Содержание

0. Предисловие

Идеалом, конечно, являются просто
открытые для всех занятия по интересам,
где отбор осуществляется просто тем,
что более ленивые сами разбегутся.

А. Н. Колмогоров
о преподавании школьникам,
(из письма В. П. Эфроимсону,
опубликовал Оскар Шейнин)

Мы старались собрать задачи, которые традиционно решаются в «математических классах» (или, более официально, в «классах с углублённым изучением математики»). Сначала они довольно простые, но со временем доля сложных увеличивается. Некоторые более сложные (или не вполне по теме) задачи помечены звёздочками. В этом выпуске речь идёт об элементарной теории чисел (или, как раньше говорили, «высшей арифметике»).

Мы советуем сначала попробовать решить задачу, не глядя в решение. Если получится — сравнить с решением (там могут быть и дополнительные комментарии). Если долго не получается, тоже можно подглядеть в решение и попытаться понять его идею и довести до конца (ну или прочитать полностью и разобраться).

В 2023 году эти задачи выкладывались (порциями) в социальных сетях по частям; были выложены также и видеоразборы большинства задач (см. таблицу в конце предисловия) — в качестве образцов «живой математической речи», со всеми оговорками, ошибками, повторами и т. п. (как обычно бывает, устный язык заметно отличается от письменного).

В подготовке текстов и видео участвовали: Вадим Вологодский, Сергей Дориченко, Дмитрий Ицыксон, Руслан Ишкуватов, Александр Калмынин, Анна Кондратьева, Татьяна Михайлова, Арман Туганбаев, Михаил Финкельберг, Владимир Фок, Александр Шаповал, Александр Шень.

Чётность	https://youtu.be/_CInGfrzXqk https://youtu.be/L-mQWUrOvQs
дополнительные	https://youtu.be/WIsO_GZ2qqc https://youtu.be/fYs4zlJ4x94
Делимость	https://youtu.be/72AQnWsGR48
дополнительные	https://youtu.be/zX8xar3l5gs
Остатки	https://youtu.be/AfvD9wZNmus
дополнительные	https://youtu.be/T8T1KL-BLkI https://youtu.be/zfXun-cntK4
Арифметика остатков	https://youtu.be/1ZX_vMP1c48
дополнительные	https://youtu.be/5rmxnw6TMF8
Простые числа	https://youtu.be/n7jqV-KcAQk
дополнительные	https://youtu.be/iZrXbDRYOls
Алгоритм Евклида	https://youtu.be/85Tygvnt9f0
дополнительные	https://youtu.be/dHVSX7AKRJA https://youtu.be/uUl7hNj23RA
Алгоритм Евклида: следствия	https://youtu.be/lTF4j6ojbs4 https://youtu.be/L4xHU_gy1EM
дополнительные	https://youtu.be/KTz1fq_mfnU https://youtu.be/eyVoGceVpF8
Разложение на множители	https://youtu.be/2s9AtS5tbWk
дополнительные	https://youtu.be/zPbOrjO--jo
Малая теорема Ферма	https://youtu.be/IWSNAyIRQvc
дополнительные	https://youtu.be/Xu71tQJoE4c
Что дальше?	https://youtu.be/COySVGJdf6A https://youtu.be/prT20bir9KM

1. Чётные числа

Целые числа: $0, 1, 2, 3, \ldots, -1, -2, -3, \ldots$. Они бывают чётными и нечётными. Число n *чётное*, если оно равно $2m$ для некоторого целого m. Остальные числа называют *нечётными*.

• Можно сказать так: в мешке чётное число n яблок, если их можно поделить поровну (для педантов: не разрезая яблок; величина яблока не учитывается, важно только их количество) между двумя людьми. Или так: если можно разложить яблоки парами. Эти два способа соответствуют умножению m на 2 (две группы по m яблок) или 2 на m (m групп по два яблока). Ещё можно сказать так: n чётно, если $n/2$ целое — но для этого нужно уметь обращаться с дробями (и делить n на 2, даже если нацело не делится).

1.1 Будет ли число 123 чётным? Будет ли число 124 чётным?

▷ Поделим: $123/2 = 61\frac{1}{2}$, нацело не делится, 123 нечётно. А $124/2 = 62$, делится, значит, чётно. ◁

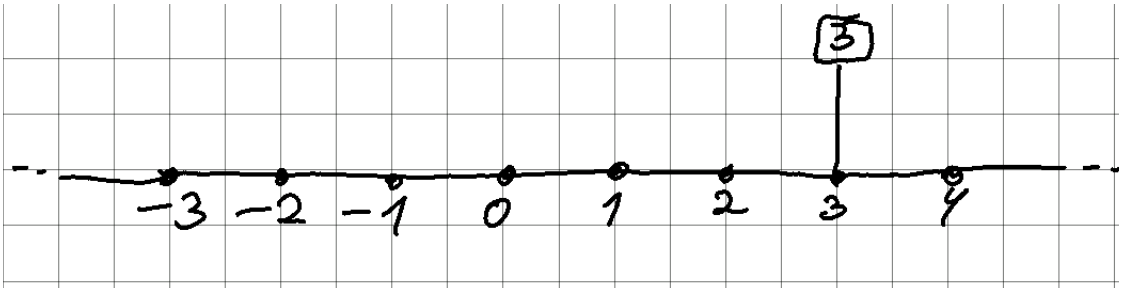
1.2 Будет ли нуль чётным числом, согласно нашему определению?

▷ Да, конечно: ведь $0 = 2 \cdot 0$, то есть $0 = 2k$ при $k = 0$, а число $k = 0$ целое. ◁

1.3 Сколько чётных среди двузначных чисел (от 10 до 99)? Кстати — а сколько всего двузначных чисел? Сколько чётных среди трёхзначных чисел (от 100 до 999)?

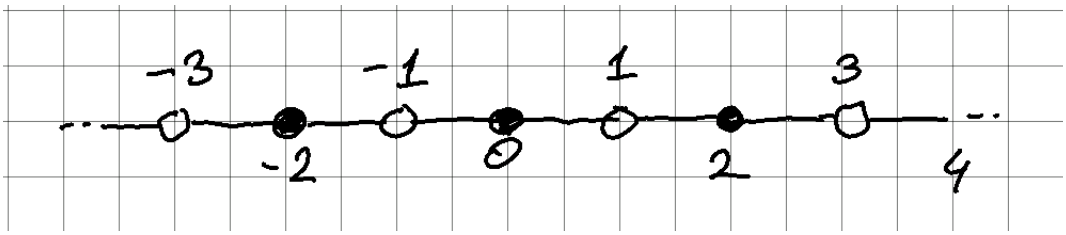
▷ Всего двузначных чисел 90. (Почему? Чисел от 1 до 99 будет, естественно, 99, из них нужно вычесть девять чисел от 1 до 9, которые не двузначные.) Чётные и нечётные числа чередуются и идут парами 10, 11 (одно чётное, другое нечётное), 12, 13 и так далее. Последняя пара 98, 99. Значит, чётных и нечётных поровну (столько же, сколько пар), то есть $90/2 = 45$. Для трёхзначных аналогичное рассуждение даёт ответ 450. ◁

Целые числа удобно изображать на числовой оси — можно представлять себе прямую дорогу с километровыми столбами. Отрицательные числа отмеряют в другую сторону



1.4 Отметьте чётные и нечётные числа на этом рисунке.

▷Они идут через одно (чередуются): между соседними чётными числами две единицы длины, и между соседними нечётными тоже.



◁

1.5 Будем выписывать положительные чётные числа в порядке возрастания: первое равно 2, второе 4, третье 6 и так далее. Чему равно 1000-е чётное число? Чему равно n-е (читается: «энное») чётное число?

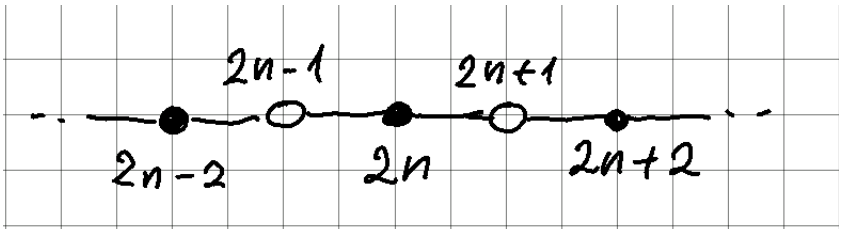
▷ Если мы считаем первым число 2, то каждое число будет вдвое больше своего номера (число увеличивается на 2, когда номер увеличивается на 1), так что тысячное число равно 2000, а n-е число равно $2n$. ◁

1.6 Те же вопросы для положительных *нечётных* чисел: первое равно 1, второе 3, третье 5 и так далее.

▷ По сравнению с чётными числами из предыдущей задачи эти (при том же номере) на единицу меньше, так что будет 1999 и $2n-1$. ◁

Из картинки видно, что чётные и нечётные числа чередуются. Значит, число $2n+1$, соседнее с чётным числом $2n$, будет нечётно. Наоборот, любое нечётное число можно записать как $2n+1$, потому что его сосед

слева чётный и его можно записать как $2n$. Получаем общую формулу: $2n$ для чётных чисел и $2n + 1$ для нечётных чисел.



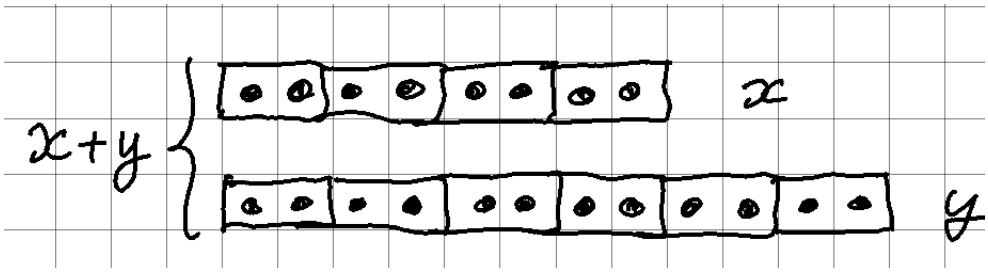
• На самом деле в этом рассуждении, если его проводить более строго, скрыто деление с остатком. Мы к этому ещё вернёмся.

1.7 Маша предлагает другую общую формулу для нечётных чисел: $2n - 1$? Права ли она?

▷ Да, конечно — только нумерация отличается на единицу (мы с этой формулой уже сталкивались). ◁

1.8 Всегда ли будет чётной сумма двух чётных чисел?

▷ Если в двух мешках по чётному числу камней, то можно разложить парами все камни из первого мешка, и отдельно все камни из второго мешка. Теперь можно объединить мешки — и все камни тоже разложены парами. Значит, их чётное число.



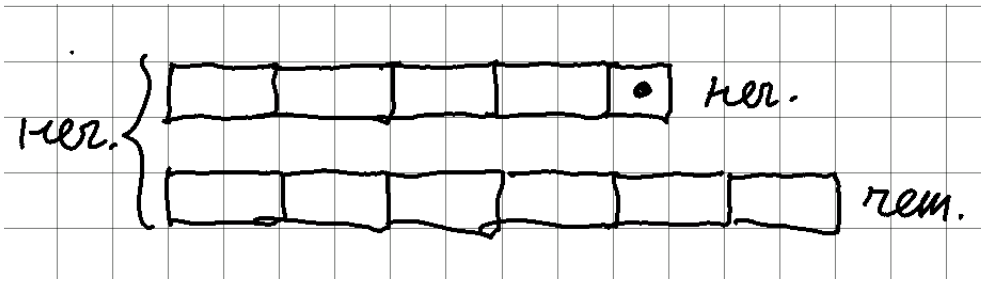
Запишем это более аккуратно. Пусть x, y — чётные числа. Докажем, что число $x + y$ чётно. (Это то, что мы хотим доказать. Теперь доказательство:) По определению чётного числа $x = 2m$, где m — целое число. Аналогично $y = 2n$ с целым n. Тогда $x + y = 2m + 2n = 2(m + n)$. Число $m + n$ целое, поэтому и $x + y$ чётно по определению. Что и требовалось доказать. ◁

1.9 Докажите, что разность двух чётных чисел чётна.

▷ Достаточно заметить, что $2m - 2n = 2(m - n)$. ◁

1.10 Будет ли чётной сумма чётного и нечётного числа? сумма двух нечётных чисел?

▷ Тут удобно воспользоваться общей формулой. Если сложить чётное число $2m$ и нечётное число $2n + 1$, то получится число $2m + 2n + 1 = 2(m + n) + 1$, то есть $2k + 1$ при $k = m + n$, то есть нечётное число.



Для суммы двух нечётных: $(2m+1)+(2n+1) = 2m+2n+2 = 2(m+n+1)$, то есть чётное число.

◁

Можно свести доказанное в таблицу сложения для чётности и нечётности:

+	Ч	Н
Ч	Ч	Н
Н	Н	Ч

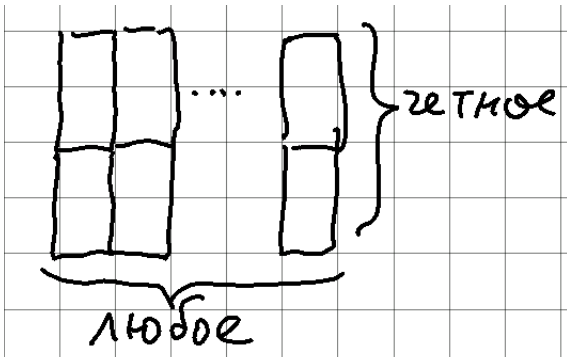
(чётности слагаемых записаны в первой строке и первой колонке, по таблице читаем чётность суммы).

1.11* Аня и Беня играют в такую игру: сначала Аня называет целое число по своему усмотрению (и Беня его слышит), потом Беня. Затем оба числа складывают. Если сумма чётна, выигрывает Аня, если нечётна — Беня. Кому выгоднее эта игра?

▷ Беня может гарантированно выиграть, если назовёт число не той чётности, что назвала Аня (сумма чисел разной чётности нечётна, см. таблицу). ◁

1.12 Составить таблицу умножения для чётности и нечётности. (Другими словами, надо определить, будет ли чётным произведение (а) двух чётных чисел, (б) чётного и нечётного и (в) двух нечётных.)

