –1 и вместе с тем, как мы понимаем, извлечь корень из любого отрицательного числа.

Арифметические действия с комплексными числами

Возникает **предположение**: если у нас есть число *i*, есть число 1 и вообще все вещественные числа, то, наверное, мы можем «домножать» вещественные числа на число *i* и получать какие-то новые числа: $x + yi$, потому что мы хотим получить систему, в которой будут возможны арифметические действия: сложение, вычитание, умножение, деление! Иначе все это мы не сможем называть числами (разве что какими-то матрицами или функциями... Ведь когда мы имеем дело с числами, нам все-таки требуется возможность выполнять арифметические операции).

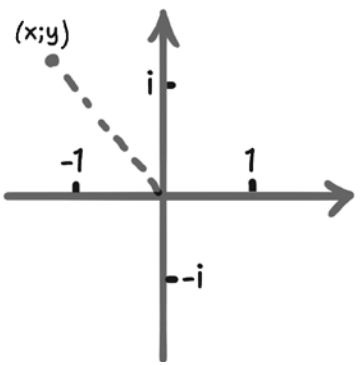
> Числа — элементы поля, а поле — это и есть то множество элементов, где по обычным правилам выполняются операции «+», «–», «×» и «:».

И мы с вами собираемся **превратить комплексные числа в поле**, а для этого нам в первую очередь нужно понять, из какого арсенала, из какого набора чисел мы исходим.

Автор утверждает, что $x + yi$ никогда не может быть равен $z + ti$ — естественно, кроме ситуации, когда $x = z$, а $y = t$.

$$\{x + yi\} \neq \{z + ti\}.$$

О чем идет речь? О том, что **любая точка плоскости** с координатами $(x; y)$ или $(z; t)$ и т. д. «производит на свет» **уникальное комплексное число**.



Понятно, что **каждой точке плоскости должно соответствовать какое-то число**: ведь мы должны уметь умножать y на i; должны уметь складывать yi и x. Значит, такое комплексное число должно существовать.

yi тоже не будет вещественным, иначе i было бы равно отношению двух вещественных чисел, то есть являлось бы вещественным.

Следовательно, числа yi и ti — совершенно новой природы, и они не равны x и z. И суммы $x + yi$ и $z + ti$ — тоже разные, они никогда не могут быть равны друг другу. Вот что важно понимать! Докажем это методом от противного.

Доказательство:

Если бы

$$x + yi = z + ti,$$

то это значило бы, что либо 1) $y = t$, тогда после сокращения мы получили бы $x = z$, это как раз тот случай, когда x и z получены из одной и той же точки плоскости;

либо 2) $y \neq t$, тогда из уравнения $x + yi = z + ti$ мы получили бы $x - z = (t - y)i$, при том что $(t - y) \neq 0$.

Раз $(t - y) \neq 0$, то на него можно делить, и $i = (x - z)/(t - y)$. Значит, i тогда тоже было бы вещественным ($\mathbb{R}$):

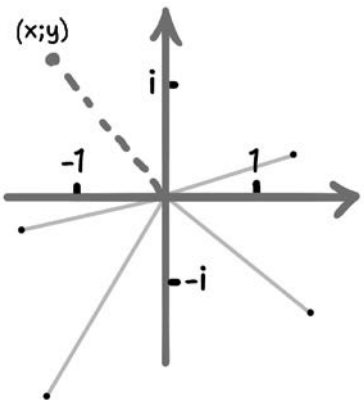
$$i = \frac{x-z}{t-y} \in \mathbb{R},$$

что является противоречием!

Вывод:

> если бы хотя бы какие-то две разные точки (где бы они ни были расположены) дали одно и то же комплексное число, то из этого обязательно следовало бы, что число i — вещественное. А мы знаем, что вещественных чисел, в квадрате дающих -1, не существует и быть не может. А значит, суммы вида $x + yi$ или $z + ti$ для всех точек плоскости — разные.

И вот так у нас словно открылся ящик Пандоры: раз мы «пригласили» в общество чисел то самое *i*, то одновременно мы «пригласили» всю прямую, на которой расположены *i* и *–i*, со всеми числами на этой прямой, да и всю плоскость в целом. Вообще всю.



* * *

А допустим, придет кто-нибудь и спросит: «А может, еще что-то “пригласили”?» Это в зависимости от того, что вас интересует. Если вас интересует огромная, бесконечная система, то тогда можете включать в нее абсолютно все. Но в нашем случае важно только одно: построить систему чисел, которая позволяет извлекать корни из отрицательных чисел и при этом будет максимально компактной, без вовлечения новых чисел. Нам нужна система чисел, которая является полем, то есть в ней можно и складывать, и вычитать, и умножать,

и делить. И вдобавок извлекать корни из отрицательных чисел. Поэтому

> нам достаточно всей этой плоскости и ничего нового не понадобится. То есть мы сможем научиться складывать, вычитать, умножать и делить комплексные числа, записанные в форме $\{x + yi\}$.

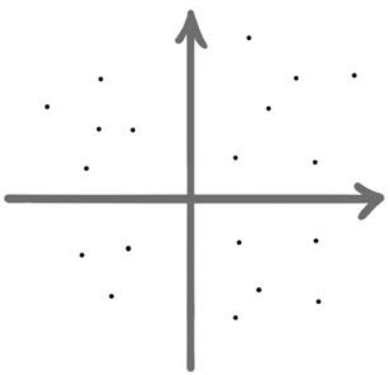
И все числа, которые в результате будут получаться, станут соответствовать той же самой форме. И если мы это установим, то можно будет заявить, что **комплексные числа представляют собой лишь плоскость: ту, в которой мы с точками научились выполнять арифметические операции**.

К этому и перейдем!

Сложение и вычитание комплексных чисел

Итак, верно утверждение:

> комплексные числа — это все точки плоскости.



Чтобы обосновать это утверждение, нам нужно **доказать, что точки плоскости можно складывать, вычитать, умножать и делить по обычным правилам**.

Но на самом деле правила уже продиктованы **двумя принципами**:

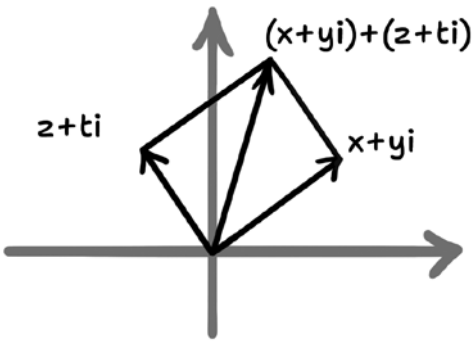
1. В результате действий с вещественными числами получаются вещественные числа.
2. Корень из –1 существует, и это число i.

Действительно, понятно, что

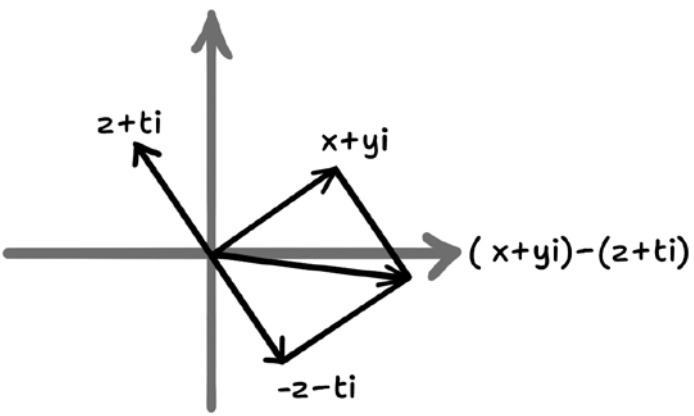
$$(x + yi) \pm (z + ti) = (x \pm z) + (y \pm t)i.$$

Мы видим, что после раскрытия скобок мы получили число того же вида, который оно имело до того, то есть **«вещественное + вещественное, кратное числу *i*»**.

Со сложением и вычитанием понятно, и геометрически проверить, что это означает, может каждый из вас. Это обычное **правило параллелограмма либо треугольника**.



Что касается разности, то мы, наоборот, вычитаем $z + ti$. Вектор, противоположный $z + ti$, направлен в обратную сторону и будет равен $–z – ti$, и векторное вычитание будет иметь следующий вид:



Умножение комплексных чисел

Попробуем сейчас просто раскрыть скобки (если вы устали от сложности уравнения Кардано (3), разжуем максимально полно, соблюдая все правила работы с вещественными числами, согласно закону коммутативности):

$$(x + yi)(z + ti) = x(z + ti) + yi(z + ti) = xz + xti + yiz + yiti = \\ = xz + xti + yzi + yti^2.$$

И вот тут мы вспоминаем, что $i^2 = -1$.

Поэтому мы сгруппируем xz с yt, поменяв знак на противоположный, и прибавим оставшуюся без изменения знака часть. Выражение приобретет следующий вид:

$$(xz - yt) + (xt + yz)i.$$

И мы видим, что

> умножение комплексных чисел дает комплексное число.

Или так:

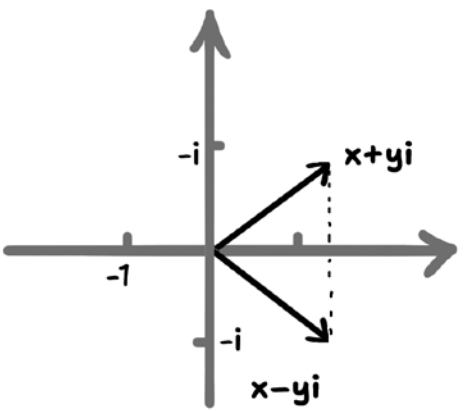
> умножение чисел формы «вещественное + произведение вещественного с i» имеет в результате ту же самую форму: сумма вещественного числа и произведение вещественного с i.

Деление комплексных чисел

Чтобы выполнить деление, нужно вспомнить об обратных числах: взять обратное комплексному число и домножить его на обратное. Наш прием здесь состоит в домножении обеих частей на то, что называется **числом, сопряженным комплексному**.

$$\frac{1}{x + yi} = \frac{x - yi}{(x + yi)(x - yi)}.$$

Посмотрите на нашу плоскость: $x - yi$ станет просто симметрично отраженным от $x + yi$ относительно вещественной прямой.



На $x - yi$ мы и домножаем (по правилам арифметики ничего не должно меняться).

Попробуем раскрыть скобки в знаменателе $(x + yi)(x - yi)$: yix и $-yix$ будут сокращены, так как это одно и то же, но с разными знаками; останется $x \cdot x$ минус $y^2 \cdot i^2$, а это зна-

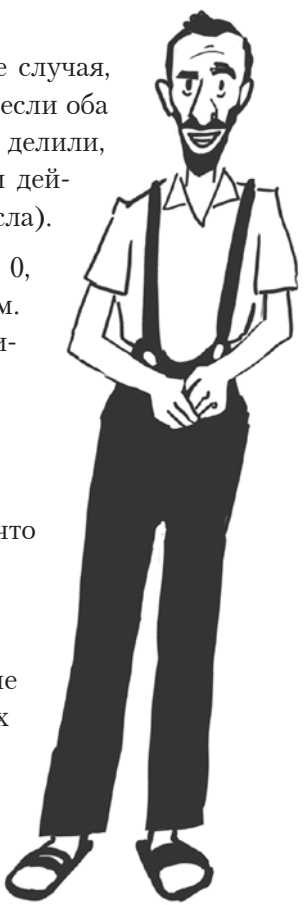
чит, что надо прибавить y^2. В итоге получаем в знаменателе $x^2 + y^2$:

$$\frac{1}{x + yi} = \frac{x - yi}{(x + yi)(x - yi)} = \frac{x - yi}{x^2 + y^2} = \dots$$

* * *

Чем хорошо выражение $x^2 + y^2$?

1. Оно вещественно.
2. Оно строго положительно, кроме случая, когда оба слагаемых равны 0 (но если оба равны 0, тогда бы мы на него не делили, так как делить на 0 нельзя — ни действительные, ни комплексные числа).



Но если хотя бы x^2 или y^2 не равно 0, то поделить на $x^2 + y^2$ мы сможем. И продолжение нашего равенства примет вид:

$$\dots = \frac{x}{x^2 + y^2} - \frac{y}{x^2 + y^2} i.$$

Сравните: это число того же вида, что и $(x \pm z) + (y \pm t)i$.

Поэтому, как нам стало ясно,

> умножение, деление, сложение и вычитание в комплексных числах не выводит за их пределы, то есть плоскости чисел нам вполне достаточно.

Подведем итоги:

1. Мы получили мотивацию изучать комплексные числа, потому что без них даже кубические уравнения решить не получится. Не говоря уже о каких-либо уравнениях гидродинамики, которая вся на них стоит.
2. Мы узнали, что комплексные числа заполняют обычную плоскость.

Удачи всем в дальнейшем изучении комплексных чисел!

7. О ТЕОРИИ ВЕРОЯТНОСТЕЙ

Помните старый анекдот?

> *Однажды у блондинки спросили, какова вероятность того, что она встретит сегодня динозавра. Подумав, блондинка ответила: «50 на 50: либо встречу, либо нет!»*

Смешно, но неправильно! А почему — мы узнаем далее, когда **противопоставим науку мифам о теории вероятностей** (сокращенно: «терве́р»).

В представлении обывателя в словосочетании «теория вероятностей» много чего намешано: его готовы приладить и к математике, и к физике, и даже к вопросу «а с какой вероятностью во-о-н из той огромной тучи польет дождь (или повалит снег)?» или «с какой вероятностью башмаки моего сына станут ему малы к следующему сезону?». При этом никакой иной вопрос, касающийся математики, не окружен таким жутким количеством мифов, как теория вероятностей.

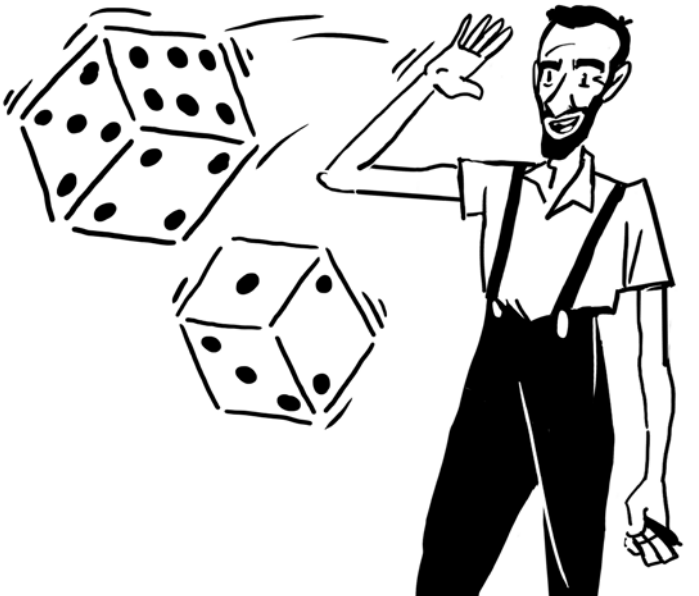
Обратите внимание: «теория вероятностЕЙ» — во множественном числе, потому что

> по жизни нам приходится иметь дело не с какой-то одной вероятностью. Обычно в мозгу просчитываются вероятности многих исходов и многих раскладов.

Бросаем мы, например, кубик. Что по этому поводу говорит теория вероятностей? Можно было бы предположить, что говорит она так: «*Любое из чисел на этом кубике может выпасть с одинаковой вероятностью*».

Такой ответ — это предположение, и это аксиома, которую мы принимаем при рассмотрении раскладов на кубиках. Это не математика. Связь теории вероятностей с жизнью в данном случае идет через кубик, который, как мы верим, объективен.

А на самом деле нет никакого закона, по которому с одинаковой частотой будет выпадать любая сторона (можно представить себе, что какой-нибудь озорной мальчишка подлил свинца в уголок между «6», «2» и «3», чтобы чаще стали выпадать соответствующие стороны. И тогда мы уже не сможем принять постулат о равновероятности выпадений сторон кубика!).



То есть

> теория вероятностей — это математическая модель жизни и способ формально строгого проведения рассуждений в этой модели. За связь модели с реальной жизнью никто из нас не ручается и не отвечает.

И если нам подсунули плохой кубик, наши формулы окажутся неверными и голову на отсечение здесь давать будет нельзя. В отличие от постулатов математики — *абсолютной, настоящей и великой*, где теорема Пифагора верна: была, есть и останется верной до скончания веков в любой вселенной. Поэтому

- теория вероятностей — это мост, ведущий от математики к реальной жизни, и этот мост называется моделью жизни;
- теория вероятностей — один из способов моделирования нашей жизни.

То есть там, где мы не способны физически точно просчитать, как летит кубик, мы *предполагаем*, как он полетит, если только перед нами не виртуоз, умеющий по заказу закручивать игральные кости при броске.

Функциональный анализ

Когда звучит слово «теория», то в большинстве обывательских голов возникает образ какой-нибудь теоремы наподобие теоремы Пифагора... И это верно, так как теорема, касающаяся нашего вопроса, как раз и есть центральная предельная теорема — очень сложная!

Состоит теория вероятностей, или тервер, **из вычисления «страшных» интегралов, иногда многомерных, а иногда бесконечномерных интегралов Ито***. Тервер — это, по сути, **функциональный анализ**: такая наука, которая на мехмате следует после анализа классического.

Обратимся, например, к проведению аукционов. Все расселись и собираются торговаться за некий предмет. И у каждого участника — априорно неизвестная** индивидуальная оценка «красной цены» этого предмета. Каждый рассуждает примерно так: «Я понимаю, что больше 200 не дам, а вот он дал бы, скажем, не больше 10, а вон тот, наверное, не больше 100...» Однако ничего, кроме априорного распределения оценок, никто не знает. И вот сидят участники, выдернутые из этого априорного распределения, как матрешки, и начинают торговаться друг с другом по правилам, которые им продиктованы и заданы организаторами торгов.

Все математические модели аукционов сводятся к системам дифференциальных уравнений сложнейшего вида, которые можно выписать только после того, как ты сформулировал игру с неполной информацией на основе аукциона...

В общем, ад кромешный.

---

* Интеграл Ито́ — это центральное понятие исчисления Ито, математической теории, обобщающей методы математического анализа для применения к случайным процессам. Теория названа в честь создателя, японского математика Киёси Ито.

** Априорно неизвестная величина — это параметр или характеристика, которые неизвестны заранее, но могут быть оценены или вычислены в процессе реальной работы системы по оперативным данным, поступающим от измерительных систем.

И это тот самый функциональный анализ, тот самый тервер в действии. Словом, чтобы просчитать итог взаимодействия на аукционе, тебе нужно знать теорию вероятностей очень глубоко, потому что есть несколько постулатов поведения людей на аукционах. И если бы этих постулатов не было и участники аукциона просто бездумно нажимали на кнопки, словно какая-нибудь случайная бабуля, то не было бы ни теории, ни гениальных случаев «продажи воздуха», как 20 лет назад в Англии мобильным операторам продали «весь воздух».

Это была сделка века, сделка всех времен и народов! Проданы частотные диапазоны мобильным операторам, сумма сделки — 600 фунтов стерлингов на одного англичанина! Даже когда шла торговля земельными участками на Луне, запрашивались меньшие суммы.

Случайностей не бывает

Достоверность предположения *о независимости поведения людей* сомнительна. Что-то в этом не так. Вот представьте: дождливый день в большом городе, например в Москве. Все дороги забиты, город стоит в пробках. В другой же день в том же городе, в такую же погоду и в то же время дороги свободны.

Эта ситуация может говорить нам о том, что иногда миллион москвичей делает тот или иной выбор (сесть сегодня за руль или нет) не вполне «независимо», и все это «не стирается» в законе больших чисел. Похоже, мы моделировали ситуацию неправильно, а другой модели выбора, зависящей, скажем, от пятен на Луне, у нас просто нет. Очевидно, другая какая-то, правильно подобранная модель

будет работать лучше той, которой мы располагаем сегодня. Но другой у нас нет. При этом кто-то по-прежнему рьяно верует в случайность, в независимость выбора. **И это уже не наука, а вера.** Данные убеждают нас в том, что есть некая взаимосвязь между тем, что сидит у всех нас в головах, и в том, что действуют некие общие, одновременно улавливаемые многими сигналы — то одни, то (в другой день, но в тех же условиях) другие.

И это касается не только пробок на дорогах. Да, мы все гоняемся за совпадениями, неожиданными случаями, ведь в жизни столько странных, невероятных совпадений, что мы не склонны думать, будто бы это все «случилось случайно».

«Случайное неслучайно» — этот тезис относится к примерам вроде истории про одну американку*, которая четырежды выиграла в одну из лотерей, где возможность выиграть минимальна в принципе — где-то один на миллиард, а четыре раза подряд — так это уже на миллиард в четвертой степени. Нулевая, можно сказать. А она выиграла! И что, нам теперь считать, что причина в *их* коррупции или все-таки она что-то знает о мире, чего не знаем мы?

Такие случайности подозрительны. Скорее верно **научное предположение**, что **случайности в таких случаях нет**. А те,

---

* Речь о Джоан Гинтер, которая в первый раз выиграла в лотерею $5,4 млн, во второй — $2 млн, в третий раз — $3 млн, в четвертый — $10 млн. Ее выигрыши растянулись на период в 18 лет, начиная с 1993 года. У Гинтер докторская степень по математике, полученная в Стэнфорде, и поговаривали, что для определения выигрышных номеров при покупке билетов оптом она использовала некий алгоритм.

кто все-таки верит, что в этой истории все — чистая случайность, «наматывают сову на глобус» уже со всеми потрохами.

> Начальная теория вероятностей — часть функционального анализа, где мера всего пространства конечна.

В школе такое объяснять сложно.

Выбор и теория вероятностей

Посредством тервера можно дать человеку некоторые навыки, например:

- обращения с кубиками — игральными костями;
- понимания раскладов в преферансе (кстати, раздача по две карты очень важна. Я много играл в преферанс и знаю, что это не просто так: там явно подключаются некие очень трудные законы того, как распределяются карты при перемешивании).

А может ли теория вероятностей помочь человеку сделать выбор? Вот для иллюстрации *задача о разборчивой невесте*. Девушке надо выбрать жениха из тысячи претендентов. Она отсматривает их одного за другим, быстро оценивает и либо посылает каждого следующего куда подальше, либо останавливает на нем свой выбор, и тогда «игра» заканчивается. Взамен того, кто ей не понравился, приводят нового, при этом ушедший больше не вернется. Вопрос: как ей следует действовать?

Если наша невеста будет смотреть всех, то последний может оказаться самым отвратительным. Конечно, она до последнего будет надеяться, что дальше будет лучше, — за это мы

любим девушек, за их нерациональность! Но давайте посмотрим, как будет выбирать жениха рациональная девушка с развитыми способностями к логическому мышлению. И перед нами возникнет строго математическая задача. Очень сложная и красивая.

Для простоты предположим, что невеста может «измерять» претендентов по какому-то единственному (самому предпочтительному для нее) параметру. И теперь на шкале от 0 до 1 нужно расположить 1000 значений и попытаться выбрать максимальное. Девушка знает, что сможет оценить каждого претендента по выбранному параметру адекватно, но не знает, окажется ли *следующий* претендент выше или ниже на шкале и вообще *появится ли* когда-нибудь тот, кто займет место выше предыдущего.

Опуская подробности, которые достаточно сложны, приведем лишь вывод из точного анализа ситуации: оказывается, ей нужно перебрать примерно $\frac{1}{e}$ (как долю в общем числе) мужчин, в нашем случае это $\frac{1000}{e}$, прогоняя их всех прочь (то есть из этих первых невеста никого не выбирает). При этом нужно запомнить, каков был максимальный уровень

претендентов «первой партии», и потом ждать, когда из оставшихся появится тот, кто окажется выше на шкале.

Кто первым окажется выше, того и брать. А если никто не окажется выше, то всё, невеста — «в пролете», придется довольствоваться последним женихом. Можно доказать, что такая стратегия приведет к выбору самого лучшего жениха с максимальной возможной вероятностью — среди всех прочих стратегий выбора!

Парадоксы теории вероятностей

> Парадоксом называется ситуация, которую обычный ум обрабатывает совершенно не так, как математическое вычисление.

Например, к парадоксам тервера можно отнести задачку из серии: «*На поле две команды играют в футбол плюс судья... С какой вероятностью окажется, что у каких-то двух человек на этом поле день рождения в один день?*» **Ответ:** вероятность — более 50 %!

Многие помнят со школьных лет, что если в классе 30 учеников, то вероятность совпадения дней рождения хотя бы у двоих из класса уже достаточно велика, больше половины. Но почему? В этом и состоит парадокс! А набрать случайным образом 70 человек, и чтобы не было совпадений дней рождения, практически невозможно. Даже если число человек в группе — за 40, уже смело можно ставить на то, что хотя бы одно совпадение дней рождения в этой группе есть!