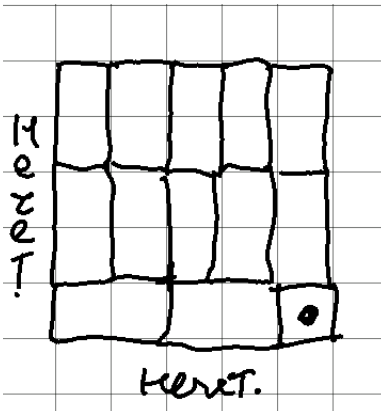
▷ Мы можем сразу заполнить три клеточки, если докажем, что произведение чётного числа на любое целое число чётно. Почему это так? Если мы умножаем чётное число $2k$ на любое число l, то получаем $2k \cdot l = 2(k \cdot l)$, а число $k \cdot l$ целое (произведение двух целых чисел).



Теперь докажем, что произведение двух нечётных чисел нечётно. Здесь тоже полезно воспользоваться общей формулой для нечётных чисел:

$$(2k + 1)(2l + 1) = 2k \cdot 2l + 2k + 2l + 1 = 2(2kl + k + l) + 1,$$

число $2kl + k + l$ целое, поэтому произведение нечётно.



Можно сказать иначе: произведение двух нечётных чисел — это значит, что мы берём одно нечётное число в качестве слагаемого нечётное число раз. А сумма нечётного числа слагаемых нечётна, потому что (это мы только что видели в таблице сложения) добавление нечётного числа меняет чётность. ◁

×	Ч	Н
Ч	Ч	Ч
Н	Ч	Н

1.13* Аня и Беня играют в такую игру: сначала Аня называет целое число по своему усмотрению (и Беня его слышит), потом Беня. Затем оба числа перемножают. Если произведение чётно, выигрывает Аня, если нечётно — Беня. Кому выгоднее эта игра?

▷ Аня может гарантировать выигрыш, если назовёт чётное число: что бы ни назвал потом Беня, всё равно произведение будет чётно. ◁

1.14* Учитель усадил по кругу вокруг стола 25 учеников своего класса (девочек и мальчиков), причём — говорит он — так, что никакие два мальчика не сидят рядом, и никакие две девочки не сидят рядом. Почему он ошибается?

▷ Потому что из условия следует, что мальчиков и девочек поровну, а число 25 нечётно. Как объяснить, почему мальчиков и девочек поровну? Пусть каждый мальчик повернётся вправо и посмотрит на сидящую справа от него девочку (а там именно девочка, потому что мальчики не сидят рядом, по словам учителя). А каждая девочка повернётся влево и посмотрит на сидящего слева от неё

мальчика (а там должен быть именно мальчик). Тогда все сидящие разобьются на пары смотрящих друг на друга, и, значит, мальчиков и девочек должно быть поровну.

Можно ещё сказать так: если девочки вершины многоугольника, то на каждой стороне (между соседними девочками) по условию один мальчик. А в многоугольнике столько же сторон, сколько вершин. ◁

1.15* По кругу написано 20 плюсов и 20 минусов в каком-то порядке. Подсчитаем число пар соседних плюсов (места, где плюсы стоят рядом). Аналогично подсчитаем число пар соседних минусов. Почему получится одно и то же число?

▷ Поставим между любыми двумя плюсами незримый минус, а между любыми двумя минусами — незримый плюс. (Между плюсом и минусом ничего не ставим.) Тогда число пар плюсов — это число незримых минусов, а число пар минусов — число незримых плюсов. Почему их поровну? потому что если считать все, и зримые и незримые, то плюсы и минусы чередуются, и их поровну. И зримых поровну, по 20. Значит, и незримых поровну. ◁

1.16* *Точным квадратом* называют квадрат целого числа (0, 1, 4, 9, 16,...). Может ли точный квадрат быть чётным, но не делиться нацело на 4?

▷ Не может: точные квадраты бывают у чётных и нечётных чисел. У нечётного числа он нечётный (по таблице), а у чётного числа $2k$ точный квадрат равен $4k^2$ и делится на 4, так что ни те, ни другие не подходят. ◁

1.17* Докажите, что точный квадрат не может быть вдвое больше другого точного квадрата, кроме того случая, когда они оба равны нулю.

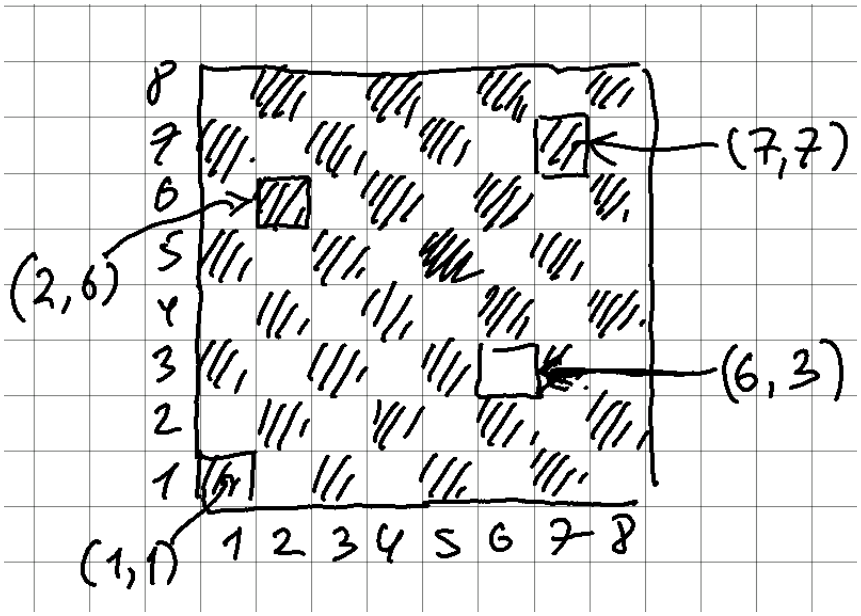
• Это формулируют так: уравнение $x^2 = 2y^2$ имеет единственное решение в целых числах: $x = 0, y = 0$. Отсюда следует, что никакая дробь x/y с целыми числителем и знаменателем не равна в квадрате 2. Как говорят, $\sqrt{2}$ — иррациональное число (не представляется в виде дроби с целым числителем и знаменателем)

▷ Пусть это не так, и есть ненулевое число n, которое одновременно и точный квадрат, и удвоенный точный квадрат: $n = x^2 = 2y^2$ при целых x и y. Тогда n положительно (квадраты отрицательными не бывают). Найдём (идя от нуля и пробуя по очереди все значения n) наименьшее такое число.

Теперь получается ерунда: n чётно (потому что $2y^2$), так что x^2 чётно, поэтому и x чётно (квадрат нечётного числа нечётный), $x = 2k$, тогда $n = x^2 = 4k^2 = 2y^2$, то есть вдвое меньшее число $n/2$ тоже равно и y^2, и $2k^2$.

Можно сказать и иначе: пусть есть дробь с целыми числителем и знаменателем, в квадрате равная 2, то есть $(x/y)^2 = 2$. Сократим эту дробь, пока можно — получим несократимую дробь x/y с тем же свойством $x^2 = 2y^2$. Теперь все четыре варианта чётности и нечётности x и y ведут к противоречию: если x нечётно, то квадрат его нечётный (а справа чётное). Если x чётно и y нечётно, то слева делится на 4, а справа не делится (после деления на 2 получается нечётное y^2), если оба чётны, то дробь сократима. ◁

1.18 Клетки шахматной доски обычно обозначают буквами и числами: a1 — левый нижний угол, a8 — левый верхний, h1 — правый нижний и так далее. Будем вертикали тоже нумеровать (вместо букв): тогда левый нижний угол будет $(1, 1)$, левый верхний $(1, 8)$, правый нижний $(8, 1)$ и так далее. Закончите предложение: «клетка (i, j) раскрашена в белый цвет, если...». (По шахматным правилам левая нижняя клетка чёрная.)



▷ Клетка (i, j) раскрашена в белый цвет, если (и только если, добавили бы педанты) $i + j$ нечётно. В самом деле, при увеличении i или j на единицу число $i + j$ меняет чётность, а клетка меняет цвет. Нижний левый угол $(1, 1)$ чёрный, и сумма чётна. ◁

1.19 Будет ли сумма $1 + 2 + 3 + \ldots + 99 + 100$ чётной или нечётной? (Ответ можно дать, не вычисляя, чему равна эта сумма.)

▷ Всего у нас 100 чисел, мы их разбиваем на 50 пар (1 и 2, 3 и 4, …, 99 и 100), в каждой по одному нечётному слагаемому, значит, сумма каждой пары нечётна, всего пар 50, то есть мы складываем 50 нечётных чисел. Их тоже можно сгруппировать в 25 пар, в каждой сумма чётна, и в сумме будет чётное число. ◁

1.20* Может ли прямая пересекать все стороны невыпуклого 13-угольника, не проходя через его вершины?

• Тут надо бы объяснить, что такое невыпуклый 13-угольник — но в задаче можно считать, что есть просто 13 различных точек (вершин) $A_1, A_2, \ldots, A_{13}$, и мы проводим 13 отрезков (сторон) A_1A_2, A_2A_3,..., $A_{12}A_{13}$, $A_{13}A_1$.

▷ Прямая, о которой идёт речь, разрезает плоскость на две части. Если сторона многоугольника её пересекает, то её концы (две вершины) с разных сторон. Но если мы 13 раз (нечётное число) переходим с одной стороны на другую, то не сможем вернуться в начальную точку. ◁

1.21 Закончите фразу: «сумма нескольких целых чисел будет чётной в тех случаях, когда в этой сумме чётное число…».

▷ …нечётных слагаемых. В самом деле, добавление чётного слагаемого не меняет чётности суммы, а добавление нечётного меняет. Начинаем мы с нуля, значит, чтобы получить чётное число, надо менять нечётное число раз. ◁

• Более точно было бы сказать «в тех и только тех случаях, когда», «тогда и только тогда, когда», «если и только если» и т.п. Этот математический жаргон подразумевает сразу два утверждения: (1) если в сумме чётное число ⟨…⟩, то она чётна, и (2) если сумма чётна, то в ней чётное число ⟨…⟩.

1.22* Придя на занятие математического кружка, некоторые школьники пожали друг другу руки. Докажите, что количество тех школьников, которые сделали нечётное число рукопожатий, чётно.

▷ Пусть каждый школьник считает, сколько рукопожатий он сделал, а потом мы мысленно складываем все эти числа. От каждого рукопожатия сумма увеличится на 2 (два слагаемых увеличатся на 1), поэтому она всегда будет оставаться чётной. Значит, в неё чётное число нечётных слагаемых — а это и требуется доказать. ◁

1.23* В классе из 15 школьников каждый считает, что у него в классе есть семь друзей (среди остальных). Докажите, что отношение дружбы

несимметрично: найдутся такие два школьника A и B, что A считает B своим другом, а B не считает A своим другом.

▷ Если бы это было не так и отношение дружбы было симметрично, то это было бы как рукопожатия (пусть все пары друзей пожмут друг другу руки), и по предыдущей задаче число людей, сделавших нечётное число рукопожатий, было бы чётно (а тут все 15 сделали по 7). ◁

1.24* Можно ли заполнить таблицу 7×11 (7 строк и 11 столбцов) целыми числами так, чтобы сумма чисел в каждой строке была бы чётна, а сумма чисел в каждом столбце была нечётна?

▷ Нет: сумму можно считать по строкам и по столбцам. По строкам она будет чётной (даже неважно, сколько строк, достаточно, что в каждой строке чётна), а по столбцам будет сумма 11 нечётных чисел, которая нечётна. ◁

1.25* Чтобы узнать, чётно ли целое положительное число, достаточно посмотреть на его последнюю цифру. Почему?

▷ Потому что многозначное число можно разбить на последнюю цифру и остальное, и это остальное измеряется десятками, поэтому заведомо чётно. ◁

1.26 Докажите, что произведение двух соседних целых чисел всегда чётно.

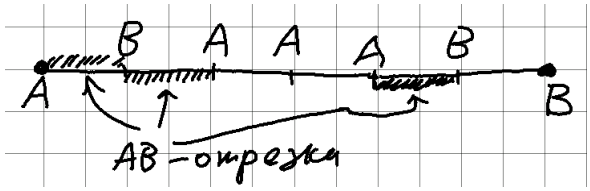
▷ Из соседних двух чисел одно нечётное, а другое чётное, значит, произведение всегда чётно. (А сумма нечётна, хоть в задаче про это и не спрашивается.) ◁

1.27* Запишем степени двойки (1, 2, 4, 8, 16, 32, …) и степени тройки (1, 3, 9, 27, 81, …). Может ли в этих двух последовательностях чисел встретиться какое-то общее число, кроме 1?

• Это утверждение, если знать про логарифмы, можно сформулировать и так: $\log_2 3$ иррационален.

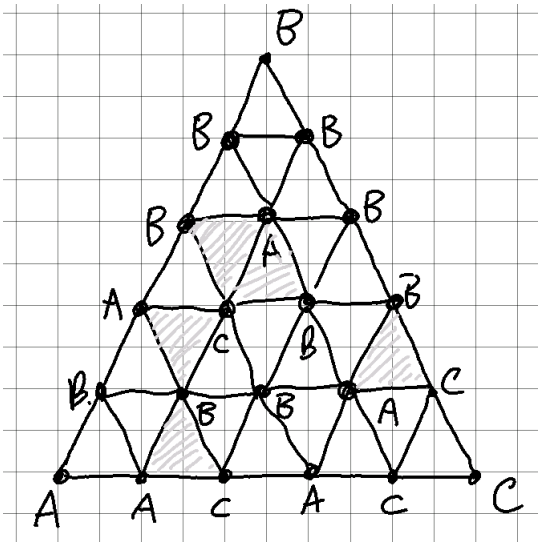
▷ Нет: в первой последовательности все числа чётны, кроме первого, а во второй — все нечётны. ◁

1.28* Отрезок AB разбит на несколько частей промежуточными точками, которые произвольно размечены буквами A или B (каждая точка либо A, либо B). Из этих частей выберем AB-отрезки, то есть те части, у которых концы помечены разными буквами (в любом порядке, так что можно было бы их назвать и BA-отрезками). (а) Докажите, что есть хотя бы один AB-отрезок. (б) Докажите, что общее число AB-отрезков нечётно.



▷ Что один AB-отрезок есть, совсем очевидно: идём слева направо, пока не встретим первую B-точку, перед ней будет AB-отрезок. Почему нечётное число: если идти слева направо, считая AB-отрезки, то появление каждого нового отрезка меняет текущую букву с A на B и обратно. А всего должно быть нечётное число перемен, раз мы начали с A и пришли в B. ◁

1.29* Треугольник ABC разрезан на меньшие (как на рисунке), и их вершины помечены буквами A, B и C произвольным образом (каждая вершина одной буквой). При этом на стороне AB использованы только буквы A и B, на стороне BC — только B и C, на стороне AC — только A и C. Докажите, что есть ABC-треугольники (в вершинах которых все три буквы), и их нечётное число.