Если только не повезет на 0,001 %... Как-то раз позвали меня выступить перед группой прикольных ребят. Говорю им: «Я мистер волшебник! Спорим, я угадаю, что у двоих

из вас день рождения в один день!» (Я-то знаю, что вероятность для 43 человек — примерно 92–93 %). Поспорили (на что-то большое) и... Не тут-то было, я проиграл! А они: «Не могли вы угадать, нас слишком мало!» Как так?! Даже для 23 футболистов с судьей уже больше 50 %!

Словом, такие задачки — парадокс, который, если ты не математик, трудно понять и представить себе. Но давайте попробуем разобраться.

Какова вероятность того, что у следующего человека дата рождения совпадет с предыдущим? Никакой? Нет, все-таки она есть: 1/365. При этом вероятность, что НЕ совпадет, такая: (1 – 1/365). Подсчитать вероятность несовпадения будет проще, чем вероятность совпадения. Если у двоих людей даты рождения совпали, это хорошо: тогда вероятность «не совпали» мы можем даже не обсуждать. Но допустим, дни рождения у двух людей НЕ совпали, — таким образом мы будто одним выстрелим выбили две мишени — две даты в году (365 дней).

При этом день рождения следующего человека НЕ должен выпасть эти две даты: (1 – 2/365). Постулат независимости говорит нам, что мы должны умножить эту вероятность на предыдущую: (1 – 1/365), и так далее:

$$1\times\left(1-\frac{1}{365}\right)\times\left(1-\frac{2}{365}\right)\times\ldots\times\left(1-\frac{n-1}{365}\right)=$$

$$=\frac{365\times364\times\ldots\times\left(365-n+1\right)}{365^n}=\frac{365!}{365^n\left(365-n\right)!}.$$

Опущу объяснения, но дальше можно уже на глаз прикинуть, когда это станет равно 1/2. Как раз примерно при 23.

Парадокс Монти Холла

Известный **парадокс Монти Холла*** в моем понимании не является парадоксом. Видимо, я слишком много о нем думал.

Итак, представьте, что вы стали участником игры...

Игра

Вам нужно выбрать одну из трех дверей. За двумя находятся козы, а за третьей — главный приз, автомобиль. Вы выбираете одну из дверей. После этого ведущий, который знает, где находится автомобиль, а где козы, открывает одну из оставшихся дверей, за которой находится коза. Затем он спрашивает вас, не желаете ли вы изменить свой выбор и выбрать другую дверь. Стоит ли изменить свой выбор?

Ответ: Да. И это, в общем, очевидно.

Попробуем изложить так, чтобы это стало совсем очевидным.

Предположим, что изначально вы находились перед дверью, за которой была коза, и вам открыли другую дверь, за которой коза, а за третьей дверью — машина. Значит, если в первый раз вы *хотели* открыть дверь, за которой коза, то, меняя впоследствии свой выбор, вы точно получите машину. Осталось определить, с какой вероятностью вначале вы подойдете к той двери, за которой находилась коза, — их

---

* Парадокс Монти Холла — задача из области теории вероятностей, демонстрирующая, что интуиция в условиях неопределенности бывает обманчива. Изначально вероятность угадать скрытый за одной из трех дверей приз составляет лишь 1/3. Когда ведущий открывает дверь, за которой приза нет, шанс игрока на удачу (если он поменяет изначальный выбор) возрастает до 2/3.

же две. При этом изначально вероятность выбрать дверь, за которой коза, у вас больше, и здесь нет никакого парадокса. Потрясающе, насколько это очевидно: вы с вероятностью 2/3 вначале возьметесь за дверь, за которой спрятана коза (и с вероятностью 1/3 — за дверь с призом). Так что, меняя выбор, вы с вероятностью 2/3 получите машину.

Есть, правда, шанс в 1/3, что изначально вы окажетесь перед дверью с машиной.

Парадокс второго ребенка

У мистера Смита два ребенка, причем по крайней мере один из них — мальчик. Какова вероятность того, что и второй — тоже мальчик?

По поводу этого вопроса сломано много копий! И это потому, что здесь не задано исходно вероятностное пространство.

> Задумав применение теории вероятностей к жизни, надо вначале задать точное пространство исходов и вероятности этих исходов.

В парадоксе Монти Холла все очевидно: есть три двери, вероятность верного выбора каждой — по 1/3. В случае парадокса второго ребенка непонятно, что считать исходами.

Если считать, что исходами являются все четыре возможности:

1) мальчик, мальчик;
2) мальчик, девочка;
3) девочка, мальчик;
4) девочка, девочка,

то совершенно ясно, что в трех из них мистер Смит скажет, что один из этих детей — мальчик, и в двух из этих трех исходов второй ребенок, получается, девочка. И лишь в одном исходе второй ребенок — мальчик. То есть при этой постановке вопроса ответ таков: **вероятность того, что второй ребенок — дочка, вдвое выше**.

Но Борис Трушин* довольно убедительно объяснял, что можно этот парадокс трактовать и по-другому. Чтобы не перефразировать Маэстро Бориса, я просто дам ему слово: перейдите по ссылке в сноске на его канал**.

Про случайные числа

Есть такая игра: *«Загадай два числа, и я скажу, которое из них больше»*.

> Что означает загадать два числа? Это значит выбрать случайное событие с предписанным списком вероятностей.

Но не существует вероятностного распределения, равномерного на всей прямой! Математически не существует, и в этом вся суть! Поэтому понятия «случайное вещественное число» не существует! Это по определению неправильная модель!

---

* Борис Трушин — директор учебной части центра онлайн-обучения «Фоксфорд», кандидат физико-математических наук, автор YouTube-канала и популяризатор математики.

** Трушин Б. Задача про лягушек или парадокс мальчика и девочки // Борис Трушин: YouTube-канал. URL: clck.ru/3RpMcG (дата обращения: 15.02.2026).

> Все вероятности вычисляются всегда только в том случае, если есть вероятностное пространство, корректно определенное, со списком исходов и вероятностями, которые суммируются или интегрируется, если их бесконечное количество, к единице.

А в данном случае **интеграл равен бесконечности и никакой модели нет**. Эта модель — про два случайных числа — неверна сама по себе, она не может быть таким образом сформулирована. **Понятия случайного числа не существует!**

О математике

Слышал такой тезис: «*Наука — это и есть ошибки. Как только вы постановите что-либо абсолютным и безошибочным, так сразу и похороните науку, именно в этом месте. Безошибочна лишь истина. Там, где истина, там нет места для науки*».

Фраза эта абсолютно верная, если говорить о естественных науках. Любая естественная наука устроена именно так, как тут было сказано. И ничего окончательного не существует. Но математика не относится к естественным наукам!

> Математика — это наука о наших мыслепостроениях. Наука об идеальных образах.

Это не естественная, а СВЕРХъестественная наука. И в ней **все**, что мы доказали, **останется верным навсегда**.

Например, в игре «Пятнашки» (в первой главе моей книги «Математика для гуманитариев»* она рассмотрена подробно) нельзя вернуть комбинацию фишек в исходное положение, если сперва принудительно вынуть из коробочки и поменять местами две стоящие рядом фишки. Не получится никогда, если вы будете двигать фишки разрешенным правилами способом! Это математически строгое рассуждение, которое устанавливает абсолютную истину. Поменять фишки по правилам — невозможно!

Представим себе, что мой сын собрал из кубиков один большой-большой куб. Я один кубик стащил. Тогда он разложил оставшиеся кубики на полу, и получился огромный квадрат.

Но я сказал ему: «Ну-ка не хитри! Я точно знаю, что ты сейчас откуда-то выудил по крайней мере один дополнительный кубик либо использовал не все имеющиеся кубики!»

А он:

«Папа, ты что, волшебник?! Откуда ты узнал?!»

«Нет, — отвечаю, — я просто математик, сынок. Я ведь забрал у тебя 1 кубик. А дело в том, что $y^2 = x^3 - 1$ не имеет ни одного положительного решения. Невозможно квадрату натурального числа отличаться на 1 в меньшую сторону от куба какого-то другого натурального числа. Да и в бóльшую сторону это возможно только в одном случае: $2^3 = 3^2 - 1$. И если бы ты сейчас не заменил его каким-то

---

* *Савватеев А. В.* Математика для гуманитариев. Живые лекции. М.: Русский фонд содействия образованию и науке, 2022; электронную версию можно скачать с сайта автора https://savvateev.xyz

новым, то куб некоего положительного числа (x^3) был бы на 1 кубик больше квадрата некоего положительного числа (y^2), а так не бывает; такое может быть только в одном случае: $2^3 = 3^2 - 1$.

> Две нетривиальные (большие, чем первая) степени двух натуральных чисел никогда не могут отличаться ровно на единицу, кроме случая 2^3 и 3^2.

Удивительно, но эта гипотеза была доказана лишь в 2002 году — в свете 3 тысяч лет истории математики можно сказать: «только что»! И это доказательство останется с нами навсегда — можно голову класть на отсечение, что доказанное утверждение является верным.

Вообще математика абсолютна, как истина. А любая другая наука — все, что имеет дело с этим грешным миром, — никогда не может претендовать на абсолютную истину, потому что это только модель и собрание неких постулатов в рамках модели. Если ученый говорит, что его постулаты — истина, значит, он верующий — верующий в свои постулаты.

Теория вероятностей — это идеальный пример того, что **в работе с реальностью имеются две стадии**:

1) адекватность модели реальности;

2) математика, которая за этим следует.

И если ваши выводы противоречат наблюдаемой реальности, то это не для реальности плохо и не для математики, которая туда заложена, а просто какие-то из постулатов, заложенных в модель, на самом деле оказались неверными на практике.

Орел и решка? А может, ребро?

Как это ни парадоксально, но вероятность падения монетки на ребро во время игры в орла и решку не так уж и мала: интернет утверждает, что за 1 000 000 подбрасываний подобное произойдет примерно 150 раз, то есть 1 раз в 2 дня, если вы будете подбрасывать монетку в течение 8 часов каждый день. Если же вы хотите, чтобы монетка дважды подряд встала на ребро, придется подбрасывать ее в том же темпе примерно полжизни — лет тридцать пять*.

* Алексей Савватеев против мифов о теории вероятностей / Наука против // НаучДок: YouTube-канал. — https://clck.ru/3S4QY9 (дата обращения: 25.02.2026).

8. ТЕОРИЯ ИГР

Теорию игр можно отнести к области научного знания, однако одновременно она представляет собой определенный образ мыслей, способ мышления. После ознакомления с этой главой станет ясно, что я имею в виду. А пока...

Поехали знакомиться с теорией игр!

Теория игр и манипулирование

Если вы по натуре теоретик-игровик, вам должно быть свойственно частенько с дотошностью «копать» в каком-либо интересном направлении. Почему я с такой экспрессией рассуждаю, например, о том, как теоретико-игровые соображения могут изменить математический прогноз эпидемий, сделанный в соответствии с некой стандартной моделью? Потому что, как тот самый теоретик-игровик, я всегда вижу чью-то волю, которая за кадром пытается изменить целеполагание целого общества или же каких-то конкретных людей.

И в принципе, **это обычная история**: советникам, визирям испокон веков было свойственно тем или иным методом намеренно искажать картину реальности, чтобы вызвать у правителя немедленное желание отреагировать. Но все шаги, предпринятые правителем, будут в действительности отражать интересы лишь того самого визиря, того самого

советника, а не страны, вверенной правителю. И в эту «стратегию визиря» можно, наверное, засунуть порядка 10 % всех мировых конфликтов, известных человечеству.

Другой вид популярного в современном обществе манипулирования — воздействие на огромное количество людей, а не адресно на правителей.

То есть в наши дни, в период почти повсеместной демократии, это неправильное целеполагание с помощью заведомо искаженной картины «вживляется» в сознание людей средствами массовой информации. Публикуется, допустим, статья о том, что в каком-то городе произошло аж пять случаев семейного насилия. Обычный человек, прочитав такое, тут же вскакивает с воплем: «Как плохо! Срочно нужен закон против семейного насилия!»

Именно такой резонанс и есть цель такой статьи!

Ее заказчиком как раз и являются те силы, которые лоббируют закон против семейного насилия. Соберите-ка, мол, быстренько побольше таких случаев!

И нам понятно, что в многомиллионном городе вроде, например, Москвы такого рода происшествий ежедневно случается огромное количество. И журналистам любого сорта, конечно же, найдется, из чего собрать статью.

> Так вот, за любой новостью теоретик-игровик всегда видит ее заказчика! Либо пытается его угадать.

Это **способ работы с информационным потоком**:

1. Вы ловите то, что прилетело в вас с полей интернета.
2. Помимо собственно изучения «контента» прилетевшей новости, вы ищете ее первоисточник.
3. Вы вспоминаете, какими были прочие материалы этого источника.
4. Вы понимаете, кто заказал данную статью.
5. Вы пытаетесь угадать, с какой целью это сделано!

Такой анализ можно назвать хирургией человеческих помыслов. Ведь, основываясь на фактах, вы восстанавливаете истинные помыслы людей и боретесь уже непосредственно с ними. Так что теория игр — очень мощное оружие, и понимание этого совершенно необходимо, если вы сами по сути своей боец.

«Гостья из будущего» — задача про звездолеты

То были вводные слова, а теперь я приведу один пример. Основой выдуманной мною задачи послужил всем известный замечательный советский фильм «Гостья из будущего».

Итак, задача не имеет математической формулировки, математического, строгого решения, которое можно было бы взять, высчитать и к чему-то применить. Она типична для анализа социальных проблем.

Непременно хочу сделать акцент на следующем важном посыле:

> Теория игр не поможет разрешать социальные проблемы и даже предсказать ход развития социума. Лучшее, что она может, — задать набор сценариев развития ситуации и показать, какое равновесие будет в том или ином сценарии.

Итак, фильм сняли в 1984 году, и он о событиях, которые произойдут через 100 лет.

Пролог: задача по мотивам «Гостьи из будущего»

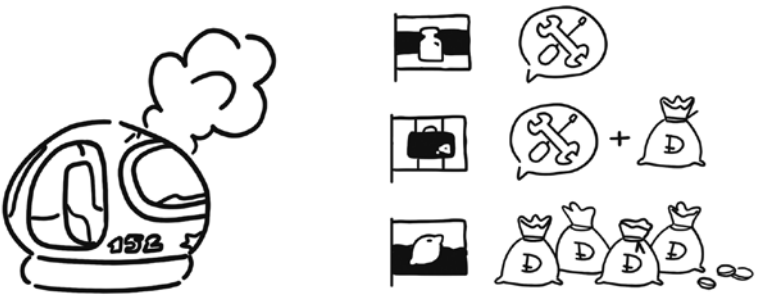
2084 год. Во всем мире люди перемещаются на малюсеньких звездолетах по принципу каршеринга: сел, проехал, оставил, ушел.

Рычаги управления звездолетов часто ломаются (по причине частых погонь), ремонт обходится в 200 нефтяных динаров. Это не очень большая сумма, но все же ощутимая.

И в этом придуманном мире будущего есть три империи: Гирляндия, Лимония и Чемодания.

Они имплементируют разные правила эксплуатации звездолетов:

1. *Гирляндия*: поломка рычагов не наказуема, только надо обязательно сразу сообщить о ней в ремонтное бюро.



Тебе скажут: «Спасибо. Но больше постарайтесь ничего не ломать». Приедет ремонтная бригада, а 200 динаров возьмут из бюджета государства.

2. *Чемодания*: гражданин обязан не только сообщить о поломке, но и заплатить 200 динаров из своего кармана.
3. *Лимония*: поломка рычагов карается жестко — штраф 2000 динаров, то есть в 10 раз больше стоимости ремонта (весьма значительная сумма).

Что скажет теоретик-игровик?

1. В Гирляндии, где поломка рычагов не наказуема, их «ПЕРЕиспользуют», то есть используют слишком неаккуратно с точки зрения социального оптимума.

   С позиции экономиста, мыслящего категориями теории игр, социальный оптимум не значит «относиться к рычагам так, чтобы они не ломались», нет! *Оптимально относиться к рычагам* — это значит приравнивать выгоду наличия рычагов (экономию времени и средств за счет быстрой езды) к ожидаемой цене поломки. То есть едешь слишком быстро — будешь часто ломать рычаги. А времени выгадаешь чуть-чуть. Однако слишком медленная езда

убивает так много времени, что может оказаться выгоднее оплатить ремонт (см. подход Чемодании).

2. В Чемодании в этом плане все устроено наиболее правильно, так как все издержки, случающиеся вследствие поломки, ложатся на виновника поломки. Человек, оплачивающий поломку, сам принимает то или иное решение: выбирает для себя ту скорость, которая будет для него оптимальна и выгодна.

   Кажется, что правила, действующие в Чемодании, — это оптимальный вариант, но так будет лишь при наличии взаимного доверия между гражданами и государством. Без взаимного доверия, без действия так называемого социального договора граждане будут покидать место поломки: «Пусть 200 динаров государство заплатит!» Иными словами, должно быть достигнуто хорошее равновесие Нэша* (о нем — чуть позже).

3. Подход Лимонии вызывает негативное отношение людей к государству. За небольшую поломку кара чересчур суровая, размышляют они, наверняка оставшиеся 1800 динаров чиновники кладут себе в карман, мы государству не доверяем! Факты поломки люди начнут

---

* Равновесие Нэша — набор стратегий в игре для двух и более игроков, когда ни один участник не может изменить свою стратегию для увеличения собственного выигрыша, если другие участники своих стратегий не меняют. То есть «если все действуют так, как сказано, то и мне выгодно действовать так, как сказано». Термин назван в честь математика Джона Нэша, доказавшего существование такого равновесия в смешанных стратегиях в любой конечной игре. Равновесие Нэша широко используется в экономике, политологии и других общественных науках для анализа поведения отдельных людей или групп в конкурентных ситуациях.

скрывать: сломал и побежал! Такова логика отсутствия общественного договора. Наверняка потом появятся камеры, полицейский контроль и все такое. Выстраивается полицейское государство, где «верх» подавляет «низ». *Примеры*: современные Китай, Сингапур. (Впрочем, не берусь осуждать государственные устои чужих стран — кто я такой, чтобы так поступать?)

Определение теории игр

Отталкиваясь от нашего примера, перейдем к определению теории игр. Это тот редкий случай, когда определение можно дать одной строкой.

> Теорией игр называется анализ конфликтов на основе математических моделей.

То есть, анализируя конфликты с точки зрения психологии, вы занимаетесь примерно тем же, чем мы, математики, но с другой точки зрения, и приходите к другим, неизвестным нам, выводам о поведении людей.

Математики же составляют уравнения, задавая — весьма узко — человеку его способ принятия решения.

* * *

Не беря в расчет теории, связанные с альтернативным подходом к оценке выигрышей и проигрышей, отметим, что

> почти все модели теории игр основаны на брутальной максимизации каждым игроком некой приписываемой ему исследователем функции выигрыша, образно говоря, вы принимаете человека за некую «машину максимизации».

При этом, ища равновесие, вы должны для каждого игрока:

- определить множество его возможностей (или, как говорят теоретики-игровики, «множество возможных стратегий»);
- выяснить, на какую из стратегий (или на целый их ряд) выйдет этот человек как «машина максимизации», если он верно угадал стратегии остальных игроков. Если игрок выходит на целый набор опций-стратегий, то с его точки зрения возможные опции (в смысле получаемого выигрыша) совершенно равнозначны, и для него они лучше всех остальных его стратегий.

Пока умолчим о ситуации использования смешанных стратегий — это чтобы в конец не запутать читателя! Скажем лишь, что смешанные стратегии могут возникать только в случае множественного оптимального набора.

В процессе «нащупывания» равновесия люди своими действиями меняют друг для друга расположение стратегий во множествах возможностей каждого из игроков относительно упорядочения «верх — низ» (то есть я меняю вашу оценку событий — какое лучше, а какое хуже для вас, а вы своими действиями меняете мою оценку).

> Выходит, что теория игр — это математический способ моделирования конфликтов, в которых каждый игрок своими действиями влияет на выигрыши или проигрыши остальных игроков.

Но начинается моделирование с того, что я, исследователь, имплементировал (предписал, назначил) каждому игроку его собственную функцию выигрыша и сказал, что каждый игрок принимает решения путем максимизации этой функции!

Человек, готовый выбирать решение наобум, «неописуем» — не может быть описан с позиции теории игр: его поведение не может быть предсказано. Честный вывод здесь должен быть таков: «*Мы не знаем, из каких соображений в данной ситуации такой человек принимает решения. И мы не можем спрогнозировать, что произойдет, окажись он вовлеченным в то или иное взаимодействие*».

Это граница теории игр — третий посыл, который я хочу сделать.

> У теории игр абсолютно четкие границы применимости. И если ваша модель ведет к некоему абсурду, это значит, что люди, которым вы предписали ту или иную модель поведения, на самом деле ведут себя иначе.

На семинарах, которые я часто провожу для бизнеса, мы, например, знакомимся с методами теории игр, и у людей часто срабатывают завышенные ожидания. А на самом деле в любой прогноз, в предлагаемое «дерево возможностей» может вклиниться любой неучтенный фактор (человек или непредвиденное событие), на который взгляд со стороны математики уж никак не повлияет.

Скажем скромно: *теория игр иногда и только отчасти может помочь человеку что-либо предвидеть.*

Попытки разработки моделей голосования, к примеру, — полная ерунда, и все, кто этим занимается, прекрасно об этом знают. Собираемые данные гораздо полезнее и интереснее, чем выводы, которые специалисты пытаются посредством этих моделей получить. Тем не менее в этом направлении тоже следует работать, как и во многих прочих (просто для накопления материала и для улучшения общего понимания).

Два самых явных примера серьезного, экономически выгодного успеха в приложении теории игр на практике — это теория аукционов и транспортное моделирование. Причина успеха в обоих случаях — четкое понимание математиками целей «игроков», то есть участников взаимодействия.

Аукцион: цель любого игрока (участника торга) — *получить предмет торга за возможно меньшие деньги (и отказаться от покупки в том случае, если цена предмета превышает некоторый предел, различный для разных участников торга)*. Это нормальная, понятная модель поведения с позиции любого бизнесмена. Выполнив соответствующую «математическую работу», ученые получили высокую эффективность моделей проведения торгов.

Транспорт: цель, как правило, — одна и та же у всех, кто намерен воспользоваться любым транспортом: *как можно скорее попасть на работу*. Как бы мы ни относились к автотранспорту (в среднем — по модулю личных предпочтений), верно, что *чем больше пробок, тем ниже вероятность того, что человек предпочтет сесть за руль, узнав об этих пробках. И тем выше вероятность того, что он воспользуется общественным транспортом. Уже этого наблюдения достаточно для отлаженной работы моделей транспортных потоков*.

Теория игр не очень требовательна! Если ее постулаты хотя бы немного совпадут с нашими вводными, мы уже получим хороший итог: сможем, к примеру, выявлять тенденции рассуждений людей.

Вехи становления теории игр

- Курно́ (1838) — анализ рынка зерна.
- Це́рмело, Кун (начиная с 1910 г.) — решение с конца, «думай за других».
- Модель Хоте́ллинга (1929) и ее развитие в модели Даунса (1957).
- Аукционы (на всем протяжении мировой истории, революционный прорыв — Ма́йерсон, 1980 и далее).
- Томас Саа́ти — теория ядерного сдерживания.

Курно*. Равновесие по Нэшу

Началось все *в 1838 году* (но есть версия, что гораздо раньше и совсем в других странах). *Курно анализировал рынок зерна*. Как он это делал?

В 1838 году Курно сформулировал понятие равновесия. В будущем оно получит название «Равновесие по Нэшу» (Курно по сути искал и находил именно его).

> Когда урожай зерна большой — цена очень низкая. Если зерна мало — цена высокая.

Допустим, едет французский фермер на рынок со своим зерном. Другие продавцы уже там. Фермер думает: «Сколько привезти? Привезу слишком много — цена может упасть настолько, что мне не будет никакой выгоды».

---

* Антуан Огюстен Курно (1801–1877) — французский экономист, философ и математик, автор экономической модели рыночной конкуренции.

Фермер подсчитывает оптимальный отклик, то есть такое количество зерна, которое, будучи привезенным им, приводит к максимально возможной прибыли. А как он может найти прибыль?

Он говорит: «Я отправлю вперед своих работников, и они узнают, сколько зерна везут на рынок все мои конкуренты». Таким образом он выведает значения (q_2, q_3...) всех привезенных другими фермерами объемов зерна (а объем его собственного зерна мы обозначим просто как q). Теперь он сможет узнать цену (p), которая зависит известным образом от суммарного количества привезенного зерна, и эта цена для него окажется функцией от объема его собственного привезенного зерна (q), ибо на объемы зерна конкурентов он повлиять не может.

«И, — говорит фермер, — я умножаю количество моего зерна (q) на вот эту функцию цены. Когда количество моего зерна ползет вверх, цена падает вниз (при этом произведение может в принципе и расти, и падать). И я нахожу точку, где оно, произведение, будет самым большим. То есть я максимизирую эту функцию по параметру q (сколько зерна я сам привез на рынок)».

Привез чуть-чуть — заработал мало, даже если цена была высокой.