▷ Будем действовать несимметрично и считать, скажем, AB-отрезки. Сначала посчитаем их по треугольникам. Каждый ABC-треугольник имеет ровно одну AB-сторону, остальные имеют либо ноль, либо две (если вершины помечены буквами A и B). Если мы сложим все эти количества, то каждый внутренний AB-отрезок будет посчитан дважды, а каждый граничный (они бывают только на стороне AB) будет посчитан один раз. Поэтому *чётность числа*

ABC-треугольников равна чётности числа граничных AB-отрезков, а мы уже знаем, что их число нечётно. ◁

• Это утверждение, которое можно обобщить на любую размерность (хотя тетраэдр сложнее разрезать на маленькие тетраэдры, но тоже можно), называется *леммой Шпернера*. Она используется в одном из доказательств *теоремы Брауэра о неподвижной точке*: всякое непрерывное отображение треугольника в себя оставляет хотя бы одну точку на месте. Схема рассуждения такая: если это не так и все точки сдвигаются хотя бы на некоторое расстояние $d > 0$, то разрежем треугольник на такие маленькие треугольники, чтобы вершины каждого переходит в близкие точки (расстояние между образами вершин много меньше d). Теперь пометим вершину буквой A, если она приближается к противоположной стороне BC, аналогично для букв B (приближение к AC) и C (приближение к AB). Поскольку точки не остаются на месте, то к одной из трёх сторон они должны приближаться и букву выбрать можно (могут сразу к двум, тогда выберем произвольно). Теперь разнобуквенный треугольник создаёт противоречие: его вершины куда-то сдвигаются, и примерно в одно и то же место, и не могут сразу приближаться ко всем трём сторонам.

В свою очередь, теорема Брауэра о неподвижной точке применяется в математической экономике (для доказательства существования равновесий в играх, в том числе *равновесия Нэша*).

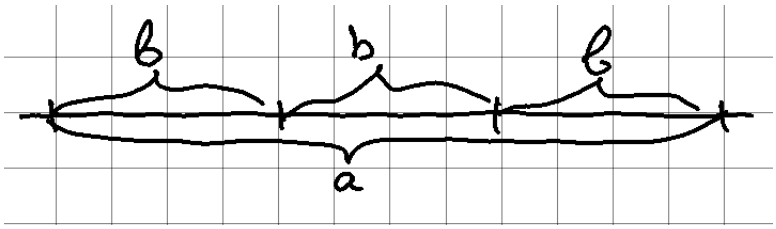
2. Делимость

Чётные числа — это числа, которые делятся нацело (без остатка) на 2, то есть равные $2k$ для какого-то целого k. Аналогично можно определить делимость на 3, 4, 5, ...:

> *целое число a делится на целое положительное число b*, если $a = kb$ для некоторого целого числа k.

Ещё говорят (это значит ровно то же самое), что a *кратно* b (число a является кратным числа b), и что b является *делителем* a.

Обозначение: $b \mid a$ (b делит a).



• Для положительного a это имеет наглядный смысл: в мешке a яблок, и их можно раздать поровну b людям. Или по-другому (переставляя сомножители): a яблок можно разложить на кучки по b яблок, и ничего не останется. Ещё: a рублей можно заплатить купюрами по b рублей.

Слово «кратное» имеет тот же смысл, что в «уплатить штраф в трёхкратном размере»: новая сумма штрафа кратна исходной (втрое больше). Другие родственные слова: «многократно», «неоднократно» и т.п.

2.1 Заполнить пробел: положительное число a кратно b, если на круговом шоссе длиной в b километров мы [...], проехав a километров.

▷ ...сделаем целое число кругов и вернёмся в точку старта. ◁

2.2 Сколько целых положительных делителей у числа 18? (Не забудьте 1 и само число 18.)

▷ Можно в уме перебрать делители: 1, 2, 3, 6, 9, 18. Видно, что их можно сгруппировать парами 1 и 18, 2 и 9, 3 и 6. (Понятно, по какому принципу они сгруппированы? Произведение в паре 18.) ◁

2.3* Найдите несколько чисел, у которых *нечётное* число целых положительных делителей? Видите ли вы тут какую-то закономерность? Если да, то можете ли её доказать?

▷ Тут помогает группировка делителей числа n в пары: x и y образуют одну пару, когда $xy = n$. Есть единственный случай непарного делителя: когда парный y равен самому x, то есть $n = x^2$. Значит, для точных квадратов делителей нечётное число, а для остальных — чётное. ◁

2.4 В определении делимости мы требуем, чтобы b было целым положительным числом, но не запрещаем случая $b = 1$. Какие целые числа делятся на 1?

▷ Все: поскольку $a = 1 \cdot a$, то $1 \mid a$ при любом a. ◁

2.5 В определении делимости мы разрешаем a быть нулём или отрицательным числом. На какие числа делится нуль? В каком случае $-a$ делится на b?

▷ (а) Нуль делится на все целые положительные b, так как $0 = 0 \cdot b$, то есть $0 = kb$ при $k = 0$. (б) От изменения знака a делимость не меняется: если a делится на b и $a = kb$ для какого-то k, то $-a = (-k)b$, то есть $a = lb$ при целом $l = -k$. ◁

2.6 При определении делимости мы запретили b быть нулём или отрицательным числом. Что было бы, если бы мы не сделали такой оговорки: какие числа делились бы на нуль? какие числа делились бы на -2?

▷ (а) Без такой оговорки на нуль делились бы числа вида $0 \cdot k$, то есть единственное число нуль. (b) От изменения знака b делимость (в этом новом временном смысле) не меняется: если a делится на b и $a = kb$ для какого-то k, то $a = (-k) \cdot (-b)$, то есть $a = l(-b)$ при $l = -k$. ◁

• Иногда люди спорят: делится ли нуль на нуль? Одни говорят, что делится: ведь $2x$ всегда делится на x, зачем же делать исключение для $x = 0$? Другие говорят, что a делится на b, когда a/b — целое число, а $0/0$ смысла не имеет. И те, и другие имеют резон, но в математике смысл терминов зависит от того, как их определить — раз уж мы договорились, что 0 (и вообще никакое число) не делится на 0, значит, не делится. Но другие могут определить иначе. И в этом нет ничего страшного — хотя неудобно: надо уточнять, как понимается слово «делится».

▷ Наиболее известный пример такого рода: является ли нуль натуральным числом? В российской школьной программе не является, но во многих книгах (а также во французской школьной программе) является. Так что надо быть осторожным, если в задаче спрашивается про натуральные числа. ◁

2.7* В ныне принятом григорианском календаре все годы имеют 365 или 366 дней; во втором случае год называется *високосным*. Правила такие: по умолчанию год N не високосный, но если N делится на 4, то год в порядке исключения будет високосным. Однако если N делится на 100, то в порядке исключения из исключения год не будет високосным — правда, если n делится на 400, то в порядке исключения (опять!) год будет високосным.

Если такой календарь продолжать неограниченно долго, то сколько в среднем будет дней в году?

• Педанты скажут, что среднее (арифметическое) определено для конечного числа лет, а календарь продолжается неограниченно долго. Строго говоря, нужно было бы говорить о пределе — к чему близко среднее арифметическое для очень больших отрезков. Но правильный ответ можно получить и из наглядных соображений, оставив строгое доказательство на будущее.

▷ Из правил видно, что всё повторяется каждые 400 лет (потому что 400 делится и на 4, и на 100). За эти 400 лет было бы 100 високосных, если бы не правило про делимость на 100. Из них надо вычесть четыре раза, когда делится на 100, и один вернуть (когда делится на 400), всего $100 - 4 + 1 = 97$. Значит, 97 раз из 400 добавляется день к невисокосному году в 365 дней, откуда получаем ответ: $365\frac{97}{400}$. ◁

2.8 Докажите, что если два целых числа a и b делятся на целое положительное c, то их сумма и разность делятся на c. Что можно сказать про $a + b$ и $a - b$, если одно из чисел a и b делится на c, а другое — нет? Что можно сказать про $a + b$ и $a - b$, если оба числа не делятся на c?

▷ Пусть a и b делятся на c. Тогда по определению $a = kc$ и $b = lc$ для некоторых целых k и l. Сложим: $a + b = kc + lc = (k + l) \cdot c$, поэтому $a + b$ получается умножением целого числа $k + l$ на c, то есть делится на c. Аналогично для $a - b = (k - l) \cdot c$.

Если a делится на c, а b не делится на c, то сумма $a + b$ не делится на c. Почему она не может делиться на c? Если бы она делилась, то число $b = (a + b) - a$ было бы разностью двух чисел $a + b$ и b, делящихся на c, и по доказанному делилось бы на c (а мы предполагаем, что b не делится).

Аналогично для разности: если, скажем, a делится на c, а b не делится, то разность $a - b$ не может делиться, иначе и $b = a - (a - b)$ делилось бы.

А вот про сумму и разность двух чисел a, b, не делящихся на c, ничего гарантировать нельзя — может делиться, а может и не делиться. Скажем,

$1+4$: два слагаемых не делятся на 3, и сумма 5 тоже не делится. А в $1+8$ оба слагаемых тоже не делятся на 3, а сумма делится. То же самое и с разностью бывает (хотя бы потому, что $a+b$ это $a-(-b)$). ◁

• Мы потом увидим, что деление чисел на (скажем) делящиеся и не делящиеся на 3 слишком грубое: его надо уточнить и среди не делящихся различать дающие остаток 1 и дающие остаток 2.

2.9 Докажите, что если a делится на b, а b делится на c, то a делится на c.

▷ Если a в k раз больше b, а b в l раз больше c, то a в kl раз больше c: из $a=kb$ и $b=lc$ при целых k и l следует $a=k(lc)=(kl)c$, и множитель kl целый, так что a делится на c. ◁

2.10 Докажите, что если хотя бы один сомножитель в произведении двух целых чисел делится на k, то и всё произведение делится на k. Верно ли обратное: если произведение делится на k, то один из сомножителей делится на k?

▷ Пусть в произведении ab сомножитель a делится на k, то есть $a=kl$ для целого l. Тогда $ab=(kl)b=k(lb)$ и делится на k (с целым частным lb).

Обратное неверно: скажем, произведение 10 и 6, равное 60, делится на 4, но оба сомножителя не делятся. ◁

• Обратное будет верным для случая *простого* k (не разлагающегося в произведение двух меньших). Мы ещё много раз про это будем говорить.

2.11* Числа a, b, c, d — целые положительные, причём $ab=cd$. Известно, что a делится на c. Докажите, что d делится на b.

▷ Если $a=kc$ при целом k, то $kcb=cd$ по условию, и на c (оно положительно) можно сократить, получится $kb=d$, то есть d делится на b. (Можно коротко сказать: составим пропорцию $a/c=d/b$.) ◁

2.12* Есть четыре целых положительных числа a, b, c, d, причём $ad+bc$ делится на $a+b$. Докажите, что тогда и $ac+bd$ делится на $a+b$.

▷ На первый взгляд это выглядит странно, но можно заметить, что сумма двух чисел, о которых идёт речь, $ad+bc$ и $ac+bd$, равна $(a+b)(c+d)$ и делится на $a+b$. Поэтому если одно делится, то и второе тоже. ◁

2.13 В трёхзначном числе все цифры одинаковы (то есть это одно из чисел 111, 222, …, 999). Докажите, что оно делится на 37.

• Тут не так много чисел, и можно их все перепробовать — но можно обойтись и без этого. Как?

▷ Число 111 делится на 37 (частное 3), а все следующие числа кратны 111 (скажем, $555 = 5 \cdot 111 = 5 \cdot 3 \cdot 37 = 15 \cdot 37$. ◁

2.14* Шестизначное число состоит из двух одинаковых групп по три цифры (как, скажем, 173173). Докажите, что оно делится на 7, 11 и 13. Что получится, если его последовательно разделить на все эти три числа?

▷ Можно заметить, что

$$173\,173 = 173\,000+173 = 1000\cdot173+173 = (1000+1)\cdot173 = 1001\cdot173 = 7\cdot11\cdot13\cdot173.$$

(Не спрашивайте, почему $1001 = 7 \cdot 11 \cdot 13$ — так вышло.) Поэтому 173 173 делится на 7, 11 и 13, а если последовательно разделить на все три, то получится 173. (Здесь 173 только для примера, можно взять любое другое трёхзначное число.) ◁

2.15* Покажите, что $a^2 - b^2$ всегда делится на $a - b$ (мы считаем, что числа a и b целые, и $a > b$). Тот же вопрос для $a^3 - b^3$, $a^4 - b^4$ и вообще для $a^n - b^n$.

▷ Можно вспомнить, что $a^2 - b^2 = (a - b)(a + b)$ и потому делится на $a - b$ (частное $a + b$). Для кубов: $a^3 - b^3 = (a - b)(a^2 + ab + b^2)$, это можно проверить умножением. Вообще,

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + a^2b_{n-3} + ab^{n-2} + b^{n-1},$$

если перемножить, почти всё, кроме двух членов a^n и b^n сократится.

Для $a^4 - b^4$ можно заметить, что это ведь квадраты a^2 и b^2, так что из самого первого утверждения мы знаем, что $a^4 - b^4$ делится на $a^2 - b^2$, которое в свою очередь делится на $a - b$.

Можно сказать и так: обозначив $a - b$ за k, мы должны доказать, что $(b + k)^n - b^n$ делится на k. Но если раскрыть скобки в $(b+k)(b+k)\ldots(b+k)$, то будет ровно одно слагаемое без k, оно будет равно b^n, а все остальные (интересующая нас разность) содержат множитель k. ◁

• Здесь $a^2 = a \cdot a$, $a^3 = a \cdot d \cdot a$ и так далее (a^n — произведение n сомножителей, равных a).

2.16* Пусть m, n — целые числа, и $5m + 3n$ делится на 11. Покажите, что $6m + 8n$ делится на 11. Покажите, что $9m + n$ делится на 11.

▷ Если $5m + 3n$ делится на 11, то и разница $11(m + n) - (5m + 3n) = 6m + 8m$ делится на 11. Кроме того, в этом случае $4(5m + 3n)$ тоже делится на 11, то есть

$20m + 12n = 11(m + n) + 9m + n$ делится на 11, и остаётся вычесть кратное 11 число $11(m + n)$. ◁

• Мы потом увидим, что такое получается из-за того, что $5/3 = 6/8 = 9$ по модулю 11.

2.17* Имеется n различных целых положительных чисел. Докажите, что любое целое положительное число, которое делится на все эти числа, хотя бы в n раз больше наименьшего из них.

▷ Пусть N, в соответствии с условием, делится на $a_1, \dots, a_n$, причём $a_1 < \dots < a_n$. Надо доказать, что $N/a_1 \geqslant n$. В самом деле, числа $N/a_1 > N/a_2 > \dots > N/a_n$ целые положительные, и их n штук, поэтому первое из них не меньше n. ◁

2.18* Найти все неотрицательные целые числа n, при которых $5n + 17$ делится на $n + 1$.

▷ Если вынести очевидно целую часть — заметив, что

$$\frac{5n + 17}{n + 1} = \frac{5n + 5}{n + 1} + \frac{12}{n + 1},$$

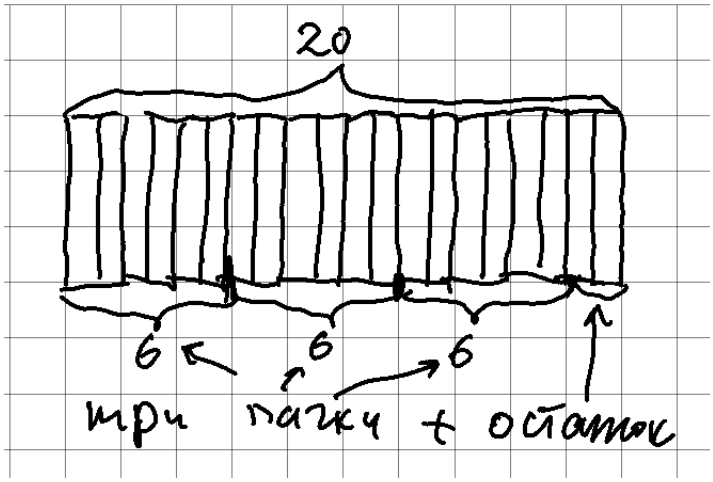
то ясно, что надо найти целые $n \geqslant 0$, для которых $n+1$ делит 12, то есть делители 12, уменьшенные на единицу: 0, 1, 2, 3, 5, 11. ◁

2.19* Есть 101 целое положительное число. Докажите, что среди них есть два, разность которых делится на 100. Почему?

▷ Запишем числа в десятичной системе и посмотрим на две последние цифры. Вариантов от 00 до 99 есть только 100, а чисел 101, поэтому у каких-то двух чисел в конце стоит одна и та же пара цифр. Тогда их разница кончается на два нуля, то есть состоит из целого числа сотен (делится на 100). ◁

3. Деление с остатком

Связывая 20 книг в пачки по 6 книг в каждой, мы получим 3 пачки и останутся две лишние книги: $20 = 3 \times 6 + 2$. Как говорят, мы делим 20 (*делимое*) на 6 (*делитель*) и получаем в результате *неполное частное* 3 и *остаток* 2.



Обозначают остаток по-разному. В математических книжках (и в языке `Pascal`) пишут $20 \bmod 6 = 2$, во многих других языках програмирования (`C`, `python`) пишут `20%6==2` (два знака равенства не опечатка, они так и пишут, чтобы отличить от присваивания).

3.1 (**а**) В году (невисокосном) 365 дней. Сколько в нём полных недель и сколько дней в остатке?

(**б**) Первое января 2022 года пришлось на субботу. Каким днём недели будет первое января 2023 года? 2024 года? (Из этих трёх лет високосный только последний.)

▷ Число недель можно подсчитать в уме: 350 дней — это 50 недель по 7 дней, остаётся 15 дней, то есть две полные недели и ещё один день. Всего в году 52 недели и один день.

Если бы этого лишнего дня не было, то следующий год начинался бы с того же дня недели, что и предыдущий. А так он на день позже. Значит, 1 января 2023 года будет воскресенье, а 1 января 2024 года будет понедельник. (Оба года 2022 и 2023 невисокосные, так как не делятся на 4. А

следующий год 2024 будет високосным, так что первое января 2025 года придётся не на вторник, а не среду.) ◁

- Раньше в школах учили делить «уголком»:

$$\begin{array}{r|l} 365 & 7 \\ \cline{2-2} 35 & 52 \leftarrow \text{частное} \\ \cline{1-1} 15 & \\ 14 & \\ \cline{1-1} 1 \leftarrow \text{остаток} & \end{array}$$

Для ленивых проще воспользоваться калькулятором:

$$365/7 = 52.142857\ldots$$

Отсюда сразу видно, что полных недель будет 52; вычислим остаток: $365 - 52 \times 7 = 1$. (Можно также сообразить, что $0.142857\ldots$ — это одна седьмая, поскольку это меньше двух десятых и тем более двух седьмых.)

3.2 (**а**) Какой остаток даёт число 1000 при делении на 17?

(**б**) Найдите наименьшее четырёхзначное число, которое делится нацело (без остатка) на 17.

▷ Калькулятор даёт $1000/17 = 58.82\ldots$, так что неполное частное будет 17, а останется $1000 - 58 \cdot 17 = 14$.

Чтобы получить делящееся на 17 число, минимум нужно добавить 3 ($14 + 3 = 17$), так что наименьшее четырёхзначное число будет 1003. ◁

3.3 Сейчас два часа дня. Сколько времени будет через 100 часов?

▷ Делим с остатком: 100 часов — это четверо суток ($24 \cdot 4 = 96$) и ещё 4 часа. Значит, будет (по суточному циклу) на четыре часа позже: шесть часов вечера. ◁

3.4 Найдите число, которое даёт при делении на 117 частное 7 и остаток 43.

▷ Надо просто вычислить $117 \cdot 7 + 43 = 862$. ◁

3.5* Поезд Москва–Владивосток вышел в пятницу в 21:25 и шёл 147 часов 38 минут. В какой день недели и в какое время (по московскому времени — железная дорога вся работает по одному времени, независимо от часовых поясов) он пришёл во Владивосток?

▷ Сначала выделим целое число суток: $144 = 6 \cdot 24$, так что поезд идёт 6 суток и ещё 3 часа 38 минут. Значит, в четверг следующей недели в 21:25 ему останется ехать эти самые 3 часа 38 минут. Через 3 часа будет 00:25 пятницы, $25 + 38 = 63$, получается 01:03 пятницы. ◁

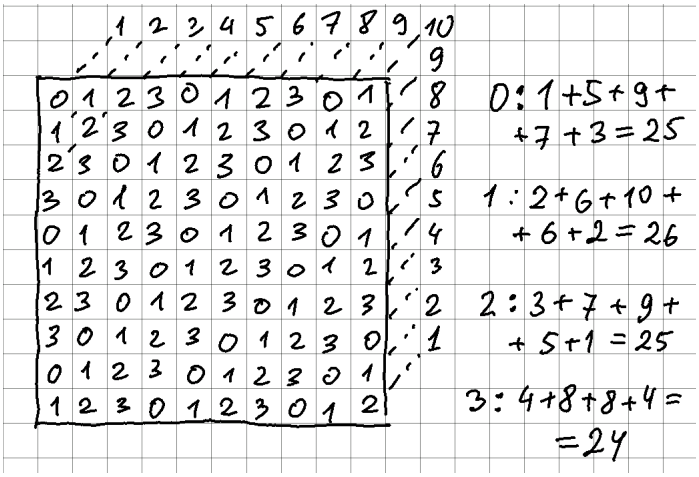
3.6 Можно ли разрезать квадрат 8×8 на прямоугольники 1×3?

▷ Нельзя: $8 \cdot 8 = 64$ не делится нацело на $1 \cdot 3 = 3$, получается $21\frac{1}{3}$ (остаётся одна клетка). ◁

3.7* Можно ли разрезать квадрат $10 \cdot 10$ на прямоугольники $1 \cdot 4$?

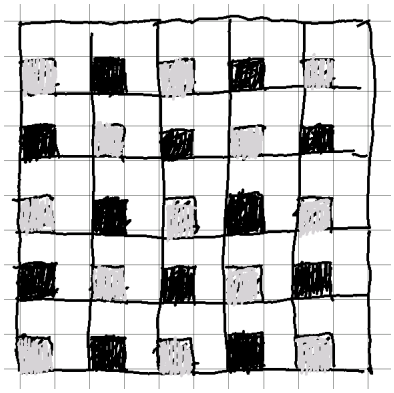
• Подсчёт показывает, что *если* можно разрезать, то получится 25 прямоугольников, это число целое. Но отсюда ещё не следует, что можно разрезать (и на самом деле нельзя, но доказательство требует изобретательности).

▷ Можно раскрасить все клетки в четыре цвета по диагоналям, меняя цвета по циклу, и заметить, что каждый прямоугольник $1 \cdot 4$ покрывает по одной клетке каждого цвета.



Значит, 25 таких прямоугольников покрывают по 25 клеток, но в реальности клеток равных цветов не поровну.

Можно использовать и другие трюки подобного рода.

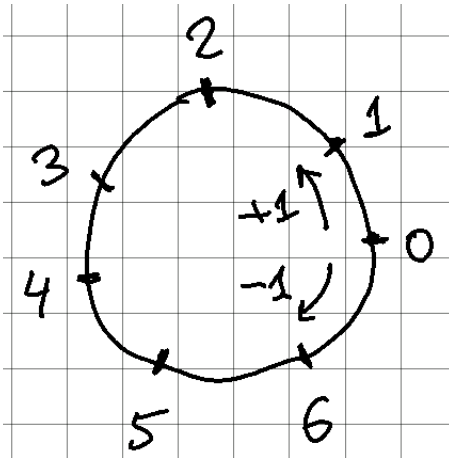


При такой раскраске каждый прямоугольник 1×4 покрывает поровну серых и чёрных клеток (по одной клетке, если вообще покрывает), а всего клеток 25, так что чёрных и серых не поровну. $\triangleleft$

• Вообще верно такое утверждение: если прямоугольник можно разрезать на прямоугольники, у каждого из которых одна сторона кратна c, то и у исходного прямоугольника одна сторона кратна c. (В нашем случае $c = 4$.) Это утверждение имеет множество разных доказательств, некоторые из них используют аналогичную раскраску.

3.8 Число x даёт при делении на 7 остаток 3. Какой остаток даёт при делении на 7 число $x + 1$? число $x - 1$? Какой остаток дают при делении на 7 числа $2x$ и $3x$?

$\triangleright$ По определению, $x = 7k + 3$ (целое число k пачек по семь книг и ещё три книги, если как в примере). Тогда $x + 1 = 7k + 4$ и $x - 1 = 7k + 2$, то есть остатки 4 и 2. Вообще прибавление единицы к числу прибавляет единицу к остатку, только вместо 6 получается 7 (аналогично и вычитание, только из нуля получается 6).



Теперь с умножением: $(7k+3)\cdot 2 = 2\cdot 7k+6$, первое слагаемое делится на 7, значит, остаток 6. Аналогично $(7k+3)\cdot 3 = 3\cdot 7k+9$, значит, остаток 9? Нет, конечно, из 9 можно выделить ещё одну целую пачку и останется 2. Другими словами, $(7k+3)\cdot 3 = 7\cdot 3k+9 = 7\cdot 3k+7+2 = 7\cdot(3k+1)+2$, остаток 2. ◁

• Можно было бы просто взять $x = 3$, и получить все нужные ответы. Но это не совсем честно: мы пока не знаем (по крайней мере официально), что важен только остаток, а какое конкретно x с этим остатком, не важно. Но это так и есть, и понять это тоже легко: если мы к x прибавим 7, то и к $x+1$, и к $x-1$ прибавится 7, а к $2x$ и $3x$ прибавятся 14 и 21 (кратные 7, которые не меняют остатка).

3.9 Найдите остаток от деления числа 1828 на 10, на 100 и на 25.

▷ Тут не нужен калькулятор, помогает десятичная система счисления, в которой записаны числа. Число 1828 содержит 182 десятка и ещё 8 единиц, так что при делении на 10 остаётся 8. Точно так же там 18 сотен и ещё 28, так что при делении на 100 остаётся 28. При делении на 25 сотни разделятся нацело на четыре группы по 25, а из 28 получится $25+3$, так что при делении на 25 остаток будет 3. ◁

3.10* Рассмотрим числа от 1001 до 2000. Будем делить их на 7. Сколько из них разделятся без остатка? Какой остаток будет встречаться реже всего?

▷ Число $1001 = 7\cdot 143$ делится на 7. Значит, остатки будут идти по циклу: $0, 1, 2, 3, 4, 5, 6, 0, 1, 2, \ldots$. Число 2002 тоже будет делиться на 7, так что последний цикл кончается в 2001. В этом цикле не будет числа 2001, которое даёт остаток

6, так что было поровну, а один остаток 6 забрали, и остаток 6 встречается реже всего. Циклов же будет 143 (с неполным последним). ◁

3.11* Подсчитайте (по возможности без бумажки), какой остаток даёт миллион при делении на 1000, на 999 и на 1001.

▷ На 1000 делится без остатка (миллион — тысяча тысяч). На 999 можно без остатка разделить 999 тысяч, оставшаяся тысяча даёт остаток 1. Делим на 1001: если разложить на 1000 куч по 1000, кучи будет неполными (недостаёт одного предмета в каждой) поэтому одну кучу можно пустить на пополнение 999 оставшихся и ещё один предмет останется. Можно также сообразить, что $999999 = 999 \cdot 1001$. ◁

3.12 Разрежем кусок бумаги на 5 частей. Затем одну из частей снова разрежем на пять частей, потом одну из частей (любую) разрежем на пять частей и так далее. Может ли после очередного разрезания получиться 34 части?

▷ Надо следить за числом частей при разрезании. Неважно, что мы разрезаем (начальный кусок, его части, части этих частей и т.п.), в любом случае число частей увеличивается на 4 (из одной части получается пять). То есть их будет $9, 13, \ldots$ — все эти числа дают остаток 1 при делении на 4. А число 34 даёт остаток 2 и тем самым невозможно (после 33 будет сразу 37). ◁

3.13 Число n даёт при делении на 143 остаток 24 и частное 13. Какой остаток оно будет давать при делении на 142? на 144?

• Разумеется, можно просто вычислить это самое n и поделить его на бумажке или с калькулятором. Но можно решить и в уме — как?