Привез слишком много — цена низкая, и выручка опять же будет маленькой.

Где-то должен быть оптимум. Но этот оптимум зависит от всех этих q_2, q_3, q_4, то есть от объемов зерна, привезенных другими фермерами (то есть продавцами).

Так вот, Курно взял и сформулировал **понятие равновесия**. Равновесием является (или не является) весь набор объемов привезенного зерна! Не объем зерна, привезенного каким-то одним фермером, а весь вектор, или весь набор объемов. В данном случае мы имеем дело с четырьмя величинами — количеством зерна в каждой из четырех повозок. **Суть понятия равновесия состоит в том, что если наш фермер правильно угадал все эти величины, то ему ничего не нужно менять: выбросив из своей повозки лишний, как ему кажется, товар, он снизит свою прибыль.** И добавив еще товара, тоже снизит! То количество, которое «подсмотрели» у него в повозке его конкуренты, и является оптимальным для него объемом зерна на продажу! И так будет для каждого из фермеров! Вот в чем суть концепции равновесия по Нэшу.

И тогда же стало ясно, что равновесие неэффективно с точки зрения взаимодействия всех продавцов друг с другом. Это означает, что **если бы все фермеры собрались у входа на рынок, вычислили функцию цены в зависимости от общего объема зерна на продажу по предыдущим годам да дружно решили бы выложить из всех повозок по некоторому количеству мешков и не продавать его ради всеобщей выгоды, то каждому из них стало бы однозначно лучше, — прибыль каждого фермера от такого сговора увеличилась бы**. Однако проблема именно в том, что в наилучшем (монопольном!)

решении у каждого из них есть стимул обмануть остальных фермеров и продать на рынке «из-под полы» какое-то *дополнительное* количество зерна! Примерно так и были открыты все базовые факты про монополию, поведение конкурентов в картеле, обман и стимулы к оппортунистическому поведению. Шел 1838 год...

Цермело*, Кун** и решение математических игр

В фокусе нашего внимания в этом разделе будут математические игры (это строго научный термин!), в которых играют несколько игроков, ходы осуществляются в строгой последовательности один за другим, и в конце концов однозначно определяется победитель либо фиксируется ничья (возможно и обобщение — ситуация с несколькими исходами, упорядоченными строго противоположным образом с точки зрения наших двух игроков). Откройте любую книгу по занимательной математике и загляните в раздел «Игры и стратегии» — вы там увидите множество примеров таких игр. Шахматы, шашки в целом тоже подходят под это определение.

В идеале в таких играх во всех мыслимых финальных позициях игры можно определить, кто выиграл, кто проиграл,

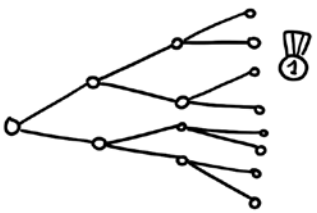
---

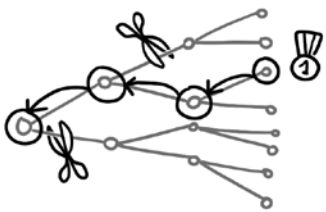
* Эрнст Фридрих Фердинанд Цермело (1871–1953) — немецкий математик, внесший значительный вклад в теорию множеств и создание аксиоматических оснований математики. Один из авторов идеи математической теории конфликта интересов.

** Гарольд Уильям Кун (1925–2014) — американский математик, специалист по теории игр.

а в более общем смысле — кто какие выигрыши получил. Чтобы строить прогнозы, надо анализировать игру каждого конкретного игрока «с конца».

1. Сначала рисуем ветку событий, определяя: «в этих точках игроку будет “плохо”, а вот в этой точке ему будет “хорошо”, и он поэтому сделает вот такой ход, чтобы ему стало хорошо...» Всю ветку событий можно «укоротить», сразу обозначив результат: «игрок сделал вот такой ход». Это будет считаться результатом не только для данного игрока, но и для всех участников, ведь он своим ходом повлиял на выигрыши остальных.
2. Потом рассматриваем каждую ветку событий, обрезая их постепенно «снизу вверх». В итоге мы сможем понять, *что произойдет в начале* (каким **должен быть** начальный ход игрока, который ходит первым). В частности, если бы компьютер смог перебрать все 10^{120} шахматных позиций с конца к началу, он ответил бы на вопрос, кто выиграет при «правильной» игре — белые или черные. Выиграют ли белые, потому что они начинали; или выиграют черные, потому что ходили вторыми; а может, получится ничья вне зависимости от того, чей ход был первым. На данный момент, правда, никакой компьютер таких подсчетов сделать не может.





Модель Хотеллинга* и пример конкуренции продавцов мороженого

Гарольд Хотеллинг

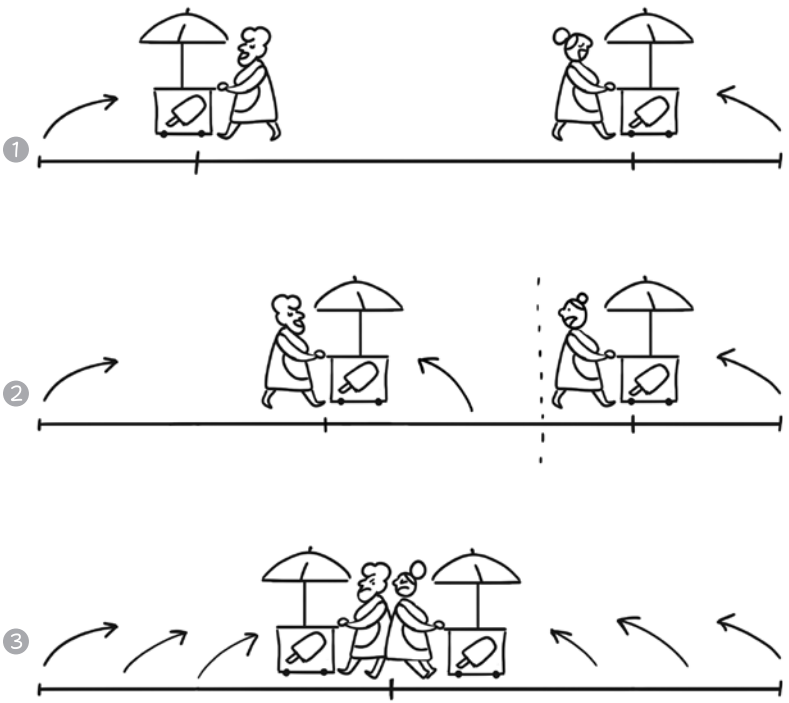
Представьте себе такую ситуацию: юг, море, жара, июль. Пляж вытянулся вдоль моря на большое расстояние, всюду «плотная упаковка» отдыхающих. Две продавщицы с тележками продают мороженое. Цены на мороженое фиксированы, продавщицы не могут их менять, — для того чтобы больше заработать, им нужно просто больше продать, и они пытаются «забраться на территорию друг друга».

Что должно происходить, если мы ищем равновесное расположение продавщиц? Где бы они ни находились изначально, ясно, что если их тележки расположены в разных местах, то та, что слева, собирает доход с левой части пляжа, а та, что справа, — с правой. Однако в таком случае каждой из них будет выгодно потихоньку начать смещаться в сторону коллеги: так, не теряя «своих» покупателей, она приобретает новых, находящихся между нею и конкуренткой. К чему это

---

* Гарольд Хотеллинг (1895–1973) — американский экономист и статистик. Автор методов определения оптимальных квот на добычу невозобновляемых природных ресурсов и цены естественных монополистов в терминах предельных издержек; создал модель линейного города, где принцип максимизации прибыли заставляет конкурентов располагаться близко друг к другу.

приведет? Несложно показать, что единственное равновесие Нэша в данной ситуации — это когда обе продавщицы встанут посередине линии пляжа попами друг к другу и будут продавать мороженое на разные стороны. (Сами определите, почему нахождение в одной точке, не являющейся центром пляжа, не может претендовать на равновесный итог их взаимодействия!)



Это и есть **равновесие по Нэшу** — совершенно неэффективное с точки зрения социума. Можно оставить в центре одну

мороженщицу — результат будет тем же (по крайней мере, в нашей теоретико-игровой модели пляжа).

В политике пытались эту же модель применить: мол, две противоборствующие партии и так могут рассчитывать на свой ультраэлекторат, и, чтобы «захватить» часть избирателей соперника, надо смещаться к центру*. В конце концов обе партии становятся похожими друг на друга по программам как две капли воды и различаются только лозунгами и флагами.

> **Но на самом деле это не так!** Этот великий парадокс пытаются каким-то образом изучать, но, по моему личному мнению, здесь теория игр не применима в принципе. Выборы — ситуация совсем не теоретико-игровая. Политические модели, в отличие от транспортных, работают плохо. А все потому, что мы неправильно понимаем и формулируем, почему люди приходят голосовать; следовательно, мы также искажаем цели тех, кто конкурирует за голоса избирателей. Из-за этого мы не можем создать реалистичную модель.

Аукционы

Как я говорил выше, здесь действительно произошел большой прорыв. Теория игр позволила разработать совершенно неожиданные и доселе неведомые форматы. *Аукцион второй*

---

* Центризм — политическая позиция, заключающаяся в балансировании между общественным равенством и общественной иерархией и противостоянии политическим изменениям — как влево, так и вправо.

цены стал общепризнанным — как в интернете, так и при других вариантах проведения, потому что у его решения есть потрясающие стратегические свойства!

Оказывается, что

> если после подведения итогов аукциона победителю (иными словами, «тому, кто был готов купить лот за максимальную цену») назначить к оплате не цену, предложенную лично им, а вторую по величине из тех, что написали участники, то это стимулирует участников называть ровно столько, сколько они в действительности готовы максимально заплатить.

Этот механизм был отмечен Нобелевской премией.

Роджер Брюс Майерсон

А далее *Роджер Майерсон** напридумывал в области аукционов еще много интересного. Но аукционы — это не только теория! В 1999 году в Великобритании был организован аукцион «по продаже воздуха»: на торги были выставлены права на использование диапазонов частот мобильного спектра. Государство суммарно выручило более 600 фунтов стерлингов на одного британца. Эта невообразимо крупная сумма была получена за одну сделку. Ну а теория игр показала миру, что она все-таки на что-то способна!

Теория ядерного сдерживания

Отмечу: теория довольно спорная. Утверждается, что Томас Саати** совместно с нашими теоретиками-игровиками разработал в середине XX века некую модель ядерного сдерживания, которая якобы предотвратила третью мировую войну и вообще конец всего. Но тут скорее мы себе льстим.

---

* Роджер Брюс Майерсон (1951) — американский экономист, лауреат Нобелевской премии по экономике 2007 года за участие в создании основ теории оптимальных механизмов.

** Томас Саати (1926–2017) — автор «Метода анализа иерархий» (технологии принятия решений на основе математических расчетов и использования метода попарных сравнений).

А вот ключевая роль теории игр в области проведения аукционов и организации транспорта, повторюсь, никакая не лесть, а объективная правда.

Является ли игра «Каркассон» теоретико-игровой?

«Каркассон» — это великая игровая модель, для иллюстрации теории игр отлично применимая. При этом никогда нельзя сказать: «Этот игрок гениально играет в “Каркассон”», ведь все зависит от того, принимают ли тебя (твою игру) остальные участники.

Например, есть игрок в «Каркассон», он мастер — великолепно «отжимает» у других поля! Но, скорее всего, именно по этой причине с ним никто не захочет кооперироваться

по городам — из-за того, что поля будут его. Придется нашему гению корректировать линию поведения.

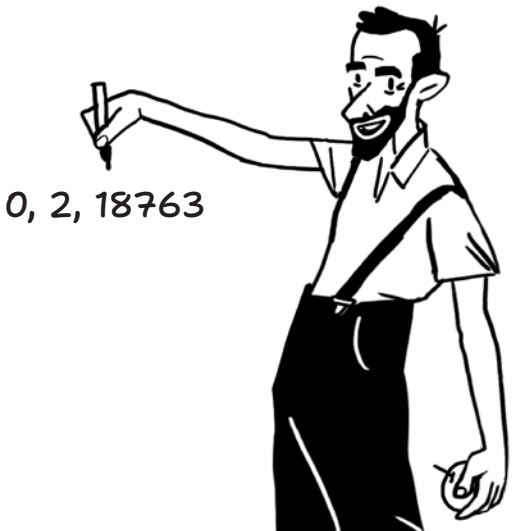
Так что очень многое переплетается в этой игре: умение договариваться, уговаривать других делать ходы, когда им этого не нужно, и т. д.

Очень теоретико-игровая игра!

Можно ли с помощью теории игр учесть возможность появления ультрапартии в случае сдвига к центризму?

Вероятный ответ: «Да». *Возможность* как таковая есть всегда, но *как ее предсказать*?

Допустим, я и мои товарищи пытаемся создать партию (много народу — один центр). Мы в центре и знаем: за нами идут миллионы людей. Но это маленькие разрозненные группки, разбросанные по всей стране. Ситуация лучше всего описывается принципом «разделяй и властвуй».



В какой момент из этого хаоса мнений и воззрений может зародиться новая партия, мы не знаем, и поэтому *предсказать момент срабатывания такой возможности не можем*.

Давайте сыграем

Когда на моих лекциях много слушателей, я предлагаю сыграть в такую игру:

Напишите на бумажке любое целое неотрицательное число из ряда: 0, 1, 2, 3, ... (любое целое неотрицательное число). Выигрывает тот, чье число будет:

а) уникальным;

б) наименьшим среди таковых.

Удивительно, но никогда не бывало, чтобы никто не победил! Ведь почему бы не предположить, что половина зала назовет 0, а другая половина — 1. И все! Но всегда (и это вопрос к психологам!) найдется тот, кто стремится записать какое-нибудь уникальное число (к примеру, шестизначное). При этом выигрывают не такие игроки! Чаще всего выигрывает кто-то, назвавший совсем маленькое число, например 2, которое почему-то никто больше не назвал. Вот и получается, что сыграло огромное количество народа, а выиграло число 2.

В этом «парадоксе победы маленьких чисел» кроются некие парадоксы нашего мышления! Но за этим не к нам, математикам. За этим к психологам. К нам — вот за чем: *мы можем найти в этой игре все равновесия по Нэшу, то*

есть ситуации, которые останутся стабильными, даже если игроки прочитали мысли друг друга. Равновесий в этой игре огромное количество, и их можно все описать. Попробуете сами?

Теория игр: личный опыт, наблюдения и практика

Как теория игр помогала автору в жизненных ситуациях

Я провел 4–5 тысяч выездных лекций более чем в 400 городах и селах России — побывал почти во всех регионах нашей страны. И у меня постоянно то там, то тут случаются те или иные казусы! Некоторыми из них очень хочется поделиться с читателями.

Сюжет 1. Предвидеть отсутствие риска

Вопреки скупердяйской идее, что если книгу можно скачать в интернете*, то в бумажном виде ее никто не покупает, книга «Математика для гуманитариев» расходится очень быстро. Сейчас ее невозможно достать вовсе, а несколько лет назад (когда произошла описываемая история) мне приходилось ее доставлять по разным адресам.

И вот отправляюсь я как-то на машине с человеком, который мне помогает, в одно учреждение, где у меня лежала огромная

---

* Электронную версию книги «Математика для гуманитариев» можно бесплатно скачать на сайте автора https://savvateev.xyz/

партия книг. Приезжаем мы к 7 утра, ну а там у охранников пересменка: один ушел раньше, чем пришел другой. И все закрыто. «Ладно, — говорю, — не беда, сейчас разберемся». Влезаю через окно и все книги выношу.

У водителя — глаза на лоб!

«Ты что творишь?! Это ж уголовщина!»

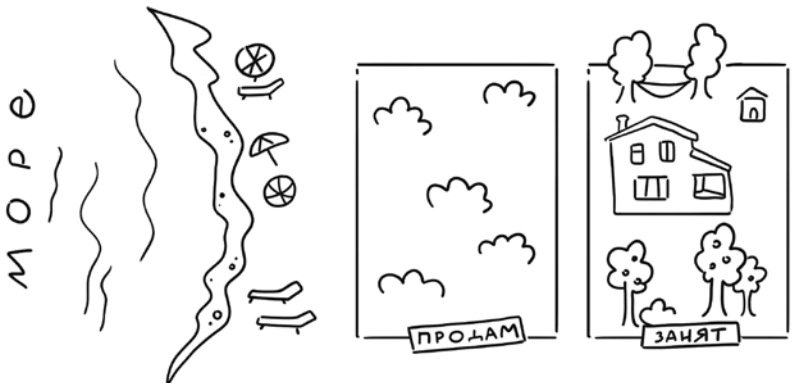
Вопрос: что должно произойти, чтоб это *стало* уголовщиной?

Ждать нам было нельзя — еще немного, и на трассе соберется здоровенная пробка. Ну а заступивший на смену охранник, конечно, быстро обнаружил, что книг нет. Так что же подсказывает теория игр? Почему я не боялся того, что охранник напишет заявление в полицию и я (гипотетически) пострадаю?

Ответ: заявление не подадут, потому что самими охранниками был нарушен режим охраны! Кто может написать заявление? Только охранник. Но тогда его уволят, потому что он отсутствовал на своем месте! А я как теоретик-игровик понимаю его поведение: он придет, обнаружит пропажу: «Блин!..» Но он же не идиот, чтобы самому себя сдавать. Потому охранник никому ничего не скажет. Таков был прогноз теоретика-игровика! И прогноз сбылся! А уж потом мы с охранником встретились, пожали друг другу руки и... подмигнули друг другу!

Сюжет 2. Заморозить продажу

Вот отличная зарисовка из жизни, которая, правда, не осуществилась так, как поведано ниже.



На рисунке «море» — это «священный Байкал». Там, где слово «Занят», находится наша дача.

Какое-то время назад между дачей и морем пустовал участок: владелец, уверенный, что место классное и земля стоит дорого, все пытался продать его по какой-то непомерной цене. Не получалось. Но затем поползли слухи, что покупателю с «живыми» деньгами он готов продать гораздо дешевле.

Сидим мы с женой расстроенные: «Через год у нас под носом начнется стройка... Шум... Конец спокойной жизни».

Я: «А вот был бы я сволочью — сделал бы так, чтобы он не продал ничего. Я знаю, как можно поступить».

Но я не сволочь, поэтому ничего не сделал.

Вопрос: что можно было бы сделать, не нарушая никаких законов и не прибегая к прямому черному пиару?

> Теория игр — вдохновляющая штука! Она открывает человеку те опции его сознания, о которых он и помыслить не мог!

Возможные действия. Звоним продавцу: «Отличный участок! Полтора миллиона? Так мало? Как круто! Отлично, я пошел собирать деньги!» А через месяц — звонок другим голосом: «Сколько?» — «А его уж покупают». — «Ай, как жа-аль! А то я бы взял!..»

И так продолжать можно было бы много лет. Ведь нам-то не нужен участок: нам надо было, чтобы никто не развел там строительство. Но я не сволочь, и я не смог так поступить!

Однако Господь воздал за нашу порядочность: когда сосед скончался, мы были первыми, кому позвонили его родственники с предложением купить участок по нормальной цене.

Вывод:

> Рыночная цена не всегда существует. В случаях, когда на продажу выставляется уникальный товар, более актуальными являются модели аукциона либо прямых торгов.

Сюжет 3. Обеспечить покой

Немало моих приколов связано с *поездами*. Вот, например:

А. В. Савватеев выступает в 2019 году
в Великом Новгороде и возвращается в Москву.

После выступления в Великом Новгороде возвращаюсь в Москву, при этом прошу организаторов взять мне билет до Владимира (на поезд «Великий Новгород — Нижний Новгород», идущий через Москву).

Вопрос: в чем смысл такой просьбы, если выходить я собираюсь все-таки в Москве? Какова моя цель?

Ответ: я не хочу, чтобы проводница будила меня заранее, мне удобнее по-солдатски: проснулся — встал — покинул поезд. Будь мой билет до Москвы, по инструкции меня бы стали тормошить за полтора часа до подъезда к столице, то есть в 4 утра. А так меня станут будить часов в 6, но я ставлю будильник на 5:25 и в 5:30 выхожу с рюкзаком в Москве.

Типичное решение теоретика-игровика! Вы меняете поведение другого человека (*меня должны разбудить*) тем, что берете билет до другой станции (*меня НЕ будят*). Помните: варианты повлиять на действия другого человека часто неочевидны, их надо придумывать и воплощать в жизнь!

Сюжет 4. Комфорт на непопулярных маршрутах

Поезда. На непопулярных железнодорожных маршрутах и не в сезон нижние места частенько пустуют, поскольку верхние полки значительно дешевле. Я покупаю верхнее место, используя бóльшую вероятность, что «нижний» пассажир не явится и я поеду с комфортом, словно с собственным кабинетом: на нижней полке буду работать за компьютером, а на верхней — спать.

Самолеты. Когда я понимаю, что самолет будет полупустой, вот что делаю. Бронирую центральное место в ряду. Возьмите на заметку: мало находится людей, кто хочет брать места рядом с чудаком, который забронировал центр. Что в результате? Весь ряд в вашем распоряжении — отдыхайте себе спокойно! «Плацкарт» — так это теперь называют борт-проводники. К сожалению, по понятным причинам в последнее время полупустых самолетов уже не бывает.

Сюжет 5. Получить добавку

Ужинают брат и сестра — Юра и Света. Света — старшая. Девочка уже съела свою порцию вермишели и хочет еще, заглядывает в тарелку брата: «Ты больше не хочешь?» —«Ну, не зна-а-ю...» — явно мальчишка не торопится делиться.

И что делает Света? Ставит на стол... тортик! Естественно, четырехлетний Юра тут же забывает про вермишель: «Мама, тортик! Я хочу тортик!» — «А вермишель?..» — «Не! Все! Не буду!»

Вот вам и дочь теоретика-игровика! Она просчитала реакцию брата и сподвигла его поступить нужным ей образом. Страшные люди эти игровики...

Подведем итог....

Все приведенные выше сюжеты имеют теоретико-игровую основу, которую можно сформулировать так:

> Если хотите менять поведение окружающих нужным вам образом, первым делом выясните, а что на самом деле всем этим людям нужно.

Транспортное моделирование

Парадокс Бра́еса на марше

В Восточном округе Москвы есть Метрогородок — микрорайон, «вторгающийся» в парк «Лосиный остров» (самый большой городской парк в Европе; практически это сплошной лес, особенно за МКАДом). Я вырос в этом микрорайоне,

закончил там 7 классов средней школы (до поступления и перехода в 57-ю школу).

Еще в далекие девяностые я обнаружил интересный эффект, который потом мы изучали в Российской Экономической Школе под специальным названием: *парадокс Браеса*.

Большой поток машин, въезжающих в Москву по Щёлковскому шоссе (в народе — «Щелчок»), дробится на несколько полноводных «речушек» в районе станции метро «Преображенская площадь». Одна из «речушек» устремляется к ВДНХ. Быстро добраться до ВДНХ, минуя все светофоры на основном пути, можно было по узенькой необорудованной полупроселочной дороге, соединяющей Щёлковское шоссе и Метрогородок (и далее от нас через лес по дороге, на которой в 1990-е годы не было ни одного светофора!).

Необорудованной и полупроселочной эта дорога была в начале 1990-х. Ее качество и многочисленные ямы, грозящие поломкой машины, не позволяли разогнаться и до 20–30 километров в час. Поэтому в то время мало кто пользовался такой «срезалкой»; бóльшая часть машин двигалась со Щелчка к ВДНХ через Преображенскую развязку, минуя Метрогородок.

Затем дорогу, ведущую со Щелчка к нам в Метрогородок, заасфальтировали и отремонтировали.

И что же произошло? Машины, идущие по Щёлковскому шоссе, частично пошли по новому пути через лес, и на нашей восхитительной лесной дороге, которую ремонт и расширение не коснулись, тотчас же образовалась пробка перед ВДНХ.

Так сложилось новое транспортное равновесие...

> Транспортное равновесие заключается в том, что время перемещения по любому из реально используемых маршрутов из пункта А в пункт Б должно быть одинаковым!

Поясним это на примере двух маршрутов. Если на втором маршруте пробка маленькая и время в пути меньше, чем на первом, — водители с первой дороги поворачивают туда. Нагрузка перераспределяется. Время в пути по первой дороге становится чуть меньше, нежели было до того, а на втором пути — чуть больше. Этот процесс «перетекания» между маршрутами продолжается до тех пор, пока время в пути на обоих возможных маршрутах не станет одинаковым. Тогда наступит («сложится») транспортное равновесие.

В нашей ситуации отремонтированная дорога узкая, и с небольшим уменьшением числа машин время в пути через Преображенскую площадь почти не меняется, — все дело в светофорах (так было в девяностые годы, по крайней мере). Поэтому переток машин продолжился до тех пор, пока время следования по короткому пути просто не выросло до времени следования по длинному. Реальной экономии не ощутил никто!

Более того, в новом равновесии с отремонтированной дорогой жители Метрогородка очень сильно проиграли: раньше у них была пустая дорога на ВДНХ через лес, а теперь она вечно забита машинами!

Подобная ситуация (когда от ремонта старых дорог либо постройки новых никто не выиграл, а часть участников дорожного движения так и вовсе проиграла), называется **парадоксом Брайеса***.

Видите, как все в теории игр на самом деле неочевидно: казалось бы, построили дорогу, всем должно стать лучше. Или хотя бы некоторым. А вот и не обязательно!

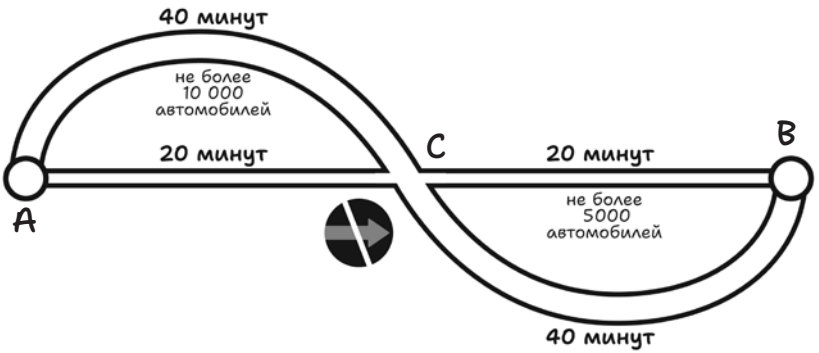
На основании этого парадокса **Юрий Евгеньевич Нестеров**** придумал некоторую транспортную сеть. Она представлена ниже. Пример можно назвать «Парадокс Брайеса наизнанку».

---

* Парадокс, приписываемый немецкому математику Дитриху Брайесу: «Добавление дополнительных мощностей в сеть при условии, что двигающиеся по сети сущности сами выбирают свой маршрут, может снизить общую производительность». Это происходит потому, что равновесие по Нэшу для таких систем не обязательно оптимально. Парадокс можно рассмотреть на примере дорожной сети. Если каждый водитель будет выбирать маршрут, который выглядит наиболее благоприятным для него, не только суммарное время нахождения в пути не обязательно будет минимальным, но и, хуже того, может статься, как в примере выше, что ни один участник не выиграет, а часть участников окажется в проигрыше!

** Нестеров Юрий Евгеньевич (род. 1956) — советский и бельгийский математик, специалист по нелинейному программированию, выпуклой оптимизации, численным методам оптимизации.

Парадокс Брайеса наизнанку



$[A \rightarrow B]$ = 8000 автомобилей — пробки по 20 минут!
→ запрет на прямое движение → экономия для всех 20 минут!

Условия задачи:

- Машины движутся из пункта *A* в пункт *B*, посередине пути находится пункт *C*. Транспортный поток из пункта *A* в пункт *B* составляет 8000 автомобилей в час. Время в пути на каждом из двух сегментов — от *A* до *C* и от *C* до *B* — составляет 20 минут, если пробок нет.
- Весь поток целиком на прямой от *A* до *B* вместиться не может: слишком узкая дорога, поэтому были построены две объездные трассы: одна от *A* до *C*, другая — от *C* до *B*. Каждая из них очень широкая, без ограничений на поток, но длинная, и время проезда по каждой из них составляет 40 минут, независимо от их загруженности. Короткие дороги не могут пропустить более 5000 машин в час — все, что сверх того, просто встает в пробку перед конечным пунктом каждого из двух сегментов. К северу

и к югу от пункта *C* — либо горы, либо озера, поэтому нельзя было построить один большой объезд от *A* до *B*, так что все дороги из пункта *A* в пункт *B* ведут через пункт *C*.

- При этом водители могут выбирать, каким путем ехать от *A* до *B*: 1) от *A* до *B* — по прямой (самый короткий маршрут, но и самый загруженный); 2) от *A* до *C* — по прямой, потом от *C* до *B* — по окружной; 3) от *A* до *C* — по окружной, от *C* до *B* — по прямой; 4) от *A* до *B* через *C* по двум окружным (самый длинный маршрут, но и самая незагруженная дорога).
- Водители, выбирающие тот или иной вариант движения, распределятся по отрезкам пути таким образом, что время движения по любому маршруту (прямому или объездному) займет 40 минут (транспортное равновесие!), потому что объездной занимает именно 40 минут.
- При этом в транспортном равновесии прогнозируются 20-минутные пробки — и на участке перед центральным пунктом *C*, и перед конечным пунктом *B*.

Итого, все участники дорожного движения в зависимости от выбранного маршрута делятся у нас на 4 категории, но любой из них затрачивает на проезд от *A* до *B* ровно 1 час 20 минут.

А теперь — внимание!

Приходит математик Юрий Нестеров и ставит знак запрета на движение из пункта *A* в пункт *B* по прямой, минуя окружные маршруты. Иными словами, если от *A* до *C* машина двигалась по прямому отрезку, то от *C* до *B* разрешается ехать только по окружной. Если к *C* приехал по окружной — дальше можно

по прямой (можно ехать и по второму полукольцу, но, как мы вскоре убедимся, никто так делать не будет).

В новом транспортном равновесии поток поделится ровно на две части: первая половина машин проедет по маршруту «прямая — полукольцо», вторая половина — по маршруту «полукольцо — прямая».

Половину потока прямая узкая дорога уже выдерживает, пробок нет ни на каком отрезке пути, и каждый участник дорожного движения экономит ровно 20 минут. Таков эффект от установки одного запрещающего знака.

Абсолютно гениально!

Рекомендуемые источники по теории игр

Настоящее просвещение — это не подача знаний на тарелочке с золотой каемочкой. Это напряжение мозгов, это стимул к самостоятельному изучению предмета. Именно такое просвещение является делом всей моей жизни! Так что все, кто заинтересовался теорией игр, — вперед, за учебники!

Книги

1. *Захаров А. В.* Теория игр в общественных науках: Учебник для вузов. — М.: Изд. дом Высшей школы экономики, 2015.
2. *Колесник Г. В.* Теория игр. — М.: Либроком, 2017.
3. *Диксит А., Нейлбафф Б.* Теория игр. Искусство стратегического мышления в бизнесе и жизни. — М.: Манн, Иванов и Фербер, 2017.

4. *Писарук Н. Н.* Введение в теорию игр. — Минск: БГУ, 2015.
5. *Данилов В. И.* Лекции по теории игр. — М.: Российская экономическая школа, 2002.
6. *Binmore K.* Fun and Games: A Text on Game Theory. Lexington; Toronto: DC Heath & Co, 1992.

Некоторые рекомендации автора перед чтением:

- 1 и 2 — серьезные книги, для профессионалов;
- 3 и 4 — подходят для начального знакомства с темой;
- 5 — для профи и сверхпрофи;
- 6 — веселая книжка с картинками из «Алисы в Стране чудес», но на самом деле не очень-то простая.

Онлайн-ресурсы автора (не только по теории игр)

1. Сайт автора https://savvateev.xyz/
2. YouTube-канал автора «Маткульт-привет!», где мы записываем подручными средствами всю математику, которую я знаю. Также все видео теперь заливаются на Рутуб и на http://sponsr.ru/savvateev, этот последний портал является основным и содержит, помимо всех выпускаемых видео, еще информацию о моих популярных лекциях по разным городам России и не только, а также мои путевые заметки.
3. «Теория игр» на YouTube.
   Короткий URL: https://clck.ru/3QwyD9
4. «Математика для всех» на YouTube.
   Короткий URL: https://clck.ru/3QwyGt
5. «Математический анализ» на YouTube.
   Короткий URL: https://clck.ru/3QwyKL

6. «Линейная алгебра и элементы топологии» на YouTube.
   Короткий URL: https://clck.ru/3QwyLz
7. «Геометрия и группы» на YouTube.
   Короткий URL: https://clck.ru/3QwyNv
8. «Математика для всех» на Stepik.org.
   Короткий URL: https://clck.ru/3QwyQJ
9. «100 уроков математики» на Stepik.org
   Короткий URL: https://clck.ru/3QwySf
10. «100 уроков математики» на сайте проекта «Дети и наука» childrenscience.ru.
    Короткий URL: https://clck.ru/3QwyWU

9. ИСТОРИЯ МАТЕМАТИЧЕСКИХ ЗАДАЧ

Убежден, что

> математика — не что иное, как часть общечеловеческой культуры, такая же как история, литература и многие другие области.

Поэтому каждый, кто считает себя образованным человеком, должен хотя бы приблизительно представлять, чем занимаются математики и что они делали на протяжении всех этих тысячелетий.

В идеале здорово было бы понимать, в какую сторону наука движется сейчас. Ну а как минимум — быть знакомым с минувшими этапами.

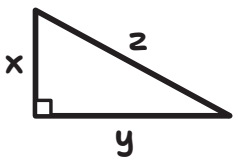
Помогать нам будут «картинки».

Я знаю, что мои взрослые читатели ценят наглядность, она помогает визуально «взбодрить» все, что было подзабыто со школьных времен. Можно назвать первую часть математики этакой **геометрической алгеброй, где формулы можно изобразить**.

Итак, поехали! На машине времени, примерно на две с половиной тысячи лет назад!

1.

Еще в Древней Индии было известно: чтобы получить прямоугольный треугольник с целыми сторонами,



нужно взять некоторые два натуральных числа m и n ($m > n$) и с их помощью вычислить длины сторон прямоугольного треугольника по формулам:

$$\begin{cases} x = 2mn \\ y = m^2 - n^2 \\ z = m^2 + n^2 \end{cases}$$

Эти формулы называются **формулами индусов**, хотя в то время еще никто не пользовался буквенной символикой в алгебре.

2.

А вот что доказал в свое время Пифагор про любой прямоугольный треугольник:

$$x^2 + y^2 = z^2.$$

Данная формула характеризует прямоугольные треугольники, и только их! Индусы, видимо, знали, что это так, но

не знали, как это доказать (Пифагор был первым на Земле, кто вообще «парился» с доказательствами!). Проверка того факта, что формулы индусов задают стороны прямоугольного треугольника, достаточно проста и сводится к прямой подстановке (самостоятельно убедитесь в том, что все пересокращается, если подставить наши формулы в соотношение Пифагора). А вот почему ВСЕ прямоугольные треугольники задаются формулами индусов? И все ли? (На самом деле этими формулами задаются все прямоугольные треугольники, у которых длины сторон в совокупности взаимно просты, то есть не имеют общих делителей, кроме 1. И на пару m, n надо наложить условие, что они взаимно простые и разной четности. Но это уже детали!)

До нас дошел вывод формул индусов в одном из томов Диофанта Александрийского*.

Посмотрите, как устроен мозг математика. Он на какую-нибудь формулу или уравнение, которые уже решены, смотрит под разными углами и начинает их развивать: усложнять, уточнять, или, если решить не получается, наоборот, упрощать, рассматривать частные случаи.

Давайте и мы для примера «потопчемся» на этом самом $x^2 + y^2 = z^2$ и рассмотрим крайние случаи.

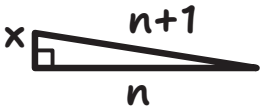
Для начала выделим из всего многообразия треугольников самые «вытянутые», «длинные» — настолько узкие, словно

---

* Диофант Александрийский — древнегреческий математик, живший предположительно в III веке н. э. Нередко упоминается как «отец алгебры». Автор «Арифметики» — книги, посвященной нахождению положительных рациональных решений неопределенных уравнений.

это две почти параллельные линии, которые смыкает малюсенькая «перегородка» (то есть один катет — максимально короткий).

Попробуем найти такой треугольник, у которого длинный катет, вот такой:



На единицу меньше, чем гипотенуза.

Стороны нашего треугольника — n, $n + 1$ и неизвестный x, и возникает задача описания таких вот «вытянутых» прямоугольных треугольников, которая сводится к тому, что из числа $(2n + 1)$ должен нацело извлекаться корень:

$$2n + 1 = x^2,$$

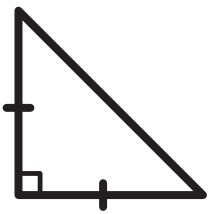
потому что тогда $(n + 1)^2 - n^2 = (n^2 + 2n + 1) - (n^2) = x^2$, а это как раз и означает, что треугольник со сторонами n, x и $(n + 1)$ является прямоугольным.

Примеры треугольников, где длина катета (n) и длина гипотенузы $(n + 1)$ отличаются друг от друга на 1:

$2n + 1$	x^2	катет x (короткий)	катет n (длинный)	$n + 1$ (гипотенуза)
9	9	3	4	5
25	25	5	12	13
49	49	7	24	25
81	81	9	40	41

(Подробнее — в одной из лекций курса автора «Вехи математики: от Евклида до Галуа» на YouTube-канале «Маткульт-привет!»*).

А теперь давайте попробуем рассмотреть прямоугольный треугольник, максимально похожий на равнобедренный.



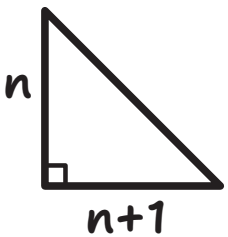
Оказывается, что задача найти равнобедренный прямоугольный треугольник нерешаема: его НЕ СУЩЕСТВУЕТ. Доказательство несуществования равнобедренного прямоугольного треугольника сводится к тому, что **корень из 2 не может быть представлен в виде отношения двух целых чисел**.

$$\sqrt{2} \neq m/n.$$

Но, возможно, существует прямоугольный треугольник, у которого длины катетов отличаются друг от друга на минимальную величину (допустим, один катет n, другой — $(n + 1)$)? Иными словами, мы ищем «почти равнобедренные» прямоугольные треугольники.

---

* Короткий URL: https://goo.su/Ln3lzR.



Ответ: да, может. Эта задача значительно сложнее задачи о поиске «узкого» прямоугольного треугольника, разобранной выше. Оказывается, существует бесконечная серия растущих по размеру прямоугольных треугольников, катеты которых отличаются ровно на 1 (и это ответ на вопрос пытливого математика ☺).

Удивительно, но данная задача сводится к решению в целых числах уравнения:

$$y^2 - 2x^2 = -1.$$

Вот как получается это уравнение (сделаем замену с y):

$$n = (y - 1)/2;$$

$$n + 1 = (y + 1)/2;$$

$n^2 + (n + 1)^2 = x^2$ домножим на 4:

$$(y - 1)^2 + (y - 1)^2 = 4x^2;$$

$2y^2 + 2 = 4x^2$ разделим на 2:

$$y^2 + 1 = 2x^2;$$

перенесем квадраты влево, -1 — вправо и наконец получим:

$$y^2 - 2x^2 = -1.$$

Вспомним, что y/x не может быть равно $\sqrt{2}$. Следовательно, y^2/x^2 не может быть равным в точности числу 2; далее умножаем на x^2 и получаем, что y^2 не может быть равным $2x^2$! Иными словами, при любых натуральных x, y верно неравенство

$$y^2 - 2x^2 \neq 0.$$

Левая часть этого неравенства является целым числом. Раз это число не может быть равно 0, то у пытливого математика должен возникнуть закономерный **вопрос**: а может ли оно быть максимально близким к нулю целым числом? Например, равным -1 (что как раз и требуется для нахождения почти равнобедренных прямоугольных треугольников)?

Ответ: да! И бесконечное количество раз!

Тут же возникает и **следующий вопрос**, если мы продолжаем играть в пытливого математика: а что, если 2 мы заменим на другое число, например m? И рассмотрим разность не только минус один, но и плюс один?

$$y^2 - mx^2 = \pm 1.$$

Возможно ли найти такие целые (или натуральные; в данном случае разницы нет, так как их все равно возводят в квадрат) числа x и y, для которых выполняется это равенство? **И снова ответ**: да, бесконечное количество раз — для любого такого m, которое само не является полным квадратом. Если m является квадратом натурального числа, то такое равенство невозможно (кроме тривиальных случаев).

Выписанное выше уравнение (при m, не являющемся полным квадратом) называется уравнением Пелля*, однако рассматривал и решал его **Пьер Ферма** (подробнее о нем и его числах — в разделе 10) — так очень часто бывает, что уравнение называется именем не того, кто его придумал на самом деле, — тот самый Ферма, который перешел к еще одному интереснейшему обобщению все того же исходного уравнения, приведенного на странице 110.

Он задался вопросом: а что, если в уравнении $x^2 + y^2 = z^2$, применить вместо квадрата другую степень — куб, 4-ю, 5-ю или вообще n-ю?..

$$x^3 + y^3 = z^3?$$
$$\vdots$$
$$x^n + y^n = z^n?$$

Поиск ответа был поистине драматическим!.. Ведь чего только не было — люди доходили до отчаяния, посвящая всю жизнь решению этого уравнения, пока в 1994 году оно не было полностью решено**.

* * *

Ну а еще одно совершенно замечательное, перспективное направление размышлений — это заменить z^2 на любое n (на какое-нибудь число):

$$x^2 + y^2 = n,$$

---

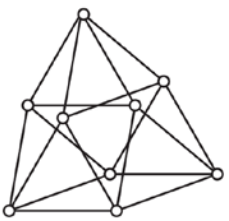
* Л. Эйлер по ошибке приписал один из способов решения этого уравнения английскому математику XVII века Дж. Пеллю.

** В 1994 году английский математик Э. Уайлс опубликовал доказательство теоремы Ферма. После некоторых доработок оно было признано исчерпывающим.

таким образом задавая **вопрос**: в каких случаях можно представить n в виде суммы двух квадратов?

Эта задача имеет прямое отношение к очень простой и красиво формулируемой гипотезе, которая называется **гипотезой Эрдёша о равных отрезках**, или **задачей Эрдёша о равных расстояниях**.

Дано несколько точек на плоскости. И мы сами должны руками их расставить так, чтобы получилось как можно больше одинаковых по длине отрезков. Например, решение (совершенно неочевидное!) для девяти точек выглядит следующим образом:



Эрдёш смог (посредством весьма хитрых манипуляций) свести данную задачу к нашей предыдущей:

$$x^2 + y^2 = n,$$

которая в свою очередь, как показал Гаусс, сводится к исследованию частного случая, когда n — простое число.

И мы приходим к **Рождественской теореме Ферма** — замечательному утверждению, что

> любое простое число вида $4k + 1$ есть сумма двух квадратов, например: $17 = 1 + 16$; $61 = 25 + 36$.

А в сердце этой последней теоремы находятся Гауссовы числа*: $\mathbb{Z}[i]$.

В задаче Эрдёша еще много белых пятен. И асимптотика** того, сколько отрезков можно уравнять друг другу, никому не известна и по сей день! Вот такая красивая задача, хотя она еще не решена.

---

* Гауссовы числа — комплексные числа, у которых как вещественная, так и мнимая часть — целые числа. С геометрической точки зрения образуют на плоскости решетку всех точек с целыми координатами. Впервые были рассмотрены К. Ф. Гауссом в 1832 году.

** Асимптотика — поведение функции в бесконечности.

10. ПОСТРОЕНИЯ ПРИ ПОМОЩИ ЦИРКУЛЯ И ЛИНЕЙКИ

Э. Галуа

Рассмотрим еще несколько задач, которые достались математике в наследство с незапамятных времен. На машине времени мы снова переметнемся туда, на 2500 лет назад!

Расскажу вам про четыре великие задачи, оказавшиеся древним математикам не по зубам. Но после величайшей математической революции конца XVIII — начала XIX века, которая связывается с именем Эвариста Галуа* (хотя и до него трудились еще с десяток гениальнейших математиков), все эти задачи были разделаны под орех! Кроме одной. Она перешла в замечательную теорему про свойства числа π, и о ней мы расскажем чуть позже.

---

* Эварист Галуа́ — французский математик, основатель современной высшей алгебры. Революционер-республиканец, был застрелен на дуэли в возрасте двадцати лет.

* * *

Итак, 200 лет назад, к 1830 году, величайшая математическая революция завершилась, и с тех пор математика приняла совершенно новый облик! Язык всего того, что делают теперь современные математики, был унаследован из записей Эвариста Галуа и продолжателей его идей.

* * *

Но вернемся к древним. Их интересовало построение конструкций, где нужно было чертить окружности и прямые. И для этого им нужны были какие-то приспособления.

«Прибор», рисующий **окружность**, устроен так:

- на плоскости даны две различные точки;
- нужно изготовить некое «плечо», длина которого равна расстоянию от одной точки до другой;
- установив плечо одним концом в первой точке, другим концом можно провести окружность радиуса, равного расстоянию между ними.

А как начертить **прямую**?

- на плоскости даны две различные точки;
- можно провести прямую линию, которая их соединяет (проходит через них).

Вы можете также случайным образом ставить всевозможные точки на плоскости и проводить какие-то конструкции через эти случайно выбранные точки.

> Важно, чтобы задача, которая вам поставлена, была разрешена с помощью доказательной геометрии,

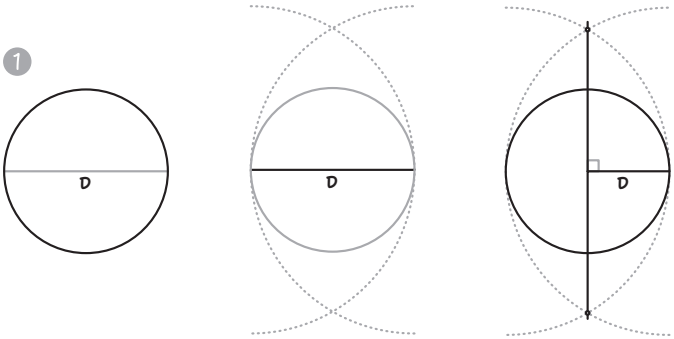
то есть чтобы вы могли **доказать**, что последовательность проведения окружностей и прямых, предложенная вами, всегда точно решает заданную вам задачу — вне зависимости от случайно выбранных вами в процессе построения точек: «Поставим-ка произвольную точку здесь да проведем вот так, а потом — точка пересечения, она вот тут, а мы потом проведем-ка... и т. д., ну а потом, мол, проведем вот такую окружность...»

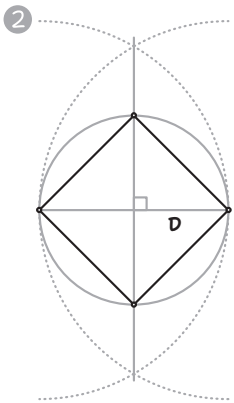
Иными словами: то, что у вас получится в результате, всегда должно удовлетворять требованиям поставленной задачи. Нужно, чтобы любые произвольные конструкции в итоге

сводились к одной и той же нужной вам точке. Каждый раз это доказывать — отдельная история.

* * *

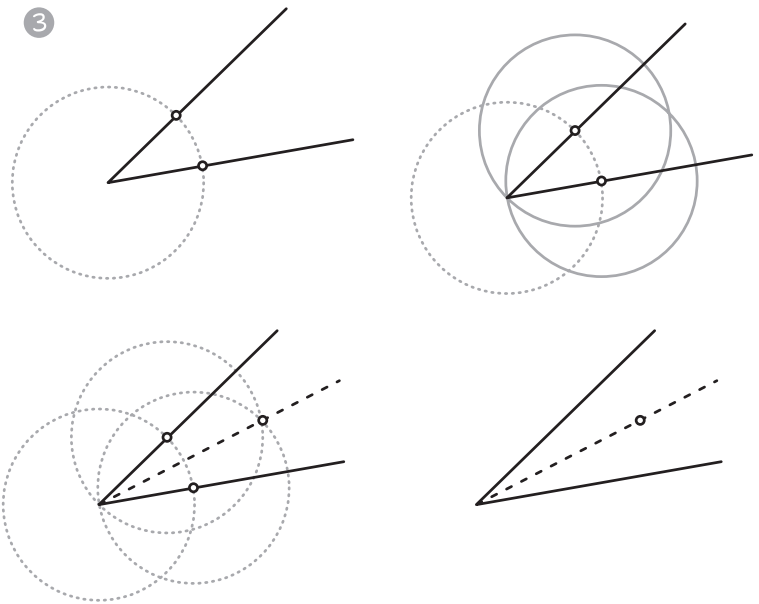
Древние умели делать многое: **строили прямые углы** (опускали перпендикуляры, поднимали из прямой перпендикуляр).





Также они **умели делить угол на две равные части**:

- из вершины угла рисовали окружность произвольного радиуса;
- из точек пересечения окружности с лучами угла чертили две окружности того же радиуса;
- луч из вершины угла, проходящий через точку пересечения двух этих окружностей, делил угол пополам;

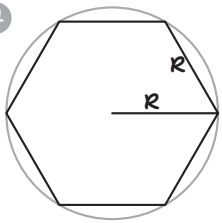


- окружности с другим радиусом давали точку, расположенную на другом расстоянии от вершины угла. При этом всегда можно было доказать, что точка пересечения двух ЛЮБЫХ (равных) окружностей, построенных по такой схеме, всегда окажется на биссектрисе угла. **Произвольность становится необходимостью!**

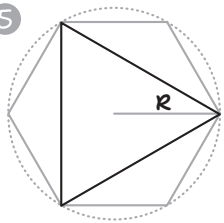
Еще древние умели **строить квадрат** (см. выше: они умели строить прямые углы).