▷ Представим себе, что мы раскладывали на пачки по 143, получилось 13 пачек и осталось 24. Если из остатка добавить в каждую пачку по одной штуке, то в пачках будет 144 и останется $24 - 13 = 11$. Видим, что при делении на 144 остаток 11. Наоборот, если из каждой пачки забрать по одной штуке, то в пачках будет 142 и останется $24 + 13 = 37$. Это меньше одной пачки, так что 37 и будет остатком при делении на 142. ◁

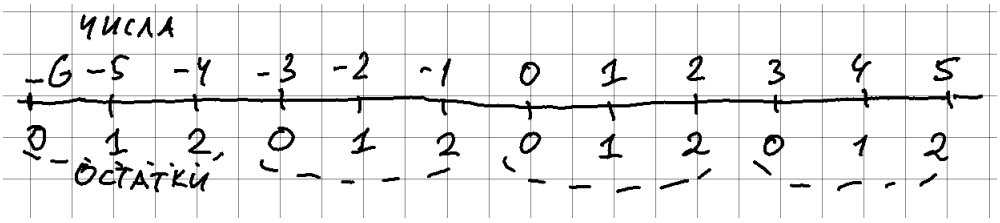
3.14 Отметьте на числовой оси числа, которые делятся на 3, затем числа, которые дают остаток 1 при делении на 3, а затем числа, которые дают остаток 2 при делении на 3. (Сделайте рисунок так, чтобы числа от -5 до 5 поместились.)

▷ Отметить числа, которые делятся на 3, несложно: они идут через два на третье, от нуля в ту и другую сторону (0, ±3, ±6, ±9, ...). А вот два других вопроса требуют уточнения: как делить с остатком отрицательные числа?

Мы не дали определения на этот случай, так что вы имеете полное право протестовать и отказаться от решения этой задачи как нечётко поставленной. Скажем, как разделить -5 на 3 с остатком?

Связывать в пачки по три книги, которых минус пять, можно только при большой фантазии — и фантазировать можно по-разному. Одни скажут, что будет частное -1 и остаток -2 (каждый получит по минус одной книге, и ещё минус две книги останутся). Или в терминах долга: мы на троих должны были 5 рублей, каждый взял на себя долг в 1 рубль, а ещё два рубля долга остались неоплаченными.

Но можно сказать и иначе: частное -2 и остаток 1 (каждый берёт на себя долг в 2 рубля, и всего выплачиваем на рубль больше). Именно так деление отрицательных чисел с остатком обычно и определяется. Получаем такой ответ:



На рисунке видно, что числа, дающие остаток 1 при делении на 3 идут через два на третье (и положительные и отрицательные); аналогично для чисел, дающих остаток 2 при делении на 3.

Сказанное про деление отрицательных чисел можно сформулировать в виде определения. ◁

Определение. Пусть a, b — целые числа, причём $b > 0$. *Разделить a на b с остатком* означает найти такие целые числа q (*частное*) и r (*остаток*), что

- $a = q \cdot b + r$;
- $0 \leqslant r < b$.

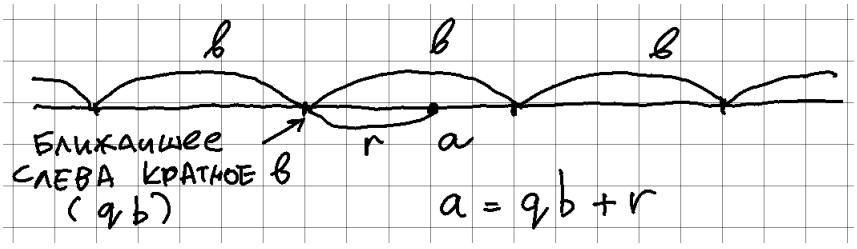
Обратите внимание, что число b должно быть положительным, а число a — не обязательно. Но даже если a отрицательно, то остаток r должен быть положительным (хотя частное q может быть и отрицательным).

3.15 Всегда ли возможно деление с остатком по такому определению? Определены ли частное и остаток однозначно (или может быть несколько вариантов, удовлетворяющих условиям)?

▷ Да, деление с остатком по этому определению всегда возможно и остаток и частное определены однозначно. Почему?

Для $a \geqslant 0$ существование такого разложения можно объяснить на книгах: связываем их в пачки по b, пока это можно. Сколько может остаться? если есть хотя бы b, то можно сделать ещё одну пачку, так что останется меньше b (но не меньше 0). Обозначим за q число пачек, а за r — число оставшихся книг, и видим, что все условия выполнены.

Но как быть с $a < 0$? Наглядно можно объяснить так: пометим на числовой оси точки, кратные b, и возьмём ближайшую точку слева от a (или само a, если оно кратно b). Эта точка кратна b, то есть равна qb для некоторого q. Чтобы получить из неё a, надо добавить к ней (то есть к bq) расстояние от bq до a, которое неотрицательно и меньше b (иначе точка не была бы ближайшей слева).



Другой вариант рассуждения: если $a < 0$, то прибавим к нему такое большое кратное b (пусть это будет kb), чтобы сумма $a' = a + kb$ стала неотрицательной. Для неотрицательных мы умеем делить с остатком, так что поделим a' на b:

$$a + kb = a' = q'b + r', \quad 0 \leqslant r' < b.$$

Тогда $a = (q' - k)b + r'$, так что можно взять $q = q' - k$, $r = r'$ и получить требуемое.

Однозначность: если $a = q_1 \cdot b + r_1 = q_2 \cdot b + r_2$ — два варианта, то $r_1 - r_2 = (q_2 - q_1) \cdot b$, поэтому $r_1 - r_2$ делится на b. Но оба числа r_1

и r_2 лежат на отрезке от 0 до $b - 1$, поэтому разность не больше $b - 1$ (расстояние между концами отрезка), и делиться на b она может, только есть она равна нулю. ◁

3.16 Учитель по ошибке написал второе условие в определении деления с остатком как $0 \leqslant r \leqslant b$. Останется ли утверждение предыдущей задачи верным для такого определения?

▷ Требование теперь более слабое (его легче выполнить), так что утверждение о существовании частного и остатка останется верным. Но единственности уже не будет: скажем, при делении 8 на 2 может быть частное 4 и остаток 0, а также частное 3 и остаток 2 (который по новому определению разрешён). ◁

3.17* Останется ли утверждение предыдущей задачи верным, если второе условие записать как $0 < r \leqslant b$?

▷ Останется, только числа, которые раньше давали остаток 0, теперь будут давать остаток b (а частное на единицу уменьшится по сравнению с обычным определением). ◁

3.18* Число 100 делят с остатком на целое положительное число, меньшее 100. Какой наибольший остаток может получиться?

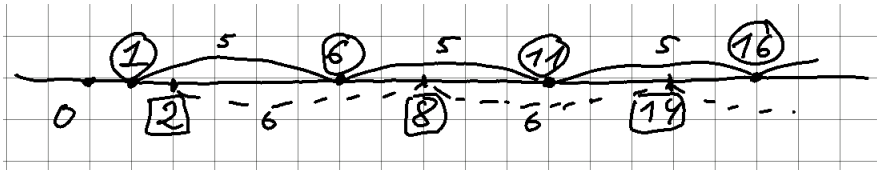
▷ Остаток не может быть больше делителя, так что делитель нужно выбирать побольше. Но если делитель близок к 100, то остаток тоже будет маленьким. Попробуем 51, тогда остаток 49. Может ли быть остаток больше? Если делитель 50 или меньше, то нет. Если 52 или больше, то остаётся до 100 только 48 или меньше, так что тоже не получится. Ответ: 49 (при делении на 51). ◁

3.19 Начав движение по кольцевой дороге длиной 120 км, машина проехала 500 км. Сколько раз она проезжала мимо места старта? (Сам старт не считается за проезд мимо старта.) Сколько километров она проехала после того, как была в точке старта в последний раз? Как это связано с делением с остатком?

▷ Движение по кольцевой дороге можно заменить на наматывание нитки на окружность. Если длина окружности 120, а нитки — 500, то будет четыре полных витка и ещё кусок длиной 20. ◁

• Вообще взятие остатка по модулю k — это, если можно так выразиться, наматывание числовой оси на окружность длины k.

3.20 Отметьте на числовой оси положительные числа, дающие остаток 1 при делении на 5. (С какими промежутками они идут?) Теперь отметьте другим цветом числа, дающие остаток 2 при делении на 6. Найдётся ли общее число (отмеченное двумя цветами)?

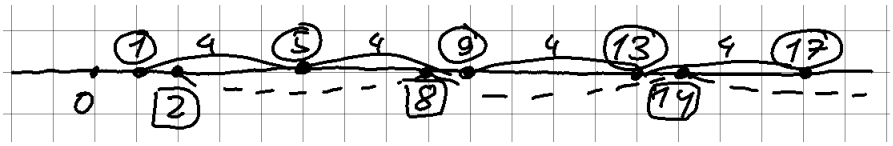


▷ Остаток 1 при делении на 5 дают числа 1, 6, 11, 21, 26, ...; они идут с промежутком 5. (Говорят, что они образуют *арифметическую прогрессию с разностью* 5.)

Остаток 2 при делении на 6 дают числа 2, 8, 14, 20, 26, ... Видно, что есть общее число 26. ◁

• Если не ограничиваться положительными числами, то можно заметить общее число -4, и прибавить к нему 30, кратное и 5, и 6. Получится как раз 26.

3.21 Отметьте на числовой оси положительные числа, дающие остаток 1 при делении на 4. Теперь отметьте другим цветом числа, дающие остаток 2 при делении на 6. Найдётся ли общее число (отмеченное двумя цветами)?



▷ Можно долго рисовать соответствующие прогрессии на числовой оси, но пересечения всё не будет и не будет. И можно понять почему: числа вида $4k + 1$ нечётные, а числа вида $6k + 2$ — чётные. ◁

• Мы ещё вспомним эту задачу, когда будем обсуждать «китайскую теорему об остатках».

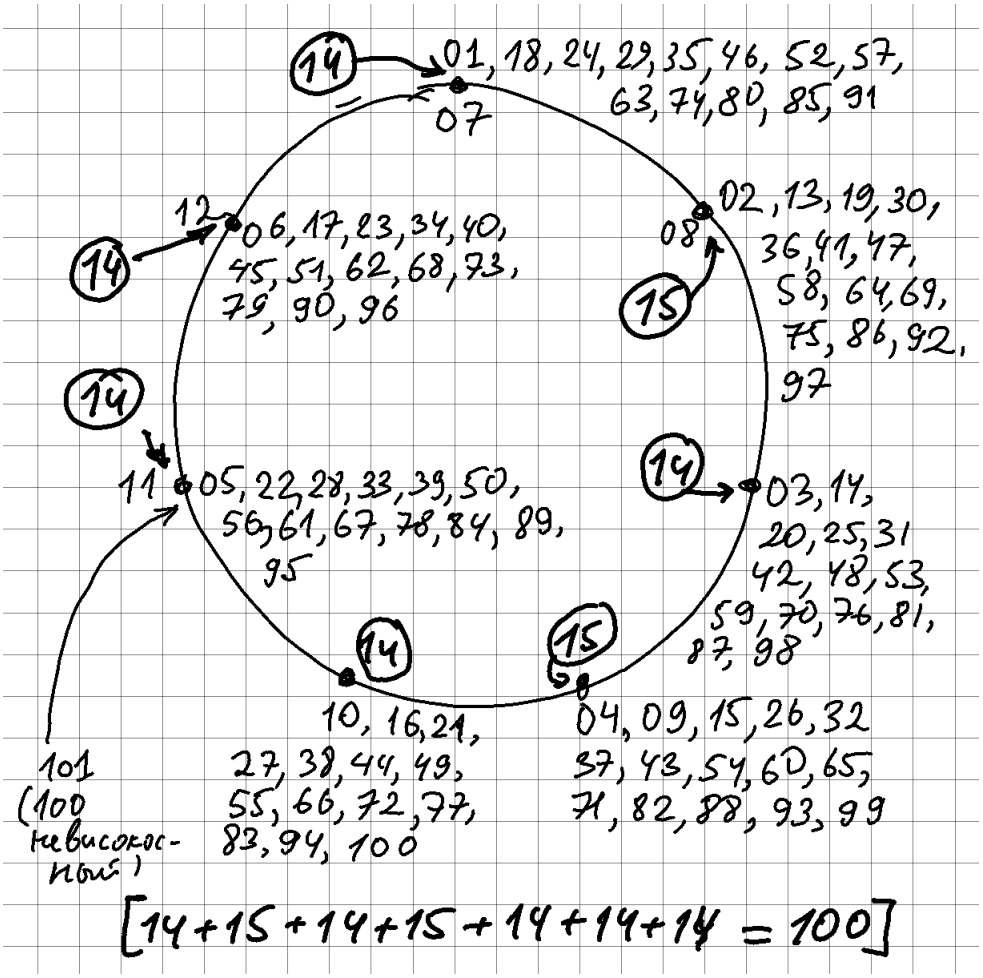
3.22* Если нынешний календарь (см. задачу 1) не будет меняться, на какие дни недели будет чаще всего приходиться новый год (1 января)?

▷ Как мы уже обсуждали, длина года повторяется с периодом 400 лет: високосные года — это те, которые делятся на 4, но не на 100, или уже тогда на

400. Оказывается, что общее число дней в этом периоде кратно 7. Проверим это: $365 \cdot 400$ обычных дней по модулю 7 даёт $400 \bmod 7$, то есть 1. Ещё надо добавить 97 високосных лет ($= 100 - 4 + 1$), всего будет $1 + 97 \bmod 7$, то есть 0.