И даже **построение правильного шестиугольника** не казалось сложной штукой. Они заметили, что если по внутренней стороне окружности последовательно «откладывать» отрезки, равные радиусу этой окружности, то получится шестиугольник, а заодно и **правильный треугольник**:

4

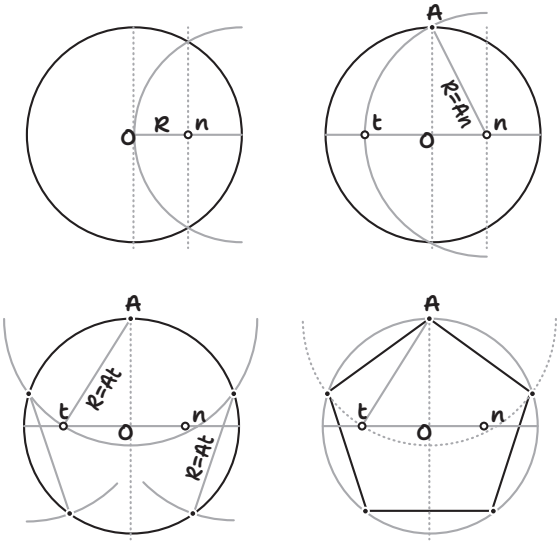


5

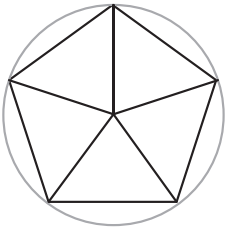


А еще древние умели строить **правильный пятиугольник**, что уже совершенно нетривиально.

6



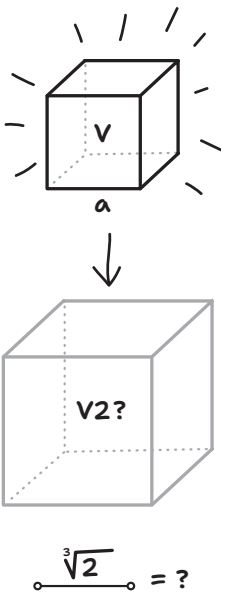
Конструкция, которую получили древние, оказалась непростой и включала в себя то, что называется золотым сечением*.



Теперь рассмотрим четыре задачи, решать которые древние не умели.

1. **Как «удвоить» куб?**

Говорят, в Древней Греции боги приказали людям за один день «удвоить» размер золотого куба при помощи циркуля и линейки.



Люди взяли и удвоили все его стороны. Боги рассмеялись: «Да вы не удвоили, а увосьмерили куб!» И люди поняли, что речь идет об объеме, то есть требовалось построить кубик, объем которого оказался бы ровно вдвое больше изначального. А по стороне, соответственно, различие будет значительно меньше.

Современное решение: люди, знающие алгебру, понимают, что «удвоение» куба означает, что нужно построить куб с длиной грани (стороной каждого квадрата), равной $\sqrt[3]{2}$ от длины изначального.

---

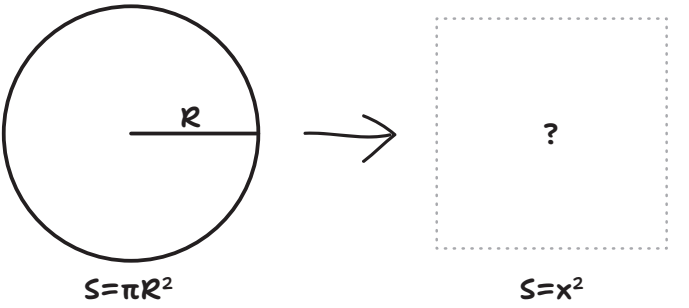
* Золотое сечение (золотая пропорция, гармоническое деление) — отношение частей и целого, при котором отношения частей между собой и наибольшей части к целому равны. Формула золотого сечения: $(\sqrt{5} + 1)/2$, что с точностью до трех знаков равно 1,618.

Эта задача на построение $\sqrt[3]{2}$, и тогдашним математикам она оказалась совершенно не по зубам.

2. **Как построить квадрат, равный кругу?**

Дан круг. При помощи циркуля и линейки нужно построить квадрат той же площади. Это известная задача о квадратуре круга.

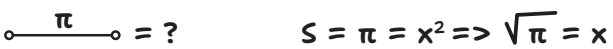
Современное решение заключается в том, чтобы найти ответ на вопрос: в какое количество раз нужно увеличить радиус



круга (примем длину этого отрезка за 1), чтобы он стал стороной квадрата с площадью, равной площади нашего круга?

Площадь квадрата равна квадрату стороны a, то есть a^2. А площадь круга равна πr^2, то есть в нашем случае площадь круга будет равна π. И нужно, чтобы это было равно квадрату какого-то числа x, то есть надо строить $\sqrt{\pi}$.

Когда мы будем этим заниматься, то поймем, что извлекать квадратный корень и возводить в квадрат отрезки при помощи циркуля и линейки достаточно легко. Так что вопрос лишь в том, чтобы построить отрезок длины π.



Если вы умеете строить $\sqrt{\pi}$, то довольно просто построить отрезок длиной π, и, наоборот, имея отрезок длины π, легко построить $\sqrt{\pi}$.

Иными словами, это задача на построение числа π.

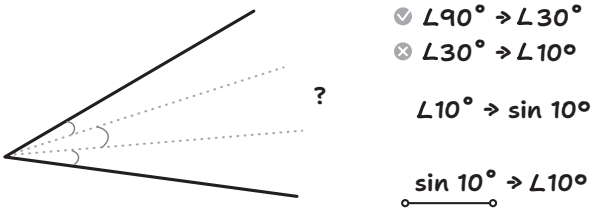
Она была решена позднее 1830 года (после завершения математической революции) из-за непонятной арифметической структуры этого «страшного» числа π.

3. **Как начертить трисектрисы?**

Дан угол. Надо разделить его на 3 равные части.

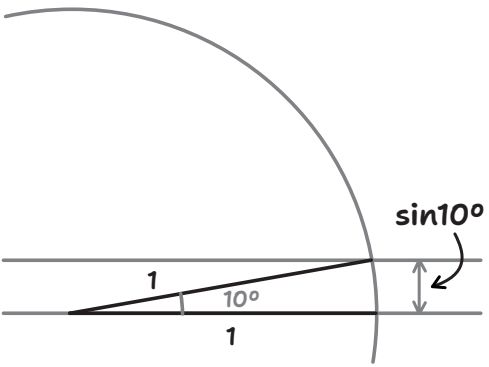
Иногда это можно сделать без проблем, например, если угол прямой: угол в 90° легко делится на три равные части, с получением углов по 30° (скажем, можно провести биссектрису в равностороннем треугольнике). Однако найти доказуемую процедуру деления произвольного угла на три равные части не удалось. Более того, деление даже конкретного угла

в 30° на 3 равные части (то есть построение при помощи циркуля и линейки угла в 10°) не удавалось произвести!



Современное решение: неудачи древних крылись в арифметической природе некоего числа — sin10°.

Если мы умеем строить угол в 10°, то понятно, что, проведя окружность радиуса 1, вы получите sin10°. И наоборот, имея возможность построить отрезок длиной sin10°, вы можете отложить его перпендикулярно некой прямой — вверх; затем провести параллельную прямую через верхний конец отрезка длиной sin10° и наконец провести окружность радиуса 1 с центром в любой точке одной из этих двух параллельных прямых, — и вы получите угол в 10° (см. рисунок).



Это эквивалентные друг другу задачи. И древние их тоже не умели решать.

Карл Фридрих Гаусс

4. Как строить правильные многоугольники?

Необходимо построить правильный n-угольник с заданным числом сторон n. Многоугольники при $n = 3$, при $n = 4$, при $n = 5$ и при $n = 6$ древние строить еще умели, а при $n = 7$ — уже нет.

Пьер де Ферма́

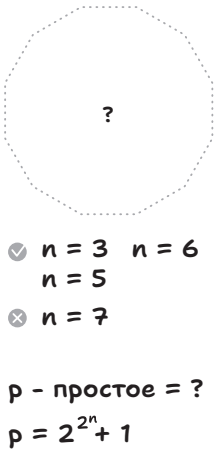
Эта задача тоже перешла в Новое время. Гаусс* доказал, что можно построить правильный n-угольник, когда n — простое число вида $2^{(2^k)} + 1$. Под n-угольниками в этой главе будем иметь в виду правильные многоугольники с числом сторон, равным n. Для двух взаимно простых нечетных чисел p, q: если построен p-угольник и q-угольник, то можно построить (pq)-угольник (просто нанеся эти многоугольники на одну и ту же окружность таким образом, чтобы одна из точек окружности была общей вершиной; доказать этот факт не так-то легко, он упирается в основную теорему арифметики (ОТА), о которой будет рассказано далее в этой книге). Например, $p = 3$ и $q = 5$, и можно построить 15-угольник.

---

* Иоганн Карл Фридрих Гаусс (1777–1855) — немецкий математик, механик, физик, астроном и геодезист. Считается одним из величайших математиков всех времен, «королем математики». С именем Гаусса связано множество теорем и научных терминов в математике, астрономии и физике.

Любой n-угольник можно превратить в $2n$-угольник, так как мы умеем делить угол на два равных угла.

А во время той самой «математической революции» было доказано, например, что семиугольник при помощи циркуля и линейки не строится. И вообще было установлено, что те простые числа p, при которых строится наш правильный p-угольник, — это такие замечательные простые числа вида $2^{(2^n)} + 1$, называемые простыми числами Ферма*.



Задача, кстати, похожа на задачу на построение трисектрисы, только здесь мы делим конкретный угол в 360° на n равных частей (а в предыдущей задаче, наоборот, количество частей было конкретным — 3, а угол мог быть любым). Здесь же нет конкретики по поводу n, то есть количество равных частей «гуляет». На какое-то количество равных частей наш двойной развернутый угол в 360° делится, а на какое-то — нет.

* * *

Оказывается, решения всех четырех задач ведут к алгебре, и, в частности, задача о квадратуре круга приводит к вопросу о том, каким алгебраическим уравнениям удовлетворяет

---

* Пьер де Ферма́ (1607–1665) — французский математик-самоучка, один из создателей аналитической геометрии, математического анализа, теории вероятностей и теории чисел. Наиболее известен формулировкой Великой теоремы Ферма, «самой знаменитой математической загадки всех времен».

число π. То есть можно ли написать какой-нибудь многочлен с целыми коэффициентами, чтобы π было его корнем?

$$a_0 + a_1x + ... + a_nx^n,\ \pi \text{ — корень...}$$

Иными словами, чтобы при подстановке π в этот многочлен получалось точное равенство $a_0 + a_1\pi + ... + a_n\pi^n = 0$.

Очень трудная теорема, доказанная Эрмитом и Линдеманом, заключается в том, что **такого многочлена не существует**.

Из этой теоремы довольно быстро вывели, что построить число π при помощи циркуля и линейки нельзя, что, естественно, привело к еще одной интересной теме для изучения — корни многочленов.

* * *

Четыре рассмотренные нами задачи родственны с пятой задачей — проблемой нахождения корней многочленов в явной форме (через все четыре арифметические операции и извлечение корней любых степеней — эти пять действий выполняются много раз подряд над коэффициентами многочлена, в результате чего получаются огромные многоэтажные дроби, щедро приправленные радикалами).

А именно, в начале XIX века (возможно, даже гораздо раньше) выяснилось, что построение при помощи циркуля и линейки тоже сводится к алгоритму,

в котором действия «+», «–», «×» и «:» сопровождаются еще и извлечениями квадратных корней на некоторых этапах.

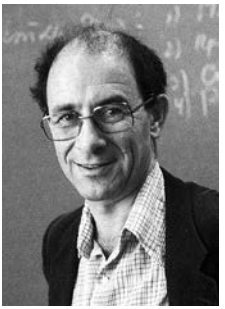
А для нахождения корней многочленов разрешается извлечение корней любых степеней и тот же арифметический набор действий.

В таком направлении как раз и двигалась алгебра начала XIX века — и появились теоремы о доказуемой невозможности существования тех или иных алгоритмов, в том числе дающих решения четырех задач античности (ситуация с n-угольниками оказалась сложной, однако исходная задача о построении 7-угольника доказуемо не имеет решения). Что касается нахождения корней многочленов, то здесь проблемы начинаются со степени 5: в общем виде выписать формулу для корней многочлена 5-й степени через его коэффициенты, используя вышеописанные 5 операций, доказуемо невозможно. Однако конкретные многочлены могут быть проще и допускать решение «через радикалы». Теория Галуа, разработанная в этом направлении, до сих пор является центральной во всей математике.

11. МАТЕМАТИЧЕСКАЯ ТЕХНИКА

Технический аппарат... Техника, друзья, есть не только на улице (сразу же представили себе что-то ездящее, убирающее) — техника есть и в математике!

Так какая же техника понадобится именно нам? А понадобится нам целый ряд утверждений, которые начинаются с визуального наблюдения за поведением чисел.



В. И. Арнольд

Владимир Игоревич Арнольд* однажды сказал:

> «Математика — это часть физики, в которой эксперименты очень дешевы».

Все верно, особых затрат они не требуют. Ведь если вы запускаете, скажем, коллайдер, — это какие-то немыслимые

---

* Владимир Игоревич Арнольд (1937–2010) — советский и российский математик, автор работ в области топологии, теории дифференциальных уравнений, теории особенностей гладких отображений и теоретической механики. Один из крупнейших математиков XX века.

деньги. Ну а в математике? Натуральные числа? Посидел какой-нибудь Васечкин Петя, пособображал — да что-то и увидел. Что, например?

Малая теорема Ферма

Первое, что увидит любой Васечкин, — **малую теорему Ферма (МТФ)**.

Как он ее увидит? Очень просто — он начнет экспериментировать! Возьмет, например, число 13 и возведет в эту степень — в 13-ю, например, число 21. Затем из 21^{13} вычтет 21. И обнаружит, что результат делится на 13:

$$21^{13} - 21 \vdots 13.$$

«А если, — скажет он, — возвести 2 в тринадцатую степень и вычесть 2? О-оу, опять делится на 13?! Что за напасть такая?!»

$$2^{13} - 2 \vdots 13.$$

«А если другое число взять — 13 заменить на 4? Эх... не получается... Ну а если что-то, например 10, возвести в одиннадцатую степень? Тоже сработало: результат будет делиться на 11!»

$$10^{11} - 10 \vdots 11.$$

Перебирая комбинации таким образом, Петя Васечкин обнаружит, что

> для любого простого p и для любого целого числа $a^p - a \vdots p$.

$$\forall \text{ простого } p$$
$$\forall \text{ числа } a$$
$$a^p - a \vdots p$$

Это и есть **Малая теорема Ферма**, значение которой для математики нельзя переоценить.

Это абсолютно необходимый результат во всех последующих серьезных исследованиях, касающихся арифметики, геометрии, алгебраической геометрии, физики (скажем, теории резонанса) — да чего угодно. Да просто всех целых чисел, как они есть.

В моих лекциях есть по крайней мере четыре красивых доказательства Малой теоремы Ферма.

Ведь результат доказательства — ядро, а на то, что в ядре, надо посмотреть под несколькими углами. В математике, как и в истории, полезно привести много разных доказательств, поскольку они по-разному проливают свет на предмет.

Арифметика остатков

- Легко заметить, что, если сложить два числа, которые делятся на некое число m, то получится число, которое тоже делятся на m.
- То же — при вычитании.
- Если умножить число, делящееся на m, на любое число (неважно, делящееся на m, или нет), получается число, делящееся на m.
- Ну а если, например, вы складываете два числа, дающие при делении на m какие-то остатки α и β, то сумма даст такой же остаток, как $\alpha + \beta$ (то есть чтобы посмотреть на остаток от деления на m, достаточно взять сумму остатков).
- То же самое — при умножении (чуть сложнее): остаток от деления произведения двух чисел на число m равен «остатку от деления произведения остатков» на то же число m.

Это не всегда будет само произведение остатков, потому что оно может вылезать за диапазон от 0 до $(m - 1)$ — кстати, и с суммой так же. Но вычислить остаток от произведения двух чисел при делении на m можно в два этапа: 1) вначале взять оба числа по модулю m, то есть остатки от деления на m; 2) перемножить и потом еще раз взять остаток от деления на m.

То, чем мы сейчас занимаемся, называется **арифметикой остатков**, то есть мы рассматриваем все числа только с точностью до делимости на m. Математики придумали

специальный символ для системы остатков от деления на m, а если точнее, то для обозначения множества классов чисел, дающих один и тот же остаток от деления на m. Таких классов чисел столько же, сколько и остатков, то есть m. Обозначение:

$$\mathbb{Z}/m\mathbb{Z}.$$

Иными словами, вместо числа мы рассматриваем его остаток при делении на m и составляем такую таблицу сложения и умножения, как делается для обычных чисел, только теперь для всех остатков от 0 до $m - 1$.

Сложение остатков при $n = 3$ и $n = 4$:

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1
$n = 3$			

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2
$n = 4$				

Умножение остатков (ненулевых) при $n = 4$ и $n = 5$:

	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1
$n = 4$			

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1
$n = 5$				

Кольцо и поле

Далее, изучив при различных m таблицы умножения ненулевых остатков (таблицы сложения будут очень похожи друг на друга, а таблицы умножения будут сильно различаться), мы обнаружим, что для некоторых из остатков мы сможем отыскать такой, который при умножении на исходный остаток даст остаток, равный 1. То есть взять «обратный» в арифметическом смысле остаток.

Например, для остатка 3 при делении на 10 можно взять остаток 7 при делении на 10: $3 \cdot 7 = 21$, но 21 при делении на 10 дает остаток 1, поэтому в арифметике остатков по модулю 10 имеет место соотношение: «трижды семь равно один».

Вообще арифметика остатков по модулю 10 — это просто таблица умножения, в которой «забыт» первый разряд. Вглядевшись в таблицу, мы убедимся в том, что для остатка 4 не найдется обратного остатка, то есть я не могу умножить 4 на какой-то остаток при делении на 10, чтобы получился остаток, равный 1. Причина в четности: в правой части равенства требуется нечетное число, а слева уже стои́т четное — 4, и остаток берется при делении на четное число — 10, поэтому ничего и не получится.

И есть некоторые числа при делении с остатком на которые, однако, для любого остатка, кроме остатка 0, можно найти обратный. И эти числа — вот сюрприз! — как раз простые (и только они!). Простые числа — это «кирпичики» всей математики.

И если вот это семейство остатков:

$$\mathbb{Z}/m\mathbb{Z}$$

при произвольном m не всегда позволяло находить обратные и математически являлось *кольцом* (не полем), то при простых $n = p$ система остатков (или говоря более научно, *вычетов*)

$$\mathbb{Z}/p\mathbb{Z}$$

является как раз *полем*.

Эти два технических термина — *кольцо и поле* — будут часто появляться в книге.

> **Кольца** — это системы чисел, в которых можно складывать, вычитать и умножать по обычным правилам целых чисел.
>
> **Поле** — это система чисел, которые можно складывать, вычитать, умножать и еще и делить как обычные вещественные числа.

При этом система может состоять как из конечного, так и из бесконечного числа элементов, которые мы складываем, умножаем, делим и вычитаем.

Техника выполнения арифметических операций также лежит в сердце современного взгляда на математику.

Определенные закономерности простых чисел

Наш пытливый Васечкин не может не заметить определенных закономерностей в последовательности всех простых чисел:

2, 3, 5, 7, 11, 13, 17, 19, ... и т. д.

И, конечно, он обратит внимание на то, что подряд могут идти только 2 и 3. Дальше уже любое простое число должно быть нечетным. При этом он обнаружит, что время от времени (в начале списка простых чисел даже довольно часто) простые числа в этой закономерности следуют с интервалом 2. Вопрос: а бесконечно ли количество пар простых чисел, идущих через 2? Самих простых чисел бесконечно много, и мы это далее докажем. Но вот пар простых чисел, идущих через 2?

Еще Евклид задался этим вопросом. Но ответа нет — по сей день эта задача не решена.

> Никто не знает, бесконечно или конечно количество пар простых, так называемых «близнецов», идущих через 2.

Открытая проблема математики!

* * *

Но вообще-то есть очень интересные закономерности в распределении простых чисел.

Например, такая: если мы возьмем некоторую арифметическую прогрессию внутри целых чисел — такую, что начальный член прогрессии и ее шаг (его математики именуют «разностью прогрессии») взаимно просты между собой, то в ней обязательно встретится бесконечно много простых чисел.

Например, количество простых чисел вида $4k + 3$ бесконечно, и количество простых вида $4k + 1$ тоже бесконечно. Оба утверждения — более сильные, чем утверждение, что всех простых чисел бесконечно много.

И простых чисел вида $12k + 5$ тоже бесконечно много. И так далее. Эту теорему доказал Дирихле.

А вот если в нашей арифметической прогрессии начальный член и шаг не взаимно просты, то понятно, что все следующие числа будут делиться на их общий делитель, следовательно, простым ни одно из них уже не будет. Максимум начальный член может быть простым.

Но если они взаимно просты, то есть шанс, что в этой прогрессии бесконечное количество простых. Например, **вопрос:** сколько существует простых вида $12k + 5$? **Ответ:** бесконечное количество! Это доказал Дирихле*.

---

* Иоганн Петер Густав Лежён Дирихле (1805–1859) — немецкий математик, внесший существенный вклад в математический анализ, теорию функций и теорию чисел.

Произведения различных наборов простых чисел

Произведения различных наборов простых чисел никогда не равны друг другу:

$$p_1 \cdot \ldots \cdot p_r \neq q_1 \cdot \ldots \cdot q_e.$$

Из этого, в частности, будет следовать, что *и дроби все разные.* Если написать две дроби, где в числителях и знаменателях какие-то разные наборы, то они никогда не будут обозначать одно и то же количество, что поначалу совершенно неочевидно.

И многие не понимают, что это связано именно с основной теоремой арифметики (ОТА). А **основная теорема арифметики** (подробнее — далее, в соответствующем разделе книги) говорит нам именно об этом:

> Любое натуральное число (кроме единицы) можно представить в виде произведения простых множителей, и притом единственным образом (с точностью до порядка сомножителей).
>
> Пример: $4200 = 2 \times 2 \times 2 \times 3 \times 5 \times 5 \times 7$.

* * *

Вот еще несколько аспектов, с которыми связана **математическая техника**, значительно более продвинутых:

- комплексные числа;
- экспонента от комплексного числа;
- полнота вещественных чисел;

- одно из свойств экспоненты: она осуществляет гомоморфизм между двумя операциями — «плюс» и «умножить»; простите меня те, кому эти слова ни о чем не говорят;
- доказательство главной формулы математики, связывающей три константы e, i, π:

$$e^{i\pi} = -1.$$

Доказательство формулы $e^{i\pi} = -1$ — это, на мой взгляд, фантастическая красотища!

А знаете ли вы, что, к примеру, **Малая теорема Ферма** лежит в основе действия:

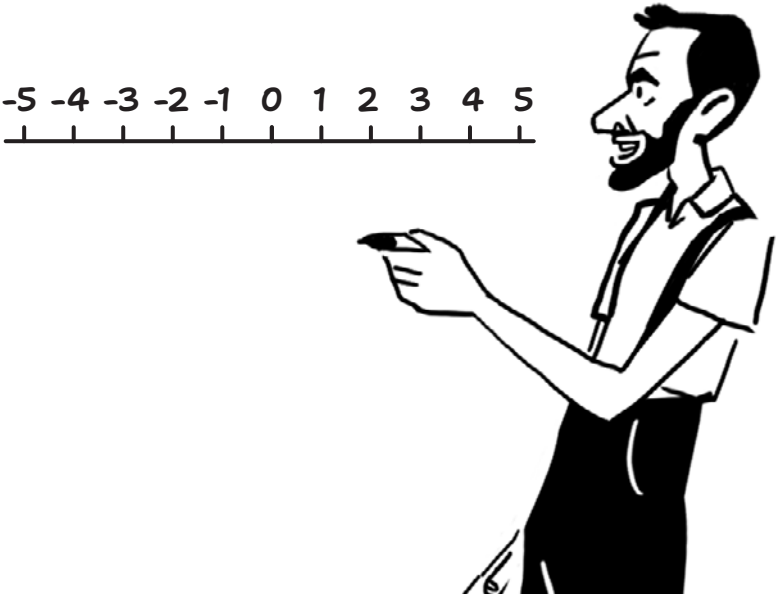
- всех кредитных карт;
- всех компьютеров;
- всех систем шифрования и кодирования на всей Земле?

Иными словами, арифметика остатков — это не просто какие-то математические изыски. Математика управляет всей нашей жизнью каждый день и каждую секунду. Вот так!