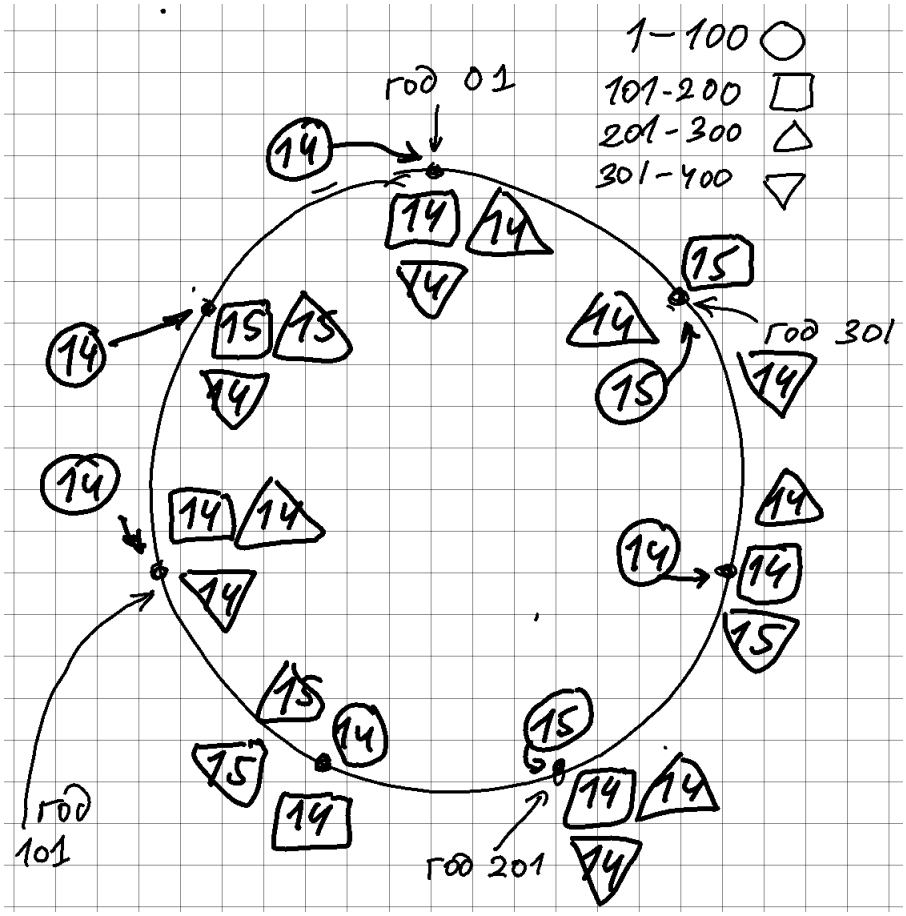
Таким образом, в следующем 400-летнем цикле всё будет повторяться — и потому важно понять, с каких дней недели чаще начинается год *в пределах одного цикла*.

Нарисуем круг, изображающий дни недели по часовой стрелке, и выберем верхнюю точку как условное начало для 2001 года (или для первого года — вообразив, что тогда григорианский календарь уже был, хотя на самом деле он был введён папой Григорием в XVI веке).

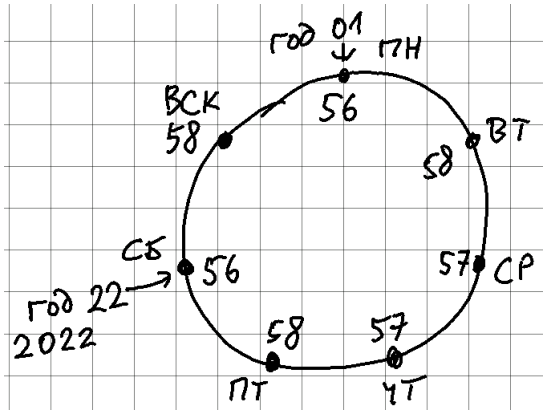


Дальше будем расставлять года, учитывая, что невисокосный год сдвигает на 1, а високосный на 2 (так что три коротких шага по часовой стрелке череду-

ются с одним длинным). Отметим, на что придётся 2101 (или 101) год, и ещё запомним, что 2022 год начинается с того же дня. Затем посчитаем и обведём в жирный кружочек число лет в период 2001 – 2100, которые начинаются с соответствующего дня. Сами годы теперь можно забыть:



В три следующих столетия тот же цикл 14–15–14–15–14–14–14 будет начинаться с других дней (каждое столетие смещает на два дня против часовой стрелки). Напишем эти числа в квадратиках и треугольниках двух видов и сложим результаты за все четыре столетия цикла.



Остаётся вспомнить, где был 2022 год и что первого января 2022 была суббота (задача 1), и получается ответ: понедельники и субботы за цикл встречаются 56 раз, среды и четверги по 57 раз, а вторники, пятницы и воскресенья — 58 раз. (Проверим, кстати: $56 \cdot 2 + 57 \cdot 2 + 58 \cdot 3$ действительно равно 400.)

Так будет в каждом цикле, так что мы можем ответить на вопрос задачи: первое января чаще всего приходится на вторники, пятницы и воскресенья (в $58/400 = 14{,}4\%$ доле всех случаев). ◁

3.23* На столе лежат книги (больше одной и меньше 100). Если их связывать в пачки по 3, то останется одна книга. То же самое (останется одна книга), если связывать по 4, по 5 и по 6. Сколько книг лежит на столе? (Достаточно указать один вариант.)

▷ Если одну книгу временно отложить, то число оставшихся (по условию положительное) будет делиться на 2, 3, 4, 5, 6. Например, годится число 60, так что книг могло быть 61.

На самом деле ответ единственный: числа, делящиеся на 2 и 5, имеют последнюю цифру 0, а числа 10, 20, 30, 40, 50, 70, 80, 90 не подходят). ◁

3.24* На столе лежат книги (больше одной и меньше 500). Если их связывать в пачки по 3, то останется одна книга. То же самое (останется одна книга), если связывать по 4, по 5 и по 6. А если связывать по 7, то ни одной не останется (все разойдутся по пачкам). Сколько книг лежит на столе? (Достаточно указать один вариант.)

▷ Если одну книгу отложить, то должно получиться число, кратное 3, 4, 5, 6. Годится любое кратное 60. Значит, достаточно найти число вида $60k+1$, которое делится на 7. Такое число есть: $301 = 43 \cdot 7$. (На самом деле это единственная возможность: как мы увидим, общие кратные 3, 4, 5, 6 обязательно делятся на 60,

а из чисел вида $60k+1$ до 500 подходит только 301, следующее будет $301+60\cdot 7 = 721$.) ◁

• Неполное частное (целое число, которое получается при делении с остатком) можно получить иначе: возьмём обычное частное (целое или дробь) и возьмём его *целую часть*. Скажем, $7/3 = 2\frac{1}{3}$, и здесь целая часть 2 (и остаётся $1/3 =$ остаток/делитель).

Целую часть можно определить как «округление вниз» до ближайшего (меньшего) целого числа. Её обозначают $\lfloor x \rfloor$, так что, скажем,

$$\lfloor \frac{7}{3} \rfloor = \lfloor 2\frac{1}{3} \rfloor = 2, \quad \text{но} \quad \lfloor -\frac{7}{3} \rfloor = \lfloor -2\frac{1}{3} \rfloor = -3.$$

Если число уже и так целое, то его целая часть равна самому этому числу.

3.25* Докажите, что для целых положительных чисел a, b, c всегда выполняется равенство

$$\left\lfloor \left\lfloor \frac{a}{b} \right\rfloor / c \right\rfloor = \left\lfloor \frac{a}{bc} \right\rfloor.$$

▷ Как ни странно, это трудно объяснить строго и коротко одновременно. Кажется, проще всего сказать так: для целого k и произвольного x условия $k \leqslant x$ и $k \leqslant \lfloor x \rfloor$ равносильны (по определению целой части), поэтому для любого целого k можно написать цепочку эквивалентностей

$$k \leqslant \left\lfloor \left\lfloor \frac{a}{b} \right\rfloor / c \right\rfloor \Leftrightarrow k \leqslant \left\lfloor \frac{a}{b} \right\rfloor / c \Leftrightarrow kc \leqslant \left\lfloor \frac{a}{b} \right\rfloor \Leftrightarrow kc \leqslant \frac{a}{b} \Leftrightarrow k \leqslant \frac{a}{bc} \Leftrightarrow k \leqslant \left\lfloor \frac{a}{bc} \right\rfloor.$$

(мы пользуемся тем, что k и kc целые). А если у двух целых чисел одни и те же целые числа, их не превосходящие, то они равны (каждое не больше себя, и потому не больше другого). ◁

3.26 Докажите, что произведение любых 5 последовательных натуральных чисел делится на 5 (и вообще произведение любых k последовательных натуральных чисел делится на k).

▷ Мы уже видели эту задачу при $k = 2$ и замечали, что из двух последовательных чисел всегда (ровно) одно чётное. Так и здесь: остатки идут по кругу, и их k штук, так что они заполнят весь круг (и один из остатков будет равен нулю). А если в произведении один сомножитель делится на k, то и всё произведение делится на k. ◁

• На самом деле произведение k последовательных натуральных чисел делится не только на k, но и на $k! = 1 \cdot 2 \cdot \ldots \cdot k$. Например, произведение любых

трёх подряд идущих чисел делится на 6 (=3!). Это можно доказать комбинаторно: $n(n-1)(n-2)/6$ равно числу способов выбрать из n человек трёх дежурных (и аналогично для k). Другой способ доказательства — считать простые множители, о которых мы говорим дальше.

4. Арифметика остатков

4.1 Число x даёт при делении на 7 остаток 5. Какой остаток дают при делении на 7 число $x+4$? число $2x$? число $4x+9$? число x^2-x? число x^3? число x^{100}?

▷ По условию $x = 7k+5$ для некоторого k. Тогда (1) $x+4 = 7k+9 = 7(k+1)+2$ и даёт остаток 2 при делении на 7. Далее, (2) $2x = 7\cdot 2k+10 = 7(2k+1)+3$ и потому $2x$ даёт остаток 3 при делении на 5. (3)$4x+9 = 4(7k+5)+7+2 = 4\cdot 7k+4\cdot 5+7+2 = 7\cdot 4k+29 = 7\cdot(4k+4)+1$, так что остаток равен 1. (4) $x^2-x = (7k+5)^2-(7k+5) = 7k(7k+5)+5(7k+5)-7k-5 = 7k(7k+5)+5\cdot 7k+5\cdot 5-7k-5 = 7(k(7k+5)+5k-k)+20 = 7(\ldots)+14+6 = 7(\ldots+2)+6$, так что остаток снова равен 6. (5) $x^3 = (7k+5)^3 = (7k+5)(7k+5)(7k+5)$. В этом выражении, если раскрыть скобки, все члены будут кратны 7, и их можно даже не выписывать, кроме одного $5\cdot 5\cdot 5 = 125 = 17\cdot 7+6$, так что остаток равен 6. Для x^{100}: будем последовательно выписывать разные степени: $x, x^2, x^3, x^4, x^5, x^6, x^7, \ldots$ дают остатки $5, 4, 6, 2, 3, 1, 5\ldots$ и дальше всё повторяется с периодом 6, так что x^{100} будет давать тот же остаток, что и x^4 (разница 96 в степенях делится на 6), то есть 2. ◁

По существу, мы систематически выбрасываем кратные 7, потому что они не влияют на ответ. Вообще вместо какого-то x, дающего остаток 5 при делении на 7, можно взять число 5, и получить ответ почти сразу. Мы сейчас объясним, почему это законно.

Определение. Говорят, что два числа x и y *сравнимы по модулю* n, если их разница делится на n.

Здесь n — целое положительное число (мы на него делим). Не имеет значения, из какого числа вычитать какое: если $b-a$ делится на n, то и $(a-b) = -(b-a)$ тоже делится на n (только частное меняет знак).

Запись: $x \equiv y \pmod{n}$; знак $\equiv$ читают как «сравнимы» или «эквивалентны», это синонимы (значат одно и то же).

Математики говорят, что отношение сравнимости (по данному модулю) является *отношением эквивалентности*. На их языке это означает выполнение трёх свойств:

- *рефлексивность*: каждое число эквивалентно самому себе;
- *симметричность*: если x эквивалентно y, то y эквивалентно x;
- *транзитивность*: если x и y эквивалентны z, то x эквивалентно y.

Эти три свойства гарантируют возможность разбиения всех объектов на непересекающиеся *классы эквивалентности*, при этом элементы одного класса будут эквивалентны друг другу, а разных — нет. В самом деле, для каждого x рассмотрим все элементы, эквивалентные x, они все эквивалентны друг другу (транзитивность), и среди них есть x. Элементы двух классов не эквивалентны друг другу (иначе классы совпадают по симметричности и транзитивности).

4.2 Закончите фразу: «два числа x и y сравнимы по модулю n, если их остатки...». Проверьте свойства отношения эквивалентности (рефлексивность, симметричность, транзитивность). Сколько будет классов эквивалентности?

▷ «...при делении на n равны». Отсюда очевидны все свойства отношения эквивалентности. Классов будет столько, сколько различных остатков, то есть n. ◁

Возможность систематического выбрасывания кратных n при действиях по модулю n гарантируется такой задачей:

4.3 Докажите, что если $a \equiv b \pmod n$, то $a + c \equiv b + c \pmod n$ и $ac \equiv bc \pmod n$. Докажите, что если $a \equiv b \pmod n$ и $b \equiv c \pmod n$, то $a \equiv c \pmod n$.

▷ (1) Если $b - a$ делится на n, то $(b + c) - (a + c)$ делится на n, потому что это то же самое число. (2) Здесь $bc - ac = (b - a)c$ делится на n, потому что один сомножитель делится на n. (3) Если $b - a$ делится на n, а также $c - b$ делится на n, то и сумма $(b - a) + (c - b) = c - a$ делится на n. ◁

4.4 Докажите, что если $a \equiv b \pmod n$ и $c \equiv d \pmod n$, то $a+c \equiv b+d \pmod n$ и $ac \equiv bd \pmod n$.

▷ Можно заметить, что если $b = a + kn$ и $d = c + ln$, то $b + d = a + c + (k + l)n$, поэтому $b + d \equiv a + c \pmod n$. Для произведения $bd = (a + kn)(c + ln) = ac + n(k + l + kln)$, поэтому $bd \equiv ac \pmod n$.

Но можно и проще: предыдущая задача позволяет заменять в сумме одно слагаемое на сравнимое по модулю n, и сумма не меняется по модулю n, после чего можно заменить и другое, она снова не изменится. Аналогично и для произведения. ◁

Эта задача показывает, что если в любом арифметическом выражении, содержащем сложение и умножение, заменить какие-то члены на

эквивалентные по модулю n (один или много раз), то значение выражения тоже заменится на эквивалентное. Математики сказали бы, что арифметические операции «корректно определены на классах эквивалентности».

▷ Можно сказать, что выбрав модуль n для сравнений, мы надеваем специальные очки, через которые мы не отличаем числа, различающиеся на кратные n, и потому позволяем себе всюду выбрасывать числа, кратные n (прибавлять и вычитать любое кратное n). Правильное вычисление остаётся правильным и в этих очках — но и неправильное, в котором ошибки кратны n, тоже покажется правильным — хотя правильным в нём будет только остаток по модулю n. ◁

4.5 Можно ли, продолжая предыдущую задачу, утверждать, что в её предположениях $a - c \equiv b - d \pmod{n}$ и $a/c = b/d \pmod{n}$?