12. РАБОТА С ЧИСЛАМИ

Все мы знаем, что математика имеет дело с числами. И числами измеряется все на свете. Например, температура, а «минус пять за бортом» подсказывает нам, что числа бывают как положительными, так и отрицательными. И, на взгляд автора, изучать отрицательные числа гораздо позже, чем положительные, — неправильно. Видимо, школьная программа математики складывалась в тех краях, где нет минусовых температур, а нам, где снег зимой, очевидно: отрицательные числа в жизни нужны.

Как можно изобразить целые числа?



На шкале обозначается точка отсчета (0), влево и вправо от которой много раз подряд откладываются отрезки равной длины. И справа — положительные целые числа, а слева находятся отрицательные.

С целыми числами человечество научилось работать. Давайте на первых порах и мы поработаем с **целыми числами** и для начала перечислим все, что мы о них знаем.

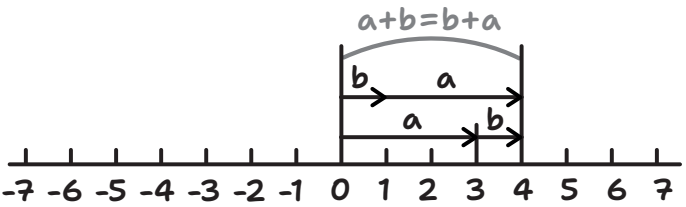
Базовые правила обращения с целыми числами

1. Мы всегда можем сложить два целых числа.

   При этом, меняя порядок слагаемых, мы получаем в результате одно и то же число (перестановочное свойство сложения):

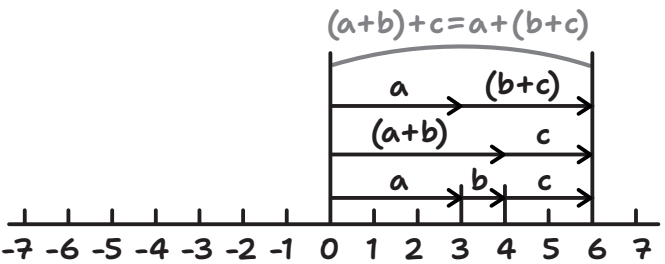
   $$(a + b) = (b + a).$$

   Это даже можно увидеть геометрически — на нашей шкале. Прибавляя к отрезку 0–1, равному 1 шагу, отрезок 1–4, равный 3 шагам, вы попадаете в точку 4. И прибавляя к отрезку 0–3, равному 3 шагам, отрезок 3–4, равный 1 шагу, вы попадаете в ту же точку 4. Вы будто перевернули картинку — просто поменяли отрезки местами.



2. Сочетательное свойство сложения выражается следующим тождеством и соответствующей ему картинкой:

$$(a + b) + c = a + (b + c).$$



3. Для каждого целого числа есть противоположное ему:

$$a + (-a) = 0.$$

4. И в придачу отметим, что для каждого числа прибавление к нему числа 0 ничего не меняет:

$$0 + a = a.$$

Еще раз кратко перечислим **базовые правила обращения с целыми числами** (их важно запомнить, потому что остальные правила сложения выводятся из этих четырех).

> Целые числа — набор неких сущностей, в которых осуществима операция сложения (про операцию умножения мы пока не говорим, она естественным образом «появится» сама, в чем мы убедимся далее).

1. Числа можно складывать в любом порядке (по-математически это называется «коммутативность», по-школьному — «перестановочность»).

2. При сложении числа можно по-разному сочетать («сочетательный закон», или «ассоциативность»; по-школьному — «сочетательность»).
3. Есть некий 0, который все нейтрализует, то есть при прибавлении к нему любого целого числа получается то же самое число.
4. Для каждого числа есть противоположное ему.

* * *

Н. Х. Абель

Обращаю ваше внимание: если у нас есть такой «набор сущностей», как числа, с которыми можно работать по обозначенным правилам, то этот набор сущностей называется **группой по сложению** — коммутативная (или абелева) группа*. В неабелевой группе $a + b$ может отличаться от $b + a$. Целые числа обозначаются буквой $\mathbb{Z}$.

Мы изучаем, как с целыми числами оперировать. И то, что целые числа обладают вышеперечисленными свойствами, открывает ключи ко многим теоремам.

---

* Нильс Хенрик Абель (1802–1829) — норвежский математик. В возрасте 19 лет решил проблему, изучавшуюся математиками с XVI века, доказав невозможность в общем случае выразить решение любого уравнения 5-й и более высокой степени в радикалах (то есть по формулам, аналогичным формулам для квадратных уравнений). Абелева группа — группа, в которой выполняется условие коммутативности (возможности переставлять элементы) групповой операции.

Сложение по Минковскому

Герман Минковский

Перед тем как перейти к умножению, остановимся на так называемом **сложении по Минковскому***, это очень важная операция для двух подмножеств целых чисел.

Если существует два подмножества целых чисел, то можно определить подмножество, которое является множеством всех таких сумм, где a принадлежит A, а b принадлежит B.

$$A, B \subset \mathbb{Z},$$

$$A \oplus B = \{a + b \mid a \in A, b \in B\}.$$

Например, к подмножеству {–1, 0, 3} прибавляем {1, 2}, то есть складываем каждый член первого подмножества с каждым членом второго и получаем новое множество:

$$\{-1, 0, 3\} + \{1, 2\} = \{0, 1, 4, 1, 2, 5\} = \{0, 1, 2, 4, 5\}.$$

Чисел в ответе оказалось не шесть, как мы могли ожидать, а пять (повторяющиеся результаты мы не учитываем, «склеиваем»).

---

* Герман Минковский (1864–1909) — немецкий математик, разработавший геометрическую теорию чисел и геометрическую четырехмерную модель теории относительности. *Сумма Минковского* двух подмножеств A и B линейного пространства V (конструкцию легко обобщить на случай произвольной группы) — это множество C, состоящее из сумм всевозможных векторов из A и B.

Вычитание

Однако пока вернемся к обычному сложению (чисел, а не подмножеств). Раз есть сложение, то существует и **вычитание**. Такая операция по определению обратна сложению. То есть это попытка решить уравнение:

$$a + x = b.$$

Решив его, я хочу получить x. И этот x будет называться разностью b и a.

Докажем лемму*: Решением данного уравнения будет служить число, являющееся суммой числа b и числа, обратного к a:

$$x = b + (-a) = b - a$$

(по определению назовем разностью двух чисел сумму первого из них с числом, противоположным второму). Это действительно надо доказывать (когда мы имеем дело с формальной математикой, приходится «работать руками»).

Для доказательства будем использовать знакомые нам аксиомы — базовые правила обращения с целыми числами:

$$(a + b) = (b + a);$$
$$(a + b) + c = a + (b + c);$$
$$a + (-a) = 0;$$
$$0 + a = a.$$

---

* Лемма — доказанное утверждение, полезное не само по себе, а для доказательства других утверждений. По этой причине она также известна как *вспомогательная теорема*.

Доказательство:

$$a + [b + (-a)] = a + [(-a) + b] =$$
$$= [a + (-a)] + b = 0 + b = b.$$

Вот так мы работаем в алгебре: мы устанавливаем, чему равен x в уравнении $a + x = b$.

Вот такой мастер-класс по работе с алгебраическими операциями!

* * *

А что, если я напишу уравнение $x + a = b$? Разумеется, ничего не изменится, потому что в силу **коммутативности** $x + a = a + x$ и решение будет то же самое.

Внимание! Если бы операция была некоммутативной, то два уравнения

$$x + a = b$$

и

$$a + x = b$$

были бы не эквивалентными друг другу и их решения были бы в общем случае различными элементами группы. Возникли бы две различные обратные операции.

Одна называлась бы **левой обратной**, а другая — **правой обратной** (и в теории групп — настоящей, где группы некоммутативны, — это действительно происходит: у нас две разные обратные операции!).

Деление

Да, мы пока не пришли естественным способом к операции умножения целых чисел, однако все и так умеют умножать, поэтому мы рассмотрим операцию деления с точки зрения операции, обратной к умножению, — по аналогии с вычитанием как операцией, обратной к сложению.

Для построения операции деления рассмотрим следующее уравнение:

$$ax = b = xa.$$

Введем определение: x, являющийся решением этого уравнения, называется результатом деления b на a. В каком порядке расположить множители a и x, здесь так же неважно в силу коммутативности операции умножения.

Но если наша операция — это возведение в степень, то уже имеет значение, решение какого уравнения я ищу:

$$x^a = b \text{ или } a^x = b,$$

потому что в одном случае получится $\sqrt[a]{b}$, а в другом случае — $\log_a b$.

$$\log_a b \leftarrow a^x = b \text{ или } x^a = b \rightarrow \sqrt[a]{b}\,.$$

Видите? Одна и та же операция возведения в степень с помощью обращения с разных сторон дает столь хорошо знакомые нам «школьные объекты» — корень и логарифм.

А в общем выходит, что

> для целых чисел такие операции, как умножение, возведение в степень порождаются одной операцией — сложением. Умножение связано со сложением, возведение в степень связано с умножением.

И первое, что надо сделать, — очень подробно изучить поведение операции «+» («плюс», или сложения).

13. ПОСТРОЕНИЕ УМНОЖЕНИЯ

Вместе со сложением, как мы убедились выше, рождается вычитание как обратная операция. Ну а раз мы умеем складывать по Минковскому, то можно по Минковскому и вычитать — почему бы и нет?

Когда мы пишем «$\ominus$» (так называемый «минус в кружочке»), мы всегда будем иметь в виду операцию «вычитания по Минковскому», то есть множество всевозможных разностей элементов двух подмножеств, A и B. (Вычитаем мы при этом всегда элемент B из элемента A, но не наоборот!)

$$A \oplus B$$

$$A \ominus B.$$

Приведем пример вычитания по Минковскому. Пусть подмножество

$A = \{1, 2, 4\}$, а подмножество $B = \{-100, 0, 2\}$. Тогда разность этих множеств по Минковскому $\{1, 2, 4\} - \{-100, 0, 2\} = \{101, 102, 104, 1, 2, 4, -1, 0, 2\} = \{-1, 0, 1, 2, 4, 101, 102, 104\}$ (повторяющееся число 2 достаточно указать один раз).

Внимание! Вычитание по Минковскому не является обратной операцией к сложению по Минковскому! Это означает, что ответом на задание «Найдите такое подмножество P, чтобы сумма по Минковскому двух подмножеств A и P совпадала с подмножеством B» почти никогда не является разность по Минковскому подмножеств B и A. Такое задание почти никогда не выполнимо: обратной операции к сложению по Минковскому построить нельзя. Разве что очень редко можно удачно попасть в ситуацию, когда сумма по Минковскому обратима. (Это не очень просто понять, увы, но простите, математика не всегда является легкой прогулкой! Дерзайте, и откроется вам!)

Обратной операцией к $A \oplus B$ не является $A \ominus B$.

> Итак, разность по Минковскому не является обратной операцией к сумме по Минковскому. К сумме по Минковскому обратной операции нет.

Операция $A \oplus B$ не превращает множество всех подмножеств целых чисел в группу по сложению.

* * *

А теперь мы «поиграем в математику всерьез». Сейчас я сформулирую глубоко нетривиальное утверждение.

Лемма

Пусть P — непустое множество целых чисел ($P \subset \mathbb{Z}$; $P \neq \varnothing$), такое, что разность по Минковскому этого множества с самим собой помещается внутри самого этого множества ($P \ominus P \subset P$). Тогда либо P состоит только из числа 0, либо существует такое натуральное число d, что P состоит ровно из тех целых чисел, которые делятся на это число d ($P = d\mathbb{Z}$): $\{\ldots -3d, -2d, -d, 0, d, 2d, 3d, \ldots\}$.

Кстати, а почему мы исключили из рассмотрения случай, когда P равно пустому множеству? Потому что сумма по Минковскому пустого множества с любым подмножеством (A) равна пустому множеству:

$$\varnothing \oplus A = \varnothing.$$

И в самом деле, откуда здесь могли бы взяться элементы? Нельзя образовать ни одной суммы с каким бы то ни было элементом из пустого множества, ибо в пустом множестве элементов нет (невозможно взять из пустого множества элемент). Значит, по определению, в правой части равенства стоит пустое множество.

Так что, говоря о сумме Минковского, мы в дальнейшем по умолчанию будем иметь в виду, что мы суммируем только НЕПУСТЫЕ подмножества.

Заметьте, как внезапно у нас возникла операция умножения — как черт из табакерки! Вроде рассматривали только сложение и вычитание (ну, по Минковскому), в лемме тоже никакого умножения не было, по крайней мере в условии. И на тебе! А все почему? А все потому, что:

> умножение — это многократное сложение!

Если сложить d с самим собой, получится $2d$; если сложить $2d$ с d, получится $3d$; то же самое со всеми $-d$ и т. д. Получается копия целых чисел, увеличенная по интервалу в d раз — разреженные целые числа. В них тоже можно складывать и вычитать по всем правилам обычных целых чисел: сумма или разность кратных d есть кратное d; в качестве результата умножения или деления на 0 присутствует 0; числа, противоположные положительным, кратным d, тоже кратны d.

Словом, это вариант представления целых чисел, только более разреженный.

И такие ситуации, когда внутри подмножества группы можно выполнять групповую операцию и обратную к ней — без выхода за пределы подмножества, определяются словом **«подгруппа»**. И то, что мы только что рассматривали, — это пример **подгруппы целых чисел**, имеющей здесь вид «все числа, кратные d»:

$$d,\ 2d,\ 3d,\ \ldots\ .$$

Утверждается, что других подгрупп в группе целых чисел не бывает. (Кстати: случай, когда P состоит только из одного нуля, формально может быть получен при $d = 0$. Поэтому (но не только поэтому!) зачастую число 0 также причисляют к натуральным числам).

Давайте раскроем, почему разность по Минковскому содержит более детальную информацию, чем если бы было написано «сумма по Минковскому лежит в P». Замена $\ominus$ на $\oplus$ делает утверждение леммы неверным. Например, можно заметить, что «натуральные числа плюс натуральные числа лежат внутри натуральных чисел». Но множество натураль-

ных чисел не является множеством всех кратных какого бы то ни было натурального числа, так как оно не содержит его отрицательных кратных.

А вот если использовать операцию $\ominus$, тогда натуральные числа уже не будут удовлетворять нашему уравнению на подмножества: $P \ominus P \subset P$.

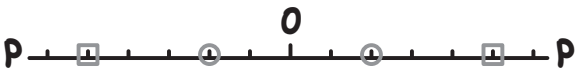
Приступим теперь к строгому доказательству нашей леммы:

1. Раз мы предположили, что P — это не пустое множество, то какое-то s (целое число) принадлежит P. Тогда 0 (а это ведь $s - s$) тоже обязан принадлежать P. И $-s$ (как $0 - s$) тоже обязан принадлежать P.

   Пусть $s \in P$.

   Тогда $0 = s - s \in P$, $-s = 0 - s \in P$.

   То есть если подмножество P содержит хотя бы один элемент (а это верно по предположению леммы), то 0 тоже должен быть там, потому что мы можем взять разность этого элемента с самим собой. А раз есть 0, то есть и противоположный элемент для любого элемента, входящего в P (см. выше обоснование). Значит, P является «двусторонним» множеством на нашей шкале — симметричным, расположенным по обе стороны от точки 0. То есть это множество включает 0, а также, возможно, какие-то еще пары противоположных друг другу чисел.



   Теперь нужно доказать, что на самом деле все множество P — это множество всех кратных какого-то одного числа.

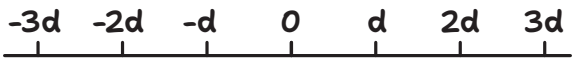
Надо рассмотреть два возможных случая:

а) ничего, кроме 0, в P нет. То, что 0 обязательно есть, мы уже доказали. Но предположим, что есть *только* 0. И тогда понятно, что $0 - 0 = 0$. То есть такое множество P, которое состоит из одного числа, и это число — 0, удовлетворяет нашему уравнению, но, с другой стороны, оно и выглядит как $0 \cdot \mathbb{Z}$ — все числа, кратные нулю (Sic!).

Этот случай неинтересный, поэтому предположим, что

б) P содержит хотя бы один ненулевой элемент. Если это так, то есть хотя бы один положительный элемент (и, по определению, противоположный к нему — отрицательный). И тогда пусть d — минимальный положительный элемент P.

Берем теперь два числа из P : 0 и d и вычитаем друг из друга: $0 - d \in P$, т. е. $-d \in P$. Далее: $(-d) - d = -2d \in P$, и так далее: все отрицательные числа, кратные d, лежат в P, в силу условия $P \ominus P \subset P$. Однако и все положительные числа, кратные d, тоже лежат в P, ибо например, $6d = 0 - (-(-6d))$, где $0 \in P$ и $(-6d) \in P$.



Таким образом мы установили, что вместе с нашим $d \in P$ все кратные $m \cdot d$ лежат в P, как положительные, так и отрицательные.

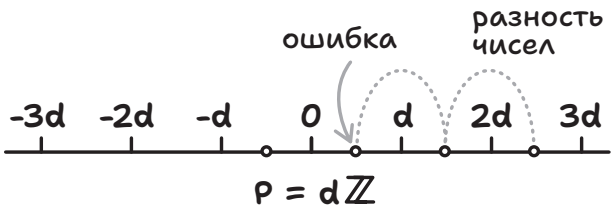
Утверждение:

Если d является минимальным положительным числом множества P, то в множестве P нет элементов, не кратных d.

Доказательство:

Предположим, что это утверждение неверно: пусть во множество P «закрался» некий элемент, который не является кратным числа d. Тогда на нашей шкале он размещается строго между двумя соседними кратными.

Но тогда по условию $P \ominus P \subset P$ разность между этим элементом и d должна принадлежать множеству P (раз и этот элемент, и d принадлежат множеству P). И далее так же: разность между следующим «закравшимся» элементом и следующим кратным d тоже принадлежит множеству P.



Рассуждая таким образом, мы шаг за шагом в конце концов «загоним» очередной элемент из множества P строго внутрь интервала между точками 0 и d. А вот это уже ошибка, противоречие! Этого не может быть, так как по условию в ка-

честве d был выбран именно минимальный положительный элемент из P.

Следовательно, никакого «лишнего» — некратного d — элемента (числа) в P не может быть. Утверждение доказано:

$$P = d\mathbb{Z}.$$

Это значит, что

> любое подмножество P целых чисел, для которого разность по Минковскому $P \ominus P$ лежит внутри P, обязательно имеет вид $d\mathbb{Z}$. И обратно: любое множество вида $d\mathbb{Z}$, конечно, тоже удовлетворяет условию $P \ominus P \subset P$.

Фактически мы получили описание подгрупп: все подгруппы целых чисел описаны и все они имеют вид $d\mathbb{Z}$, то есть разреженных чисел (и еще есть нулевая подгруппа, в которой имеется всего одно число — 0).

Это ключевое утверждение, и теперь дальше на основании доказанной леммы мы сможем выводить множество следствий. Фактически мы здесь обошли стороной стандартный прием, который называется **«алгоритм Евклида»***.

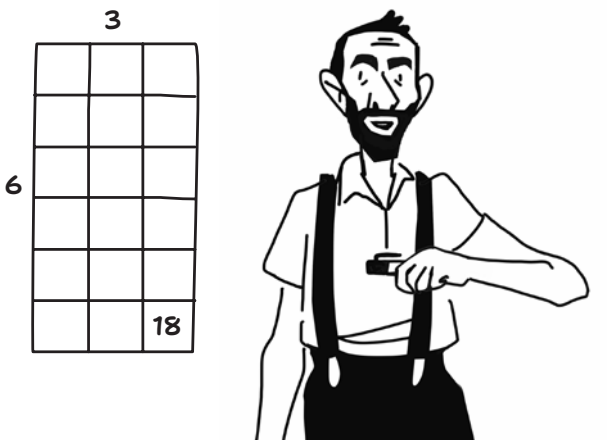
* * *

Получив кратные, мы получаем доступ к **операции умножения**.

---

* Алгоритм Евклида — эффективный алгоритм для нахождения наибольшего общего делителя двух целых чисел (или общей меры двух отрезков). Один из старейших численных алгоритмов, используемых в наше время. Впервые описан греческим математиком Евклидом (III век до н. э.).

Что значит «умножить»? Если взять, например, произведение чисел 3 и 6, то визуально это площадь прямоугольника, состоящая из 18 клеточек (их легко посчитать): 3 — по ширине и 6 — по высоте.



Операция, противоположная умножению, называется **делением**. О свойствах умножения и деления — в следующем разделе.

14. УМНОЖЕНИЕ И ДЕЛЕНИЕ

Кольцо

Посмотрите на формулу, связывающую умножение и сложение.

$$a(b + c) = ab + ac.$$

Это основное правило, связывающее операцию умножения с операцией сложения. Множество с двумя основными операциями — «плюс» и «умножить» — называется кольцом в том случае, если, во-первых, относительно сложения оно является абелевой группой, и, во-вторых, если всегда выполняется только что приведенное правило, связывающее сложение и умножение.

Если не предъявлять больше никаких требований, то можно считать, что это самое абстрактное кольцо. Но обычно умножение удовлетворяет еще каким-либо свойствам, например **ассоциативности**:

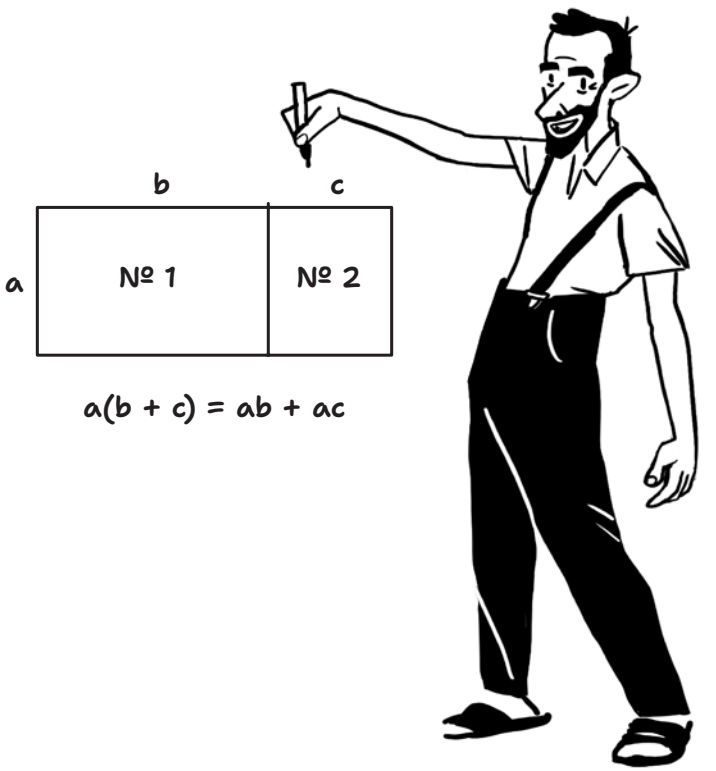
$$(ab)c = a(bc).$$

Вопрос:

Почему во множестве целых чисел всегда выполняется соотношение $a(b + c) = ab + ac$?

Ответ:

Если нарисовать прямоугольник шириной $(b + c)$ и высотой a, то в его площадь — $a(b + c)$ — будут входить площади двух меньших прямоугольников: № 1 и № 2.



Визуально очевидно:

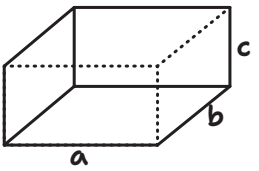
> если фигура составлена из двух фигур, которые соприкасаются общей границей, то суммарная площадь этих двух фигур равна площади всей фигуры.

Поэтому равенство $a(b + c) = ab + bc$ верно (ну, как минимум для положительных чисел, а проверка для отрицательных сводится к набору технических соглашений). Это правило называется **законом дистрибутивности умножения относительно сложения**.

* * *

Равенство $(ab)c = a(bc)$ тоже можно объяснить красиво.

Надо нарисовать прямоугольный параллелепипед и вычислить его объем двумя различными способами. С одной стороны объем равен произведению площади нижней грани (основания, ab) на длину вертикального ребра (то есть на высоту, c), а с другой стороны он же равен произведению длины ребра основания (a) на площадь боковой грани (bc). Каким способом объем ни считай, получится одно и то же.



(ab)c = a(bc)

Кстати, в таких рассуждениях нам помогает некая интуиция, связанная с пространством. Ее полезно нарабатывать с очень раннего возраста, обращаясь к визуальным образам чисел, множеств и т. д.

Умножение на 1

> При умножении 1 на любое число получается то же самое число.

$$1 \cdot a = a \cdot 1 = a.$$

При этом в целых числах ($\mathbb{Z}$) не всегда есть такое b, что $a \cdot b = 1$. Более того, на самом деле его почти никогда нет: оно есть только при $a = 1$ (тогда $b = 1$) или при $a = -1$ (тогда $b = -1$). То есть взять обратное в целых числах нельзя почти никогда. Но все-таки уравнение $ax = b = xa$ иногда разрешимо и в том случае, когда a и b отличны от 1. В этом случае мы говорим, что b делится без остатка на a (и обозначаем этот факт так: $b \vdots a$).