▷ Первое верно (например, можно заметить, что $-c \equiv -d \pmod{n}$, умножая сравнение на -1, а потом сложить). Второе же не имеет смысла (по крайней мере пока): числа a/c и b/d вообще могут быть не целыми, так что для них сравнение по модулю не определено. (И если даже случайно и получатся целые, то тоже может быть неверно: $5 \equiv 10 \pmod{5}$, но $5/5 \not\equiv 10/5 \pmod{5}$.) Как и когда имеет смысл делить сравнения, мы ещё обсудим. ◁

4.6 Найдите остаток от деления на 7 чисел 8^{100} и 6^{100}.

▷ Поскольку $8 \equiv 1 \pmod{7}$ и $6 \equiv -1 \pmod{7}$, можно с тем же успехом искать остаток от деления 1^{100} и $(-1)^{100}$, оба числа равны 1, так что оба искомых остатка равны 1. ◁

4.7 Найдите остаток от деления числа 2^{100} на 7.

▷ Поскольку $2^3 \equiv 1 \pmod{7}$, то множители 2^3 по модулю 7 можно сокращать, а $100 = 3 \cdot 33 + 1$, поэтому останется единственный множитель 2, который и будет искомым остатком. ◁

4.8 Будем брать степени какого-то фиксированного числа a по модулю b (другими словами, брать остатки $a^k \bmod b$). С какого-то момента они начинают повторяться по циклу (одна и та же группа повторяется снова и снова). Почему так обязательно случится?

• Скажем, для степеней двойки по модулю 10 (последние цифры): 1, 2, 4, 8, [1]6, [3]2, [6]4, [12]8,...: группа $2, 4, 8, 6$ повторяется (а начальная единица — нет).

▷ Каждое следующее число получается из предыдущего умножением на a. Рано или поздно остатки по модулю b повторятся, и потом уже всё пойдёт по тому же пути (потому что мы можем умножать остаток на a по модулю b). ◁

4.9 Докажите, что число $2^{1001} + 3^{1001}$ делится на 5.

▷ Можно просто вычислить соответствующие остатки, как в предыдущей задаче. Но можно и сразу заметить, что $3 \equiv (-2) \pmod 5$, поэтому выражение сравнимо с $2^{1001} + (-2)^{1001} = 0$. (Внимание: тут важно, что показатель степени 1001 нечётный.) ◁

• То же самое верно (и по тем же причинам) для любых целых положительных a и b: число a^n+b^n при нечётном n делится на $a+b$. Это же можно усмотреть и из формулы

$$a^n + b^n = (a + b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \ldots - ab^{n-2} + b^{n-1}),$$

которая верна при нечётном n и проверяется перемножением скобок в правой части, там всё посокращается. (Что будет при чётном n?)

4.10 Докажите, что если $a \equiv b \pmod n$, то $a \equiv b \pmod{n'}$ для любого n', делящего n.

▷ Если число $a - b$ делится на n, то оно делится и на любой делитель n' числа n. ◁

4.11 Докажите, что если $a \equiv b \pmod c$, то $ka \equiv kb \pmod{kc}$ (здесь мы предполагаем, что k и c — положительные целые числа). Верно ли обратное?

▷ Если $a - b$ делится на c, то число $(a - b)/c$ целое. Но это же число можно записать и как $k(a-b)/kc$, так что $k(a-b)$ делится на k. То же самое в обратном направлении: если $ka - kb$ делится на kc, то $(ka - kb)/kc = (a - b)/c$ будет целым. Так что и обратное верно. ◁

4.12 Можно ли сокращать сравнения на ненулевой множитель? Верно ли, что если $ka \equiv kb \pmod c$, а $k \not\equiv 0 \pmod c$, то $a \equiv b \pmod c$?

▷ Не всегда. Например, $2 \cdot 3 \equiv 2 \cdot 8 \pmod{10}$, и $2 \not\equiv 0 \pmod{10}$, но $3 \not\equiv 8 \pmod{10}$. ◁

• Мы потом увидим, что иногда сокращать можно: если сокращаемый множитель взаимно прост с модулем сравнения.

4.13 Покажите, что записанное обычным образом (в десятичной системе) целое положительное число сравнимо по модулю 9 с суммой своих цифр. Как из этого вывести признаки делимости на 9 и на 3? (Они говорят, что число делится на 9 [на 3] тогда и только тогда, когда сумма его цифр делится на 9 [на 3].)

▷ Числа $10, 100, 1000, \ldots$ все сравнимы с 1 по модулю 9 (потому что $100\ldots0 - 1 = 99\ldots9$ делится на 9. Можно ещё заметить, что $10 \equiv 1 \pmod 9$ и потому $10^k \equiv 1^k \equiv 1 \pmod 9$.

Поэтому, скажем,

$$2357 = 2{\cdot}1000+3{\cdot}100+5{\cdot}10+7{\cdot}1 \equiv 2{\cdot}1+3{\cdot}1+5{\cdot}1+7{\cdot}1 \equiv 2+3+5+7 \pmod 9,$$

и вообще любое число сравнимо со своей суммой цифр по модулю 9, так что если одно делится на 9, то и другое тоже. Сравнимость по модулю 9 влечёт за собой сравнимость по модулю 3, так что для 3 годится то же рассуждение. ◁

4.14* Можете ли вы предложить какие-то признаки делимости на 4, 8, 11, которые бы реально упрощали выяснение делимости? (Имеется в виду — без калькулятора и даже по возможности без бумаги и карандаша.)

▷ Для проверки делимости на 4 можно оставить только две последние цифры (потому что 100 делится на 4), для проверки делимости на 8 — три последние (и их уже делить честно). Поскольку $10 \equiv -1 \pmod{11}$, то для проверки делимости на 11 можно вычислить сумму цифр с чередующимися знаками (из суммы цифр на чётных местах вычесть сумму на нечётных). ◁

Иногда на обложках тетрадей печатают таблицу умножения натуральных чисел. (Таблицу сложения не печатают — видимо, считают, что это слишком просто.) Ясно, что в неё нельзя включить все возможные пары сомножителей, их бесконечно много. Однако для остатков по модулю n (если мы не различаем сравнимые по модулю n числа) такие таблицы составить можно, это будет таблица $n \times n$ (не считая заголовка). Мы уже по существу составляли такую таблицу для $n = 2$ с «чётом» и «нечетом»; теперь мы могли бы сказать, что это остатки 0 и 1 и каждый из остатков символизирует все сравнимые с ним числа.

4.15 Составьте такие таблицы (сложения и умножения) для $n = 3, 4, 5, 6, 7, 10$. (Их даже имеет смысл сохранить для следующих задач.)

▷ Вот эти таблицы (сначала для модулей 3, 4, 5, потом для 6, 7 и потом для 10). Последнюю таблицу можно иногда увидеть как таблицу умножения на школьных тетрадках, если смотреть только на последнюю цифру произведения.

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

◁

4.16 Глядя в таблицу умножения по модулю 3, найдите в ней доказательство такого утверждения: если произведение двух целых чисел делится на 3, то одно из них делится на 3. Верно ли аналогичное утверждение для 4, 5, 6, 7, 10?

▷ Интересующее нас утверждение можно переформулировать так: если оба сомножителя не делятся на 3, то и произведение не делится на 3. Другими словами, нас интересует произведение *ненулевых* остатков, так что на первую строку и первый столбец (не считая тех, что с множителями, то есть в квадратной части таблицы) не смотрим. А в остальных четырёх клеточках только 1 и 2, нулей нет.

Для $n = 4$ есть нуль $2 \cdot 2$, для $n = 6$ нули тоже есть (скажем, $2 \cdot 3$), для $n = 10$ тоже (скажем, $2 \cdot 5$). А для $n = 5$ и $n = 7$, как можно убедиться, посмотрев на таблицы, нулей нет. ◁

4.17 Какова может быть последняя цифра положительного целого числа n в десятичной записи, чтобы число n^2 кончалось на ту же цифру?

▷ Смотрим на диагональ (произведение чисел на себя) в последней таблице, и находим ответы (клетки, где стоит то же число, что и в заголовке таблицы): $0, 1, 5, 6$. ◁

4.18* Найдите трёхзначное число, квадрат которого оканчивается на это число (то есть $n^2 \equiv n \pmod{1000}$). (Числа 000 и 001 за трёхзначные не считаются.)

▷ Удобно искать нужное число с конца. Мы уже знаем, что оно должно заканчиваться на $0, 1, 5, 6$. Попробуем, скажем, 5 (тогда уж точно 001 и 000 не получатся). Какая может быть предпоследняя цифра?

$$(10k + 5)^2 = 100k^2 + 100k + 25$$

так что квадрат числа, оканчивающегося на 5, всегда оканчивается на 25, и со второй цифрой выбора нет. С третьей:

$$(100k + 25)^2 = 10000k^2 + 5000k + 625,$$

так что квадрат числа, оканчивающегося на 25, оканчивается на 625. Получаем ответ: $625^2 = 390\,625$.

Точнее сказать, это один из ответов. В задаче про это не спрашивалось, но можно пытаться найти все: $x^2 \equiv x \pmod{1000}$ означает, что $x^2 - x = x(x-1)$ делится на 8 и на 125. Если $x(x-1)$ делится на 8, то один из сомножителей (который чётен) делится на 8, получаем, что $x \equiv 0$ или $x \equiv 1$ по модулю 8. То же самое по модулю 125. Получаем 4 комбинации остатков по модулю 8 и 125 (см. дальше «китайскую теорему об остатках»), и четыре ответа: 000, 001, 625, 376 ($376^2 = 141\,376$) ◁

4.19 Какие последние цифры бывают у целых положительных чисел, которые делятся на 6? Какие остатки может давать число, делящееся на 2, при делении на 6? (Ответы на оба вопроса можно увидеть прямо по таблицам умножения, если правильно в них посмотреть.)

▷ Надо посмотреть в таблице умножения по модулю 10 тот ряд (столбец или строку), где умножают на 6, там стоят числа 0, 2, 4, 6, 8.

Для таблицы умножения по модулю 6 надо посмотреть ряд, где множат на 2, там стоят числа 0, 2, 4. ◁

4.20* Докажите, что квадрат одного целого числа не может быть втрое больше квадрата другого целого числа (за исключением случая, когда оба числа равны нулю).

▷ Это соответствует иррациональности числа $\sqrt{3}$. ◁

▷ Пусть $x = a^2 = 3b^2$, и $x \neq 0$. Возьмём минимальное такое x. Раз a^2 делится на 3, то и a делится на 3 (потому что ненулевые остатки в квадрате дают ненулевые), $a = 3z$. Тогда $a^2 = 9z^2 = 3b^2$, и $x/3 = 3z^2 = b^2$, так что x не минимальное — противоречие. ◁

4.21 Уравнение $x^2+y^2 = 1003$ не имеет решений в целых числах (другими словами, число 1003 нельзя представить в виде суммы двух квадратов). Как в этом убедиться, не перебирая все варианты?

▷ Можно посмотреть на него по модулю 4: любой квадрат даёт остаток 0 или 1 при делении на четыре (в зависимостости от чётности), поэтому сумма двух квадратов может давать остаток 0, 1, или 2, но не 3 (как у 1003) ◁

▷ А что для других чисел (не только 1003)? Математики знают ответ (в терминах разложения на простые множители, о котором дальше): все простые числа вида $4k + 3$, входящие в разложение n, должны входить в чётной степени (парами), тогда можно представить n в виде суммы двух квадратов (а иначе — нельзя). Но это не так просто доказать. ◁

5. Простые и составные числа

Целое число $p > 1$ называется *простым*, если оно не имеет делителей, кроме 1 и самого себя. Если же такие делители есть, то число называется *составным*.

• Мы использовали здесь букву p, её часто используют для простых (английское prime) чисел. Но, конечно, в математике такого жёсткого правила нет (это в физике m почти всегда масса, а g — ускорение свободного падения).

Напомним кстати, что по нашим соглашениям делители должны быть целыми положительными числами, так что -1 или $-p$ делителем не будет.

5.1 Докажите, что целое число $n > 1$ является составным тогда и только тогда, когда его можно представить в виде произведения двух меньших положительных целых чисел.

• Странное выражение «тогда и только тогда» означает, что надо доказать две вещи: (1) если число n составное (не является простым, то есть имеет делитель помимо 1 и n), то его можно представить в виде произведения двух меньших положительных целых чисел и (2) если число n можно представить в виде произведения двух меньших положительных целых чисел, то оно не является простым (имеет делитель помимо 1 и n).

Оговорка про положительность сомножителей нужна: число 3 простое, но равно произведению $(-3) \cdot (-1)$.

▷ Оба утверждения по существу очевидны, тем не менее скажем подробно.

Если n составное, то оно имеет некоторый делитель m, отличный от 1 и n. Делимость n на m значит, что $n = mk$ для некоторого k. Оба числа m, k целые и положительные, не совпадают с 1 и n (про m это мы знаем; если k равно 1 или n, то m равно n или 1 соответственно), их произведение равно n, поэтому оба меньше n.

Напротив, если $n = ab$, где $0 < a, b < n$, то a является (по определению) делителем n. По предположению $a < n$ и потому a не совпадает с n. Если же $a = 1$, то $b = n$, что противоречит предположению $b < n$. Поэтому n имеет делитель a, помимо 1 и n, и потому не простое (составное). ◁

• Будет ли число 1 простым или составным? Обычно его не считают ни таким, ни сяким (как и, скажем, 0, или $1/3$, или -5, или π), в нашем определении *классифицируются на простые и составные только целые числа, большие* 1. Это удобно в некоторых формулировках.

5.2 Покажите, что *минимальный* делитель любого числа n (не считая 1) всегда простой. (Если n простое, то этот минимальный делитель совпадает с самим n.)

▷ Если какой-то делитель не простой, то множители, на которые он разлагается, будут меньшими делителями — значит, делитель этот не минимальный. ◁

5.3 Покажите, что любое составное число n имеет делитель, больший 1, но не превосходящий $\sqrt{n}$. Как этот факт можно использовать при проверке простоты?

▷ Делители числа n группируются в пары (произведение в каждой паре равно n): если a делит n, то по определению $n = ab$, и b тоже делит n. Ясно, что в паре оба члена не могут быть больше $\sqrt{n}$, иначе их произведение будет больше n.