Иными словами,

> b делится на a тогда и только тогда, когда существует такое c, что b равно ac.

$$b \vdots a \Leftrightarrow \exists\ c \text{ такой, что } b = ac.$$

Это соотношение называется **делимостью чисел**. Из свойств отношения делимости мы сможем вывести целый ряд утверждений (см. далее).

Почему нельзя делить на 0?

В самом начале книги, в разделе «Почему нельзя делить на ноль», приведены два способа рассуждений о том, почему 1 не делится на 0. Здесь мы дополним второе, математическое рассуждение до степени абсолютной строгости!

А именно, утверждение «1 делится на 0» эквивалентно утверждению, что существует такое c, что $1 = 0 \cdot c$.

$$1 \vdots 0 \Leftrightarrow \exists\ c \text{ такой, что } 1 = 0 \cdot c.$$

Но площадь прямоугольника, у которого одна из сторон равна 0, будет всегда равна 0!

А почему, спросите вы, произведение любого числа на ноль равно нулю? Докажем и это:

$$0 \cdot c = (0 - 0)c = 0c - 0c = 0.$$

Чему бы ни было равно $0 \cdot c$, мы из этого числа вычли его же самого. Получили, конечно, 0. Суммируем наши формальные изыскания:

> Если бы 1 делился на 0, это бы означало, что существует такое число c, что 1 был бы равен произведению 0 и этого числа c. Но 0 при умножении на любое число дает 0.

Словом, 1 был бы равен 0, но в целых числах это, естественно, не так,

$$1 \neq 0.$$

* * *

Прибавим к аксиомам, обозначенным выше, еще одну: $ab = ba$ (справедливую для целых чисел).

Теперь у нас полный набор аксиом:

$$a(b + c) = ab + ac;$$

$$(ab)c = a(bc);$$

$$1 \cdot a = a \cdot 1 = a;$$

$$ab = ba.$$

Если для элементов некоторой абелевой (относительно сложения) группы определена еще одна операция — умножение, и дополнительно выполнен весь этот набор аксиом, то мы говорим, что наша абелева группа образует кольцо — коммутативное, ассоциативное и с единицей.

А если к тому же можно найти обратный элемент для любого ненулевого элемента нашего кольца (в целых числах это не так!), то мы говорим, что имеем дело с полем. (Обратного числа для 0 не существует, о чем мы только что долго рассуждали.) В поле все ненулевые элементы образуют группу по умножению.

Суммируем вышесказанное. В поле есть две операции:

1) операция «плюс». Поле образует группу относительно «плюса» — **группу по сложению**;
2) операция «умножить». Все элементы поля, за исключением нуля, образуют группу по умножению;

3) выполняется свойство дистрибутивности умножения относительно сложения:

$$a(b + c) = ab + ac.$$

Что такое простое число?

Целые числа не образуют поля, а лишь образуют кольцо. В кольцах, как правило, наиболее сложная и богатая арифметика, а предмет науки арифметики как раз и составляет исследование свойств отношения делимости. Первейшим и наиболее фундаментальным с точки зрения делимости понятием является понятие простого числа. Мы дадим определение в терминах натуральных чисел, как обычно в школе.

Число, большее или равное двум, называется простым в том случае, если оно делится только на себя и на 1.

Ну а на 1 и на себя оно делится строго по определению:

$$p = p \cdot 1$$

отвечает двум условиям утверждения

$$b \vdots a \Leftrightarrow \exists\, c : b = ac:$$

- p делится на p, так как существует c, равное 1, при умножении на p дающее p;
- p делится на 1, так как существует c, равное p, при умножении на 1 дающее p.

Если у числа p других делителей, кроме p и 1, нет, то p — простое число. Заметим, что при рассмотрении арифметики целых чисел надо добавить к делителям p еще два делителя: (-1) и $(-p)$. Но это уже детали!

* * *

Вопрос о том, какие делители есть у произвольного числа n, является интересным и чрезвычайно красивым. На первый взгляд кажется, что этот вопрос сложный. Но на самом деле он сводится к вопросу о разложении числа n в произведение простых чисел, и в конце концов выводит нас на Основную теорему арифметики (ОТА).

Если бы мы спросили: **«Какие числа делятся на n?»**, то ответ был бы очевиден: числа вида $n\mathbb{Z}$ — все кратные n (подгруппа целых чисел, которые делятся на n).

А вот вопрос о делителях числа n — более деликатный. Его мы и рассмотрим в следующем разделе!

15. ДЕЛИТЕЛИ НАТУРАЛЬНЫХ ЧИСЕЛ

В разделе «Построение умножения» мы обсудили, что все кратные числá d мы обозначаем как $d\mathbb{Z}$ и называем **подгруппой в группе целых чисел по сложению,** то есть любые два числа, которые кратны d, в сумме дают число, также кратное d, и разность двух чисел, кратных d, тоже делится на d.

Теорема: если непустое подмножество P всех целых чисел таково, что разность по Минковскому ($P \ominus P$) лежит внутри P, то P обязательно имеет вид $d\mathbb{Z}$.

* * *

И теперь перед нами стоит следующий вопрос: давайте найдем для данного числа n все такие d, при которых будет верно, что n делится на d. То есть мы рассмотрим произвольное натуральное число n и увидим, в какие множества вида $d\mathbb{Z}$ оно попадает (если n попадает в такое множество, значит, n является кратным числа d.

Вопрос нахождения делителей числа n появляется очень во многих задачах математики, даже в обычной жизни порой требуется выяснить, какие у числа есть делители. Так что

полезно уметь их находить. Вопрос не из самых тривиальных, и мы рассмотрим одну олимпиадную задачку, которую однажды задали на игре «Форт “Боярд” математиков» (в которой участвовал и автор).

Учимся определять количество делителей числа, или Задача «О шкафчиках и дверцах» (начало)

Условие:

- В детском саду 100 детей, у каждого — собственный шкафчик с индивидуальным номером, и все номера из набора: 1, 2, 3, ..., 100. Каждый ребенок встает рядом со своим шкафчиком.
- По *1-му* свистку *ВСЕ дети* дружно открывают дверцы своих шкафчиков.
- По *2-му* свистку дети, стоящие через одного, начиная со 2-го (*каждый четный* ребенок), свои дверцы захлопывают.
- По *3-му* свистку положение дверок *каждого 3-го* шкафчика (3-й, 6-й, 9-й и т. д. — до 99-го) меняется на противоположное (открытые — закрывают, а закрытые — открывают).
- По *4-му* свистку меняется положение дверцы *каждого 4-го* шкафчика, по 5-му — 5-го и т. д.: по свистку k меняют положение дверцы шкафов под номерами, кратными k.

Вопрос: какие шкафчики в итоге останутся открытыми?

Решение:

1. *По 1-му свистку* меняют состояние все шкафчики (потому что это множество всех чисел, кратных 1). Запишем этот факт с использованием теоретико-множественной терминологии, согласно которой знак ∩ обозначает пересечение двух множеств: множества всех целых чисел $\mathbb{Z}$ и множества натуральных чисел в диапазоне от 1 до 100:

$$1)\ \mathbb{Z} \cap \{1, 2, 3, \ldots 100\}.$$

2. *По 2-му свистку* меняют свое состояние все шкафчики с номерами, кратными 2 (то есть пересечение множества $2\mathbb{Z}$ со множеством всех чисел от 1 до 100):

$$2)\ (2\mathbb{Z}) \cap \{1, 2, 3, \ldots 100\}.$$

3. ...
4. По свистку с любым порядковым номером k меняют свое состояние все шкафчики с номерами, кратными k, то есть пересечение множества $k\mathbb{Z}$ со множеством всех чисел от 1 до 100:

$$k)\ (k\mathbb{Z}) \cap \{1, 2, 3, \ldots 100\}.$$

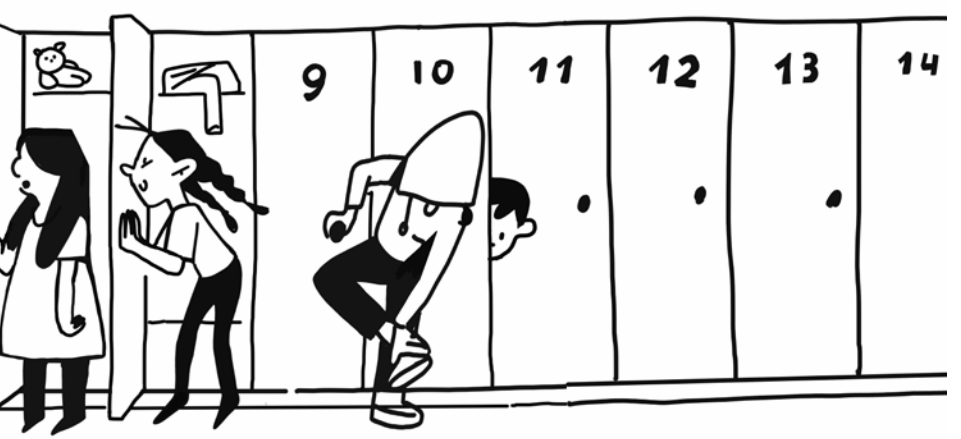
5. Последний свисток — 100-й, по 100-му свистку меняет состояние только 100-й шкафчик.

Очевидно, что по звонкам с номерами от 51-го по 99-й меняет положение дверок каждый раз только один шкафчик, а именно шкафчик с номером, совпадающим с номером звонка. В самом деле, следующее число, кратное номеру звонка, уже не попадает в диапазон от 1 до 100, и шкафчика с таким номером просто не существует.

Итак, эта странная волна открывания и закрывания дверей прошла, и в нашей задаче требуется найти, **какие шкафчики в итоге останутся открытыми**.

Давайте рассуждать...

В какой момент дверца меняет положение? В момент, когда свистят в свисток под таким номером, что номер шкафчика кратен номеру свистка (грубо говоря, *номер шкафчика делится на номер свистка*). Это очевидно из $(k\mathbb{Z}) \cap \{1, 2, 3, \ldots 100\}$.



При этом дверцы, которые в итоге остались открытыми, меняли свое положение нечетное количество раз (открылись-закрылись — четное количество действий; открылись и остались открытыми — нечетное).

Соответственно нужно понять, **у каких натуральных чисел нечетное количество делителей**.

Теперь отвлечемся от дверок, шкафчиков и свистков, ведь сначала хорошо бы разобраться с тем, **какие делители у каких натуральных чисел есть**, то есть нам надо научиться **находить делители числа**.

Для примера давайте узнаем: четное количество делителей или нечетное у числа 100.

«Банально-брутальный» подход к поиску делителей числа 100 состоит в том, чтобы перебрать все числа подряд от 1 до 99, проверяя, на какие из них делится число 100. Но это бессмысленно долго!

> Математика — наука ленивых людей, тех, кто хочет экономить время и знает как.

Подсказка: **достаточно проверять делимость только на простые числа**, ибо если 100 делится на a, и a — не простое число, то у a всегда есть какой-то простой делитель p, из чего будет следовать, что и 100 делится на это p — согласно основному принципу делимости, который я сформулирую в виде мема

> Делитель моего делителя — мой делитель! (Ибо делители — это вам не вассалы!)

Доказать наличие у составного числа a простого делителя легко. Разложим a в произведение двух множителей. Если среди них сразу обнаружится простое число, то вот мы уже и доказали наличие у a простого делителя.

Если же сразу простого делителя не обнаружится, то будем теперь раскладывать на множители уже делители первоначального числа a, помня о главном меме: **Делитель моего делителя — мой делитель!**

Ясно, что бесконечно раскладывать на множители положительное целое число мы не можем: в итоге все равно «упремся» в простые числа. А значит, у каждого числа всегда найдется какой-то простой делитель.

Кстати, математически строгая формулировка моего мема звучит следующим образом (для «прошаренных» читателей добавлю: она выражает транзитивность отношения делимости):

> Если некое число a делится на b, а b делится на c, то a делится на c.

$$a \vdots b,\ b \vdots c \Rightarrow a \vdots c.$$

Итак, перед тем как найти все делители числа 100, перечислим все его простые делители, а потом подумаем, что это нам даст.

Разложим число 100 в произведение простых чисел:

$$100 = 2 \cdot 50 = 2 \cdot 2 \cdot 25 = 2^2 \cdot 5^2.$$

С помощью этого разложения мы теперь легко перечислим все (не только простые!) делители числа 100. Кажется оче-

видным, что любой делитель числа 100 имеет вид: 2 в некоторой степени умножить на 5 в некоторой степени:

$$2^a \cdot 5^b.$$

Здесь a — либо 0, либо 1, либо 2; и b — либо 0, либо 1, либо 2.

Но есть проблема! Последний вывод, на самом деле, неявно подразумевает верность двух утверждений. Первое из них состоит в том, что никакие другие простые числа не могут быть делителями числа 100. (Второе утверждение более тонкое и касается степеней простых чисел 2 и 5, входящих в разложение делителей числа 100. К нему мы впоследствии вернемся.) Итак, почему бы числу 100 не иметь каких-то других простых делителей? Потому что если б это было так, то тогда бы мы получили совершенно иной способ разложить число 100 на множители:

$$100 = 2^a \cdot 5^b = 11 \cdot m.$$

В 5–6 классе школы свойство всех чисел иметь единственное уникальное разложение в произведение простых множителей объявляется общим правилом, неким законом, справедливость которого школьникам не обосновывают. Мол, вот вам разложение на простые, и все тут. Однако, как бы странно это ни выглядело, но правило однозначного разложения на множители совершенно не очевидно! Его необходимо строго доказывать. В следующем разделе книги мы этим и займемся, а пока сформулируем соответствующую теорему — **основную теорему арифметики (ОТА)**:

> Любое натуральное число, начиная с числа 2 и далее, единственным образом записывается в виде произведения простых множителей,

либо, если мы сгруппируем его в уже знакомой нам форме $2^a \cdot 5^b$, то можно сформулировать ОТА в другой, эквивалентной ей форме. А именно: любое натуральное число, начиная с числа 2 и дальше, единственным образом раскладывается в произведение нескольких чисел, каждое из которых является определенной степенью какого-то простого числа, и на этот раз уже все простые числа выбираются разными.

Важно, что в обоих формулировках ОТА речь идет именно о разложении в произведение простых множителей (либо их степеней — во второй формулировке), иначе теорема, очевидно, была бы неверна. Например, имеют место вот такие два разных разложения числа 100 в произведение двух множителей:

$$100 = 10 \cdot 10 \text{ и } 100 = 2 \cdot 50.$$

Оба равенства верные, но это не противоречит ОТА, а просто мы еще «не завершили» процесс разложения на множители. И в первом выражении, и во втором равенстве можно продолжить раскладывать, доходя до простых чисел, и в конце концов оба разложения будут отличаться лишь порядком полученных простых множителей (перестановка множителей, конечно, результата не меняет):

$$10 \cdot 10 = (2 \cdot 5) \cdot (2 \cdot 5) = 100 = 2 \cdot 50 = 2 \cdot (2 \cdot 5) \cdot 5.$$

В этом, собственно, и состоит суть *основной теоремы арифметики*. Далее она нам потребуется в качестве инструмента для решения задачи «О шкафчиках и дверцах», но предварительно нам придется ее доказать. Вообще все, что мы используем, мы будем доказывать.

16. ОСНОВНАЯ ТЕОРЕМА АРИФМЕТИКИ (ОТА)

Итак, мы приступаем к доказательству **основной теоремы арифметики**, формулировку которой воспроизведем здесь еще раз:

> Любое натуральное число, начиная с числа 2 и далее, единственным образом записывается в виде произведения простых множителей.

При этом нужно помнить про правило перестановки: $2 \cdot 5 \cdot 2 \cdot 2$ и $2 \cdot 2 \cdot 2 \cdot 5$ — это, разумеется, одно и то же разложение на множители, а не два различных.

Чтобы доказать ОТА, нужна подготовительная работа, которую мы уже начали в предыдущих разделах.

Давайте припомним доказанную в разделе 13 лемму:

$$P \ominus P \subset P \Rightarrow P = d\mathbb{Z},$$

что значит:

> если при вычитании по Минковскому из некоторого множества его же самого получается результат, лежащий внутри этого же множества, то рассматриваемое

> множество состоит из всех кратных некоторого целого неотрицательного числа d (возможно, равного 0 или 1).

Как мы договорились ранее, подмножества, которые мы рассматриваем, — **не пустые**.

* * *

Теперь изучим некоторую конструкцию.

- Рассмотрим два различных (строго говоря, это необязательно, но в случае одинаковых не получится ничего интересного!) натуральных числа a и b и рассмотрим два множества — всех кратных первого из них ($a\mathbb{Z}$) и всех кратных второго ($b\mathbb{Z}$).
- Сложим их друг с другом по Минковскому и полученное множество обозначим буквой P:

$$a\mathbb{Z} \oplus b\mathbb{Z} = P.$$

Утверждение заключается в том, что множество P удовлетворяет нашей лемме $P \ominus P \subset P \Rightarrow P = d\mathbb{Z}$.

Доказательство:

Давайте убедимся, что разность двух элементов, каждый из которых лежит в P, оказывается также внутри P ($P \ominus P \subset P$).

1. Каждый элемент из множества P имеет вид: какое-то число, кратное a, плюс какое-то число, кратное b. Один элемент может быть таким: $ax + by$; другой — таким: $ax' + by'$.
2. Разность этих элементов имеет вид:

   $$a(x - x') + b(y - y'),$$

   и, естественно, это снова элемент из $a\mathbb{Z} \oplus b\mathbb{Z} = P$: $a(x - x')$ — это кратное числа a, так как получено умножением $x - x'$ на a; $b(y - y')$ — кратное числа b, так как получено умножением $y - y'$ на b.

   Таким образом мы убедились в том, что «P минус P» лежит в множестве P.
3. Отсюда следует, что сумма по Минковскому $a\mathbb{Z}$ и $b\mathbb{Z}$ равна $d\mathbb{Z}$:

   $$a\mathbb{Z} \oplus b\mathbb{Z} = d\mathbb{Z},$$

   то есть любое выражение, имеющее вид: «кратное a + кратное b», представляется в виде кратного некоторого положительного числа d. (Поймите сами, почему не может быть $d = 0$!) Заметим, что само d как элемент множества $a\mathbb{Z} \oplus b\mathbb{Z}$ тоже имеет вид: $ax + by$ (запомним это утверждение, далее оно нам пригодится).

* * *

По поводу нашего d мы установим два утверждения.

Утверждение 1:

> d является делителем как a, так и b.

Доказательство будет состоять из нескольких шагов:

1. Нам понадобится **вспомогательное Утверждение 1**:

   > Какое-то число l делится на какое-то число k в том и только том случае, когда $l\mathbb{Z}$ целиком лежит внутри $k\mathbb{Z}$:
   >
   > $$l \vdots k \Leftrightarrow l\mathbb{Z} \subset k\mathbb{Z}.$$

   Это совершенно очевидно, так как если l делится на k, значит, l — одно из кратных k. Следовательно, l лежит в этом множестве, так же как и любое кратное l. И наоборот: если $l\mathbb{Z}$ лежит внутри $k\mathbb{Z}$, то l лежит в $k\mathbb{Z}$ и, следовательно, l является кратным k. Такая «тавтологическая» переформулировка **свойства делимости** на языке подмножеств их включений нам сейчас пригодится. (Вам доставит удовольствие обратить внимание на то, что в выше приведенном рассуждении мы молчаливо воспользовались мемом про делители, то есть транзитивностью свойства делимости!)
2. Понятно, что $a\mathbb{Z}$ лежит в $a\mathbb{Z} \oplus b\mathbb{Z}$:

   $$a\mathbb{Z} \subset a\mathbb{Z} \oplus b\mathbb{Z},$$

   потому что во множестве $a\mathbb{Z}$ лежат числа, кратные a, в то время как в $a\mathbb{Z} \oplus b\mathbb{Z}$ — всевозможные суммы, состоящие из «кратное a плюс кратное b» (при этом справа за кратное b можно взять 0, и тогда справа будут получены все числа подмножества $a\mathbb{Z}$).

3. Так как

$$a\mathbb{Z} \oplus b\mathbb{Z} = d\mathbb{Z},$$

то это и означает, что $a\mathbb{Z}$ лежит внутри $d\mathbb{Z}$. Следовательно, a делится на d:

$$a\mathbb{Z} \subset d\mathbb{Z} \Rightarrow a \vdots d.$$

Аналогично и b делится на d:

$$b\mathbb{Z} \subset d\mathbb{Z} \Rightarrow b \vdots d.$$

Так мы установили, что число d, множество кратных которого совпадает с суммой по Минковскому $a\mathbb{Z} \oplus b\mathbb{Z}$, является делителем как a, так и b. Иначе говоря, d принадлежит множеству общих делителей (ОД) чисел a и b:

$$d \in \text{ОД}(a, b).$$

Утверждение 2:

> Число d — такой общий делитель чисел a и b, который делится на любой другой общий делитель,

из чего сразу следует, что d является наибольшим общим делителем (НОД). Ведь если будет установлено, что d делится на любой другой общий делитель, то он уже не сможет быть меньше любого другого: меньшее натуральное число не может делиться на большее. (Общие делители мы ищем только среди чисел натуральных; впрочем, все вышесказанное можно сформулировать и для целых чисел, если вместо «больше» говорить «больше по модулю».)

* * *

Докажем, что d не только общий делитель, но и что он делится на любой другой.

Доказательство № 1:

1. Пусть s тоже принадлежит множеству общих делителей чисел a и b, то есть является одним из делителей:

$$s \in \text{ОД}(a, b).$$

2. Тогда a делится на s и b тоже делится на s, то есть $a\mathbb{Z}$ лежит в $s\mathbb{Z}$ и $b\mathbb{Z}$ тоже лежит в $s\mathbb{Z}$.

   Но тогда и сумма по Минковскому $a\mathbb{Z} \oplus b\mathbb{Z}$ «попадает внутрь» $s\mathbb{Z}$ (ведь любой элемент из $a\mathbb{Z}$ и любой элемент из $b\mathbb{Z}$ оказываются кратными s, поэтому и их сумма тоже:

$$a\mathbb{Z} \subset s\mathbb{Z},\ b\mathbb{Z} \subset s\mathbb{Z} \Rightarrow a\mathbb{Z} \oplus b\mathbb{Z} \subset s\mathbb{Z}.$$

3. Но сумма по Минковскому $a\mathbb{Z} \oplus b\mathbb{Z}$ равна $d\mathbb{Z}$, поэтому мы фактически доказали, что $d\mathbb{Z}$ лежит в $s\mathbb{Z}$, а значит, d делится на s:

$$a\mathbb{Z} \oplus b\mathbb{Z} = d\mathbb{Z} \Rightarrow d\mathbb{Z} \subset s\mathbb{Z} \Rightarrow d \vdots s.$$

Доказательство № 2:

Как уже было упомянуто, само число d имеет вид $ax + by$. Остается отметить, что любой общий делитель чисел a и b делит как ax, так и by (вспомним мем!), следовательно, и их сумму тоже. А сумма как раз равна d!

Итоговое утверждение:

Для любых двух натуральных чисел a и b существует такое натуральное число d, которое:

> 1) представляется в виде $ax + by$ при некоторых x и y (то есть является целочисленной линейной комбинацией чисел a и b);

> 2) при этом является общим делителем чисел a и b;
>
> 3) делится на любой другой общий делитель чисел a и b, в частности является наибольшим общим делителем чисел a и b.

Проанализировав эти утверждения, мы заключаем, что

> наибольший общий делитель любых двух натуральных чисел представляется в виде их целочисленной линейной комбинации $ax + by$ (где сами x и y, в отличие от a и b, — целые числа; они могут быть, да и будут всегда, разных знаков. Исключение составляет «неинтересный» случай, когда одно из чисел, например a, делится нацело на другое — на b. Тогда их наибольший общий делитель d будет равен b, и в целочисленной линейной комбинации $d = b = ax + by$ будет выполнено $x = 0$, $y = 1$).

Именно это утверждение нам и понадобится для доказательства ОТА.

Итак, повторим и немного переформулируем, заменяя x и y на m и n соответственно — чтобы зафиксировать их на века:

Для любых двух натуральных чисел a и b существует натуральное число d, которое:

1) является НОД (наибольшим общим делителем) для чисел a и b;
2) делится на любой ОД (общий делитель) чисел a и b;
3) равно $am + bn$ (m и n — какие-то целые числа).

Это утверждение — путеводная звезда, которая приведет нас прямо к **основной теореме арифметики**.

Для подготовки к доказательству ОТА нам необходима еще одна лемма.

Лемма:

Пусть p — простое число*, а какие-то числа a и b не делятся на p. Тогда произведение a и b тоже не делится на p.

$$a, b \nmid p \Rightarrow ab \nmid p.$$

Обратите внимание: утверждение верно только для простых чисел (ведь если взять, к примеру, какое-то число m, не являющееся простым, равное произведению lk, то ни l, ни k, каждый будучи меньше m, не будут делиться на m, а их произведение, будучи как раз равным m, на m, естественно, делится!).

Теперь докажем лемму.

Доказательство:

1. Если a не делится на p, то НОД (a, p) равен 1, так как у p только два делителя (1 и p); при этом у a один из этих двух делителей точно отсутствует (а именно p).
2. Значит, среди всех «кандидатов» на то, чтобы быть общими делителями для a и для p, остается только 1. Соответственно, будучи НОД, 1 представляется в таком виде:

$$\text{НОД}\ (a, p) = 1 = d = am + pn.$$

---

* Напоминалочка: простое число — это число, которое делится только на себя и на 1 (в случае натуральных чисел), ну а за компанию еще и на −1 и на «минус себя» (среди всех целых чисел). 1 и −1 простыми не считаются. — *Примеч. А. С.*

3. Итак, если a не делится на какое-то простое число p, то тогда существуют два целых числа m и n — такие, что $am + pm = 1$.
4. Полученное равенство умножаем на b:

$$b = (ab)m + p(bn).$$

5. Обратим внимание, что число $p(bn)$ делится на p, и если бы было верно, что ab делится на p, то число b как сумма двух чисел, делящихся на p ($(ab)m + p(bn)$), тоже делилось бы на p.

А это неверно по условию, то есть ab не может делиться на p!

Утверждение, что

> произведение двух чисел, не делящихся на p, не может приобрести делимость на p,

доказано.

* * *

Все же эту лемму бывает тяжеловато понять — как школьникам, так и взрослым, поэтому сформулируем доказательство еще раз, но в сжатом виде.

Краткое доказательство:

Поскольку a и p взаимно просты, то суммой $am + pn$ можно представить число 1:

$$1 = am + pn.$$

1 — это НОД a и p (ранее мы доказали, что НОД любых чисел представляется в виде целочисленной линейной ком-

бинации $am + bn$, а в данном случае в виде этой комбинации представлено число 1).

Чтобы стало понятнее, для примера можно купюру с номиналом 1 рубль представить как разность: какое-то количество (m) купюр номиналом a рублей минус какое-то количество (n) купюр номиналом p рублей; или наоборот: какое-то количество (n) купюр номиналом p рублей минус какое-то количество (m) купюр номиналом a рублей. Утверждение о том, что можно представить число 1 в виде целочисленной линейной комбинации чисел a и p, является экономическим: требуется заплатить 1 рубль, используя несколько купюр достоинством a и несколько купюр достоинством p, причем достаточное количество купюр обоих достоинств есть и у продавца, и у покупателя (на самом деле в нашей ситуации, когда p — простое число и a на него не делится, можно заплатить любую сумму: достаточно несколько раз подряд с помощью нашей схемы заплатить 1 рубль).

Вернемся к математике. Теперь мы умножаем $am + pn = 1$ на b:

$$b = (ab)m + p(bn).$$

Если бы у нас ab делилось на p, то сумма двух чисел, делящихся на p, тоже должна была бы делиться на p. Но сумма как раз равна b! А b по условию не делится на p. Значит, наше предположение неверно, и произведение чисел a и b не может делиться на p.

Теперь у нас есть все что нужно, чтобы замахнуться на «великую и ужасную» — **основную теорему арифметики (ОТА)**.

Доказательство ОТА

Доказательство теоремы проведем способом (или приемом) «от противного».

1. Предположим, что существует число $n > 1$, которое умеет раскладываться на множители какими-то двумя способами:

$$n = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_e.$$

   Эти наборы простых чисел p и q отличаются друг от друга существенно, не просто перестановкой!

2. Давайте сократим в этих наборах все числа, которые совпадают (если таковые будут), после чего мы получим какое-то (новое) число — оно будет меньше, чем n (либо то же самое n, если совпадающих не найдется и сокращать будет не на что). Получившиеся после сокращения наборы (в них уже ничего сократить невозможно) будем представлять в виде чисел с тильдой.

$$\tilde{n} = \tilde{p}_1 \cdot \ldots \cdot \tilde{p}_s = \tilde{q}_1 \cdot \ldots \cdot \tilde{q}_v.$$

3. После сокращения должны возникнуть:

   1) некое существенное произведение простых чисел (как минимум одно простое число здесь должно быть);

   2) и какое-то другое произведение — тоже простых чисел, но совершенно иных.

То есть совершенно разные наборы простых чисел при перемножении дают одно и то же число.

Сейчас мы убедимся в том, что **это противоречит нашей лемме, потому что если два простых числа — разные, то ни одно из них на другое не делится** (помним: из определения простых чисел следует, что простые числа делятся только на себя и на 1). Следовательно:

1) $\tilde{p}_1 \nmid \tilde{q}_1$;

2) $\tilde{p}_2 \nmid \tilde{q}_1$;

3) ...;

4) и т. д. — вплоть до последнего: $\tilde{p}_s \nmid \tilde{q}_1$.

4. Применив лемму много-много раз, мы заключим, что произведение $\tilde{p}_1 \cdot ... \cdot \tilde{p}_s$ не может делиться на $\tilde{q}_1$.

Здесь сразу возникает **противоречие**: произведение $\tilde{p}_1 \cdot ... \cdot \tilde{p}_s$ — это в точности $\tilde{n}$, которое в силу записи $\tilde{n} = \tilde{q}_1 \cdot ... \cdot \tilde{q}_v$ как раз делится на $\tilde{q}_1$, так как оно равно $\tilde{q}_1$, умноженному на какое-то натуральное число.

Доказательство кратко:

1) $\tilde{n} = \tilde{p}_1 \cdot ... \cdot \tilde{p}_s = \tilde{q}_1 \cdot ... \cdot \tilde{q}_v$.

2) Если наборы пересекаются, то сокращаем максимально — и теперь это два совершенно разных набора — $\tilde{p}_1 \cdot ... \cdot \tilde{p}_s$ и $\tilde{q}_1 \cdot ... \cdot \tilde{q}_v$. Из набора с $\tilde{p}$ все простые числа не делятся на первое число из набора $\tilde{q}$, а значит, их произведение тоже не делятся на $\tilde{q}_1$, но произведение этих чисел равно $\tilde{n}$.

3) Значит, $\tilde{n}$ не делится на $\tilde{q}_1$.

4) И это прямо противоречит утверждению, что $\tilde{n}$ равно произведению $\tilde{q}_1$ на некое число, равное произведению остальных простых чисел из второго набора.

Это означает, что

> **никакое число не может раскладываться в произведение простых чисел по-разному!**

Основная теорема арифметики полностью доказана!

Эта важнейшая теорема будет всем читателям очень полезна в дальнейшем изучении математики, а мы с ее помощью «добьем» задачку «О шкафчиках и дверцах»!

17. ОПИСАНИЕ ВСЕХ ДЕЛИТЕЛЕЙ НАТУРАЛЬНОГО ЧИСЛА

Скажу сразу: описание делителей числа n — это одно удовольствие!

Начнем!

- Используя основную теорему арифметики (ОТА) разложим число n в то единственное произведение простых чисел, коим оно является.
- Сгруппируем простые делители числа n так, чтобы вначале шли одинаковые копии самого маленького из них (фактически это означает, что первое простое число возводится в некоторую степень), затем — одинаковые копии второго по величине простого делителя числа n, и так далее. Мы получим разложение:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}. \qquad (6)$$

Полученное нами разложение (6) для любого натурального числа, начиная с числа 2, будет единственным, строго фиксированным, его «личным» разложением в произведение групп возрастающих простых чисел в различных положительных степенях.

Как выглядят делители числа n?

Пусть $n = m \cdot l$.

Но m и l (каждый из них) тоже имеют свое уникальное, «личное» разложение на множители! Утверждение, которое я делаю сейчас, состоит в том, что на самом деле простые делители чисел m и l — те же самые, что и в наборе (6). Ска-

жем, для m мы должны будем иметь вот такое разложение в произведение групп простых делителей:

$$m = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_r^{\beta_r}. \qquad (7)$$

Единственное отличие состоит в том, что некоторые из показателей могут теперь быть нулевыми, и тогда соответствующий множитель (простое число в нулевой степени) нужно пропустить.

Почему это так? Потому что появление любого другого простого числа (не из набора (6)) в разложении числа m будет противоречить ОТА: из равенства $n = ml$ получается делимость числа n на это новое простое число, а из равенства (6) — нет. Противоречие с ОТА налицо, так как равенство $n = ml$ можно далее продолжить, и это простое число уже в нем не исчезнет.

При этом степени в (7) будут не выше, чем степени в (6): если бы какая-то степень простого числа в (7) была выше, чем степень того же числа в (6), то при сокращении равенства $n = ml$ на максимальную степень этого простого числа оказалось бы, что в левой части сокращенного равенства этого простого числа больше нет, а в правой оно есть, что снова противоречит ОТА.

Это именно то утверждение, которое мы упомянули, но не обсудили подробно в главе 15. Вернемся к примеру с числом 100. Почему не может быть делителя m числа 100, в который, например, входит простое число 5 в 3-й степени? Потому что тогда мы бы имели двойное равенство $100 = 2^2 \cdot 5^2 = ml = 5^3sl$, где $m = 5^3s$. Сокращая на 5^2, получаем $2^2 = 5s$, и это снова противоречит ОТА. (Конечно, в случае с числом 100 все и так очевидно, я лишь на его примере демонстрирую общий прием.)

Суммируем все вышесказанное. Описание делителей числа n, заданного в форме (6), очень простое:

$$\forall \text{ делитель числа } n \text{ — это } p_1^{\beta_i} \cdot \ldots \cdot p_r^{\beta_r},$$

где $0 \le \beta_i \le \alpha_i$.

Как это нам поможет перечислить все делители и посчитать их количество? Ответ состоит в том, что мы независимо выбираем степень для числа p_1 (любую — между 0 и α_1), потом независимо выбираем степень для числа p_2 (между 0 и α_2), как угодно их перемножаем, опять совершенно любым способом выбираем степень для p_3 и т. д. Получается...

Теорема:

Множество делителей $\mathbb{D}$ числа n есть произведение по Минковскому* нескольких подмножеств натуральных чисел.

$$\text{Множество делителей } \mathbb{D}(n) =$$
$$\left\{1, p_1, \ldots, p_1^{\alpha_1}\right\} \otimes \left\{1, p_2, \ldots, p_2^{\alpha_2}\right\} \otimes \ldots \otimes \left\{1, p_r, \ldots, p_r^{\alpha_r}\right\}.$$

Пример:

$$\mathbb{D}(600) = \{1, 2, 4, 8\} \times \{1, 3\} \times \{1, 5, 25\}.$$

---

* Произведение по Минковскому (так же как и сумма, и разность по Минковскому) определяется как множество всевозможных произведений. Если мы перемножаем несколько множеств по Минковскому, это значит, что мы рассматриваем множество всех результатов перемножения чисел из наших множеств — произвольно взятых по одному из каждого множества. — *Примеч. А. С.*

Согласно ОТА (теперь нам без нее никуда!), все такие произведения будут различны (будут давать различные числа), потому что различаются соответствующие наборы степеней простых множителей (то есть разложения на простые множители у любой пары делителей будут разными, следовательно, согласно ОТА, и сами эти делители обязаны быть разными). И значит, всевозможные попытки строить такие произведения приводят к нахождению разных делителей.

Теорема доказана!

Следствие:

- Количество элементов в множестве $|D(n)|$ (то есть число делителей числа n) равно произведению числа элементов во всех приведенных в теореме множествах.
- В самом первом множестве количество разных чисел — $\alpha_1 + 1$; в следующем — $(\alpha_2 + 1)$; и в последнем — $(\alpha_r + 1)$.

Итак, мы получили очень важную формулу. Теперь мы знаем, сколько делителей у числа, разложенного таким образом на множители. Это произведение следующего вида:

$$|D(n)| = (\alpha_1 + 1)(\alpha_2 + 1) \cdot \ldots \cdot (\alpha_r + 1).$$

Ну а нам пора вернуться к задачке «О шкафчиках и дверцах» из игры «Форт Боярд математиков».

Определение количества делителей — задача «О шкафчиках и дверцах» (продолжение)

Помните, мы определили, что остались открытыми те шкафчики, чьи номера суть чи́сла с нечетным числом делителей.

Вопрос: как в произведении многих разных чисел

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdot \ldots \cdot (\alpha_r + 1)$$

может получиться нечетное число?

Ответ: только одним способом: если каждое из чисел, которые мы перемножали, было нечетным. Если хотя бы один из множителей будет четным, то и произведение будет четным числом.

Поэтому нечетное количество делителей у числа n возможно только в том случае, когда нечетным будет каждое из чисел $(\alpha_1 + 1)$, $(\alpha_2 + 1)$, ..., $(\alpha_r + 1)$. А из этого следует, что числа α_1, α_2, ..., α_r, наоборот, — все четные.

Ну а это означает, что n является полным квадратом, так как он равен квадрату целого числа:

$$n = \left[p_1^{\frac{\alpha_1}{2}} \cdot p_2^{\frac{\alpha_2}{2}} \cdot \ldots \cdot p_r^{\frac{\alpha_r}{2}} \right]^2 .$$

При возведении в квадрат степени должны удваиваться, и так как степени все были четные, то мы смогли построить число, записанное внутри скобок этой формулы: оно будет целым и будет являться квадратным корнем из числа n.

* * *

Мы доказали следующее замечательное утверждение:

> Натуральное число имеет нечетное количество делителей тогда и только тогда, когда оно является полным квадратом.

Таким образом, мы можем дать **ответ на задачу «О шкафчиках и дверцах»**:

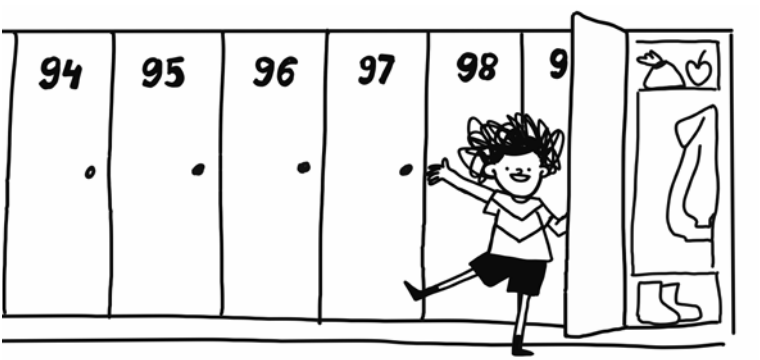
Шкафчики с номерами *1, 4, 9, 16, 25, 36, 49, 64, 81 и 100* будут открыты, а все остальные будут закрыты.

Задача «О шкафчиках и дверцах» решена!

Ниже, в главе 18, мы решим эту задачу более простым и прямым способом. Но тот долгий путь, который мы прошли, методологически более правильный, ибо ведет через описание множества делителей произвольного числа и задействует много других важных результатов школьной математики (в частности, ОТА)!

Итак, мы доказали **Основную теорему арифметики** и решили задачу «О шкафчиках и дверцах» на **определение количества и конкретного вида делителей произвольного натурального числа!**

И теперь нам предстоит двигаться вперед, извлекая из ОТА новые следствия.



18. СЛЕДСТВИЯ ИЗ ОТА

Для начала приведем **пример**. Обратимся все к тому же числу 100. Вспомним, каково его уникальное разложение на простые множители, точнее в произведение групп различных простых делителей в степенях?

$$100 = 2^2 \cdot 5^2.$$

И теперь мы знаем, что **это единственный способ разложения числа 100 на простые множители**, а значит, множество всех делителей числа 100 получается перемножением по Минковскому следующих двух наборов чисел:

$$\{1, 2, 4\} \otimes \{1, 5, 25\} = \{1, 2, 4, 5, 10, 20, 25, 50, 100\}.$$

1) Делители 1, 2, 4 последовательно умножим на 1, получим: 1, 2, 4;

2) потом умножим на 5, получим: 5, 10, 20;

3) и затем умножим на 25, получим: 25, 50, 100.

Это же можно компактно записать в табличку.

1	2	4
5	10	20
25	50	100

Мы видим, что множителей — 9: нечетное количество. Это полностью согласуется с тем, что из 100 без остатка извлекается квадратный корень:

$$\sqrt{100} = 10.$$

Ну и напоследок давайте разберем обещанное более «прямое» решение задачи «О *шкафчиках и дверцах*».

Задача «О шкафчиках и дверцах» (окончание) — короткое решение

1. Рассмотрим все делители числа n, перечислим их по возрастанию:

   $$n = \{1, ..., n\}.$$

   (если n — простое, то многоточия нет).
2. Каждому делителю сопоставим делитель такого вида:

   $$d \leftrightarrow n/d.$$

   Ясно, что это инволютивное отображение множества делителей в себя, то есть делителю n/d будет сопоставлен делитель $n/(n/d)$, то есть d (вернулись обратно к d!).

   Как сказал бы профессиональный математик, «если это отображение возвести в композиционный квадрат», то есть выполнить два раза подряд, то мы получим отображение, которое ничего не меняет.
3. Теперь посмотрим, какие делители каким соответствуют при этом отображении для числа 100:
   - делитель 1 переходит в 100;
   - делитель 2 — в 50;

- делитель 4 — в 25;
- делитель 5 — в 20.

4. А во что переходит 10?
   - 10 переходит само в себя!

   То, что число 10 переходит само в себя (ибо $10 = 100/10$), в точности отвечает тому факту, что 100 является полным квадратом: у числа 100 есть такой делитель, который переходит в себя. Все остальные делители разбиваются на пáры: «1 —100», «2 — 50», «4 — 24», «5 — 20».

   Таким образом, разбиение делителей на пары происходит в том и только том случае, когда число n не является квадратом целого числа, потому что в этом случае действительно ни один делитель не переходит в себя:

   разбиение на пары $\Leftrightarrow$ n — не квадрат целого числа.

5. И в этом случае (если n не является квадратом целого числа) у числа n будет четное число делителей, так как число делителей равняется тогда числу пар (целому!), умноженному на 2.
6. Ну а если n является квадратом, то все делители, кроме $\sqrt{n}$, имеют пару, не равную себе самому. А для делителя $\sqrt{n}$ парой является он сам. Поэтому общее количество делителей в этом случае окажется нечетным ($2k + 1$, где k — число пар).

Итак, если n — квадрат, то количество его делителей — нечетное; а если n не является квадратом, то количество делителей числа n — четное.

Ответ на задачу «О шкафчиках и дверцах»:

> Открытыми останутся шкафчики под номерами, являющимися точными квадратами.

Суммирование делителей числа

Теперь мы продолжим исследовать делители натуральных чисел и их свойства.

Давайте попробуем **сложить все делители** числа n. Функция $\sigma(n)$ — это сумма всех делителей натурального числа n:

$$\sigma(n) = \sum \text{всех делителей } n.$$

Для этой функции тоже можно выписать формулу, используя знакомый нам подход: если множество всех делителей — это произведение по Минковскому нескольких подмножеств, например, для числа 100 — все тех же {1, 2, 4} и {1, 5, 25}, то нельзя ли догадаться до какого-то простого выражения для суммы всех делителей рассматриваемого числа (100 или любого другого)?

Задача:

Чему равна сумма всех выражений вида $p_1^{\beta_1} \dots p_r^{\beta_r}$, когда показатели степеней различных простых делителей числа n независимо друг от друга пробегают диапазоны от нуля до показателя, с которым они входят в разложение числа n.

$$\sigma(n) = \sum p_1^{\beta_1} \dots p_r^{\beta_r}.$$

Решение:

Если мы возьмем сумму по всем наборам β такого вида, то она будет в точности равна произведению сумм выражений типа $p_1^{\beta_1}$ (где β_1 — от 0 до α_1), типа $p_2^{\beta_2}$ (где β_2 — от 0 до α_2) и т. д., и $p_r^{\beta_r}$ (где β_r — от 0 до α_r).

$$n = p_1^{\alpha_1} \dots p_r^{\alpha_r}, \ \sigma(n) = \left(\sum_{\beta_1=0}^{\alpha_1} p_1^{\beta_1} \right) \cdot \left(\sum_{\beta_2=0}^{\alpha_2} p_2^{\beta_2} \right) \dots \left(\sum_{\beta_r=0}^{\alpha_r} p_r^{\beta_r} \right). \quad (8)$$

После раскрытия скобок по законам школьной алгебры любое произведение таких групп даст какой-то делитель числа n, и все делители числа n по одному разу у нас появятся. (Напомню, что для обоснования последнего утверждения нам вновь нужно сослаться на ОТА!)

Знаете, есть такие утверждения, для которых справедливо выражение: «Это невозможно объяснить — это можно только понять!», и перед нами одно из них. Для того чтобы осознать этот прием, давайте проделаем всю операцию с числом 100 — и нам станет все понятно:

$$(1 + 2 + 4)(1 + 5 + 25) =$$
$$= 1 + 2 + 4 + 5 + 10 + 20 + 25 + 50 + 100.$$

Раскрыв скобки, мы действительно получили сумму всех делителей числа 100.

Прочувствовали всю красоту этого утверждения?!

Так что для любого n получается, что:

$$\sigma(n) = (1 + p_1 + \dots + p_1^{\alpha_1})(1 + p_2 + \dots + p_2^{\alpha_2}) \dots (1 + p_r + \dots + p_r^{\alpha_r}). \quad (9)$$

Это более «щадящая» запись того, что мы расписывали ранее в (8).

Вот такие замечательные функции у нас есть!

1) Количество делителей натурального числа n:

$$\sigma(n) = (1 + \alpha_1) \ldots (1 + \alpha_r)$$

и

2) сумма делителей числа n, равная произведению сумм подряд идущих степеней каждого простого делителя числа n, начиная от нулевой степени и заканчивая максимальной — той, с которой данный простой делитель входит в уникальное разложение для числа n согласно формуле (6). Сумма делителей задается формулами (8) и (9), которые представляют собой одно и то же выражение — в короткой и развернутой форме соответственно.

Дискретный логарифм по модулю простого числа

В качестве последней «вишенки на торте» давайте в нашей книге введем понятие дискретного логарифма числа n по модулю простого числа p.

$\mathrm{Ord}_p n$ — это та степень p, которая входит в разложение числа n.

Например, дискретный логарифм числа 100:

- по основанию 2 равен 2,
- по основанию 5 тоже равен 2,
- по основанию 11 равен 0 (потому что число 11 в разложение числа 100 не входит. В таком случае Ord просто равен 0).

Говоря о логарифме, мы должны проверить выполнение формулы:

$$\mathrm{Ord}_p(nm) = \mathrm{Ord}_p(n) + \mathrm{Ord}_p(m).$$

Разумеется, для установления этого закона нам снова потребуется ОТА! Я полагаю, что читатель, который смог дочитать до последней страницы, не сломавшись по пути, легко самостоятельно выведет справедливость этого соотношения: как и полагается логарифму, он переводит произведение чисел в сумму логарифмов этих чисел. Так что это довольно удачное обозначение, часто используемое в теории чисел!

Итак, все задачи, которые мы хотели решить в этой книге, решены, все утверждения доказаны!

На этом

маткульт-пока!

Алексей Савватеев

О математике с любовью. Маткульт-привет!

В оформлении обложки использовано фото Александра Беляева

Руководитель дивизиона	*А. Кривцов*
Ведущий редактор	*О. Морозова*
Художник	*М. Вахрушева*
Литературный редактор	*М. Зимина*
Корректоры	*Н. Быкова, Г. Шкатова*

Изготовлено в России. Изготовитель: ООО «Прогресс книга». Место нахождения и фактический адрес: 194044, Россия, г. Санкт-Петербург,Б. Сампсониевский пр., д. 29А, пом. 52. Тел.: +78127037373.

Дата изготовления: 05.2026. Наименование: книжная продукция. Срок годности: не ограничен.

Налоговая льгота — общероссийский классификатор продукции ОК 034-2014, 58.11.1 — Книги печатные.

Импортер в Беларусь: ООО «ПИТЕР М», 220020, РБ, г. Минск, ул. Тимирязева, д. 121/3, к. 214, тел./факс: 208 80 01.

Подписано в печать 08.04.26. Формат 60×90/16. Бумага офсетная. Усл. п. л. 12,000. Тираж 3000. Заказ 0000.

Роман Юдаев

ЗВЕЗДАНУЛО: ВЕСЕЛО И ДОСТУПНО ПРО ПРОБЛЕМЫ СОВРЕМЕННОЙ ФИЗИКИ И АСТРОНОМИИ

Автор понятным языком, с большой долей юмора разбирает проблемы современной физики. Объясняет, что такое черные дыры, изучает «генеалогическое древо» вещества, рассказывает историю возникновения квантовой физики (а вы знали, например, что кот Шрёдингера был призван опровергнуть положения квантовой механики, но в итоге сам стал ярким ее примером?).

Автор — энтузиаст физики, дотошный почемучка, и ему хочется видеть науку не только в формулах, но и в смыслах.

Это — долгожданная книга по подкасту «Звезданулo», в которой Роман Юдаев переводит науку на человеческий язык.