Отсюда следует, что при проверки простоты достаточно проверить делители до $\sqrt{n}$ включительно. Если их нет, то и дальше уже не будет — вплоть до самого n. ◁

5.4 Покажите, что количество делителей у любого положительного целого n не превышает $2\sqrt{n}$.

▷ В предыдущей задаче мы видели, что делители группируются в пары, и меньшие члены пар не больше $\sqrt{n}$. Значит, и самих пар не больше $\sqrt{n}$. (Может быть делитель, парный самому себе, но тогда в этой «паре» только одно число, и делителей только меньше.) ◁

5.5* Покажите, что число $2^{128} - 1$ — составное. Найдите его разложение в произведение семи целых чисел, больших 1.

▷ Можно последовательно применять формулу $n^2 - 1 = (n + 1)(n - 1)$ к $n = 2^{64}$, $n = 2^{32}$ и так далее, получится

$$2^{128} - 1 = (2^{64} + 1)(2^{32} + 1)(2^{16} + 1)(2^8 + 1)(2^4 + 1)(2^2 + 1)(2 + 1)(2 - 1)$$

(восьмая скобка, равная единице, написана для красоты, она в число семи множителей не входит). ◁

• На самом деле два первых сомножителя можно разложить дальше, но это сразу не видно. (Числа такого вида называются *числами Ферма*.)

5.6* Покажите, что число 999 991 составное, разложив его в произведение меньших. (Это можно сделать в уме, почти без вычислений.)

▷ Заметим, что $999\,991 = 1\,000\,000 - 9 = 1000^2 = 3^2 = 997 \cdot 1003$. (Можно и дальше разложить, но это уже не так сразу видно: 1003 делится на 17.) ◁

5.7 Число 2 простое и чётное. Бывают ли другие такие числа?

▷ Нет, конечно: у чётного числа есть делитель 2, и если само число не 2, то простым оно не будет. ◁

5.8 Числа 2 и 3 — соседние простые числа (отличающиеся на 1). Бывают ли другие такие пары?

▷ Нет: из двух соседних чисел одно должно быть чётным, и если оно просто, то это должно быть 2 (см. предыдущую задачу). ◁

5.9 Три простых числа $3, 5, 7$ идут через одно (следующее больше предыдущего на 2). Бывают ли другие такие тройки?

▷ Нет — это следует из того, что из трёх чисел, идущих через одно, всегда одно делится на 3. В самом деле, пусть это числа n, $n+2$, $n+4$. Посмотрим, какой остаток даёт при делении на 3. Если 0, то первое из трёх делится на 3, если 1, то второе, если 2, то третье. А простое число, делящееся на 3, может быть только 3. ◁

• Простые числа, отличающиеся на 2, называют «близнецами»: таковы, например, 9 и 11, 137 и 139, и так далее. Известны очень большие пары простых близнецов, с сотнями тысяч цифр — но пока никто не может доказать, что их бесконечно много. (Опровергнуть тоже не могут.)

Самих по себе простых чисел, как мы увидим скоро, бесконечно много.

5.10 Числа $8, 9, 10$ — три подряд идущих составных числа. Найдите 5 подряд идущих составных чисел. Найдите 7 подряд идущих составных чисел.

▷ Искомые примеры небольшие, и их можно найти, просто смотря на все числа по порядку: $24, 25, 26, 27, 28$ — пять идущих подряд составных чисел. А $90 = 9 \cdot 10, 91 = 7 \cdot 13, 92 = 46 \cdot 2, 93 = 31 \cdot 3, 94 = 47 \cdot 2, 95 = 19 \cdot 5, 96 = 48 \cdot 2$ — семь подряд идущих составных чисел. ◁

5.11* Докажите, что можно найти и 100 подряд идущих составных чисел, и вообще любое количество подряд идущих составных чисел.

▷ Если какое-то число a делится на 2, 3, 4, 5, 6,..., 101, то все числа $a+2$, $a+3$, $a+4$, $a+5$, $a+6$,..., $a+101$ будут составными: скажем, $a+47$ делится на 47. А их как раз 100 подряд. Остаётся подобрать такое a. Можно просто взять произведение

всех этих чисел $2 \cdot 3 \cdot 4 \cdot \ldots \cdot 101$ в качестве a, потому что произведение делится на все свои множители. ◁

• Бывают и меньшие — скажем, незачем умножать на 2, если мы умножаем на 4. Математики бы сказали, что вместо 101! можно взять наименьшее общее кратное чисел от 2 до 101.

5.12* Выпишем в порядке возрастания нечётные простые числа: 3, 5, 7, 11, 13, 17, 19, 23,.... Докажите, что среднее арифметическое двух соседних чисел в этой последовательности — всегда составное число.

▷ Эта задача сильно проще, чем кажется на первый взгляд: среднее арифметическое двух соседних чисел лежит между ними, а там простых чисел нет, потому что они были соседними. (Поскольку соседи были простыми нечётными, то сумма их чётна, и среднее арифметическое целое. Надо ещё заметить, что оно не может быть 2.) ◁

• Почему простые числа называют простыми, не очень понятно (по-английски, кстати, они prime, а не simple). Легче объяснить, почему составные называют составными (по-английски composite): их можно *составить* (compose) из меньших множителей, скажем, 6 состоит из 2 и 3 ($6 = 2 \cdot 3$, 30 состоит из 2, 3 и 5, и так далее.

5.13 Докажите, что любое целое число, большее 1, можно *разложить на простые множители*, то есть представить в виде произведения простых сомножителей. (Одно и то же простое число может входить в произведение несколько раз. Допускаются и «произведения», состоящие из одного сомножителя.)

▷ Если число $n > 1$ простое, его мы считаем произведением из одного сомножителя. Если оно составное, то по определению его можно представить в виде произведения ab двух меньших чисел, которые сами могут быть простыми или составными. Если они простые, то разложение уже получено, если составные, то повторим рассуждение и разложим их на меньшие, и так далее. (Процесс закончится, потому что на каждом шаге числа уменьшаются.) ◁

▷ Это называют «рассуждением по индукции»: мы доказываем, что n можно разложить на множители, предполагая, что для меньших чисел (в нашем случае a и b) это утверждение уже известно. ◁

5.14 Разложите на простые множители числа 1000 и 1001.

▷ Про 1000 сразу ясно: $1000 = 10^3 = 2\cdot5\cdot2\cdot5\cdot2\cdot5 = 2^3\cdot5^3$. Про 1001 надо пробовать разные делители, но (к счастью для нас) они оказываются небольшими: $7 \cdot 11 \cdot 13$. ◁

Составное число можно по-разному разбить на сомножители: скажем, $30 = 2 \cdot 15 = 3 \cdot 10$. Но если разлагать дальше, пока части не станут простыми ($15 = 3 \cdot 5$, $10 = 2 \cdot 5$), то получится в итоге одно и то же разложение $2 \cdot 3 \cdot 5$. Это не случайно — можно доказать, что *любые два разложения на множители данного числа по существу одинаковы — отличаются лишь порядком множителей*. Это утверждение называется *теоремой об однозначности разложения на простые множители* (а иногда торжественно объявляется «основной теоремой арифметики»). Может показаться странным, но это не само собой разумеется и даже не так просто доказать (нам потребуется некоторая подготовка).

5.15 Дотошный ученик считает, что опроверг теорему об единственности разложения, обнаружив пример двух разложений.

$$78227 \cdot 244999 = 19165536773 = 99599 \cdot 192427$$

Прав ли он — и если неправ, то в чём его ошибка?

▷ Разложения правильные (проверьте!) — но вот только множители в них не простые, и на самом деле

$$\begin{aligned} 78227 &= 137 \cdot 571, \\ 244999 &= 337 \cdot 727, \\ 99599 &= 137 \cdot 727, \\ 192427 &= 337 \cdot 571. \end{aligned}$$

Если продолжить разложение, то получатся одни и те же четыре простых множителя. ◁

- «Задача нечестная — как можно найти эти множители, не зная их заранее?» Действительно, так сразу их не угадаешь, а проверять все довольно долго. Можно написать программу (или просто указать запрос типа `factor(78827)` на сайте `wolframalpha.com`), а можно воспользоваться алгоритмом Евклида для поиска общих множителей, о котором мы расскажем дальше.

5.16 Дано положительное целое число n (можно взять, скажем, 1000). (а) Докажите, что есть число, которое делится на все числа от 2

до n. (б) Докажите, что есть число, большее 1, которое даёт остаток 1 при делении на все числа от 2 до n. (в) Докажите, что есть число, большее 1, которое не делится ни на одно из чисел от 2 до n.

▷ Если перемножить все числа от 2 до n, получится число, которое на все эти числа (от 2 до n) делится. Если теперь прибавить единицу, то получится число, которое даёт при делении на все эти числа остаток 1 — и, значит, на них не делится. ◁

5.17 Докажите, что простых чисел бесконечно много. (Можно переформулировать это так: простые числа нигде не кончаются, для любого n есть простое число, большее n.)

• Это — одна из самых первых теорем теории чисел, она есть в знаменитых «Началах» Евклида. В книжке «Математическая смесь» Дж. Литлвуда (М.:Наука, 1990) автор спрашивает себя, какие настоящие математические результаты можно объяснить «с минимумом сырого материала», и пишет, что «“Общеизвестное” евклидово доказательство бесконечности множества простых чисел может, конечно, претендовать на первое место».

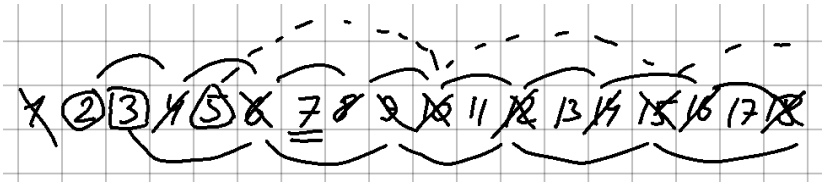
▷ Если бы все простые числа были меньше n, то какие были бы простые делители у числа из предыдущей задачи, которое не делится ни на одно из них? А хоть один-то простой делитель должен быть (само число, если нет других). ◁

• Вот как это излагает Литлвуд: «Евклидово доказательство бесконечности множества простых чисел может быть для профессионала сжато в одну строчку: если $p_1, \dots, p_n$ простые, то $1 + p_1 p_2 \dots p_n$ не делится ни на одно p_n».

5.18* Докажите, что остаток от деления любого простого числа на 30 будет либо 1, либо простое число.

▷ Если исходное простое число меньше 30, то оно и будет остатком. Пусть теперь оно больше 30. Тогда оно не делится ни на 2, ни на 3, ни на 5. Значит, и остаток не делится ни на 2, ни на 3, ни на 5. Какие есть составные числа до 30, которые не делятся ни на 2, ни на 3, ни на 5? Никаких (если наименьший простой делитель 7, то число будет минимум 49, так как должен быть ещё один простой делитель, не меньший 7). ◁

Как составить таблицу простых чисел? Можно написать все числа $1, 2, 3, 4, 5, 6, \dots$ подряд и выбросить составные (и единицу). Сначала выбросим все чётные, кроме 2. Потом — все кратные 3, кроме 3. Потом — кратные 5, кроме 5, и так далее. (Понятно, почему можно пропустить кратные четырём? потому что они уже учтены среди кратных двум.)



Такой процесс называют «решетом Эратосфена» (того самого, про которого рассказывают, что он первым измерил размер Земли, сравнивая тени в Александрии и Сиене). «Решетом» — потому что мы «просеиваем» простые числа. Один этап просеивания можно описать так: у нас уже найдены несколько первых простых чисел и вычеркнуты все их кратные. Берём наименьшее невычеркнутое число (не считая уже найденных простых), оно будет следующим простым, и вычёркиваем все его кратные.

5.19* (а) Почему наименьшее невычеркнутое число будет простым? (б) Как долго нужно продолжать этот процесс, если мы хотим составить таблицу простых чисел до 1000?

▷ (а) Если бы оно было составным, то имело бы *простой* делитель, меньший его самого, а меньшие простые числа уже найдены и все их кратные вычеркнуты. (б) Достаточно остановиться, вычеркнув все кратные 31. В самом деле, следующее простое число будет 37 и его квадрат больше 1000 — поэтому любое составное число до 1000 имеет простой делитель, меньший 37. ◁

5.20* Докажите, что при достаточно больши́х n (достаточно взять $n \geqslant 100$, например), простые числа составляют не больше трети от всех чисел 1 до n. Можно ли найти такое n, чтобы среди чисел от 1 до n не меньше 90% были бы составными? Тот же вопрос для 99%.

• Простые числа — дело тонкое, и на самые невинно звучащие вопросы ответ может оказаться неизвестным. Скажем, никто не знает, всякое ли чётное число, начиная с 4, представляется в виде суммы двух простых чисел (ни одного контрпримера не известно, но и не доказано, что их нет). Это утверждение называют *гипотезой Гольдбаха* (она сформулирована в 1742 году в переписке Христиана Гольдбаха и знаменитого Леонарда Эйлера).

▷ Первую часть легко проверить: в каждой шестёрке $6k, 6k+1, 6k+2, 6k+3, 6k+4, 6k+5$ при $n \geqslant 1$ четыре числа из шести заведомо составные (кроме второго и последнего), потому что делятся на 2 или на 3. Остаются неучтённые: $1, 2, 3, 4, 5$ (здесь три простых числа из пяти) и сколько-то в последней шестёрке (если она неполная, то там может быть максимум одно простое число). Чтобы скомпенсировать это, достаточно найти шесть неучтённых составных чисел, скажем 25, 35, 49, 55, 65, 75 (и есть ещё, скажем, 95).

Вторая часть: на самом деле можно найти любую долю, сколь угодно близкую к единице. Но доказать это не так просто. Подсчитаем долю чисел, которые останутся после k этапов просеивания в решете, то есть не делятся на первые k простых чисел $p_1, \ldots, p_k$ (как мы это делали для 2 и 3). Эти числа идут по циклу с периодом $p_1 \cdot \ldots \cdot p_k$, и доля их в этом периоде равна

$$\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{3}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right)$$

($p_1 = 2$, $p_2 = 3$, так что мы написали их явно). Это следует из «китайской теоремы об остатках», которую мы потом докажем. Надо показать, что при больши́х k это произведение может быть сильно меньше 1%, тогда числа в неполном последнем периоде и в первом периоде сильно дела не изменят.

Это доказывается с помощью такого удивительного приёма: умножим обе части на

$$B = \left(1+\frac{1}{2}+\frac{1}{2^2}+\ldots\right)\cdot\left(1+\frac{1}{3}+\frac{1}{3^2}+\ldots\right)\cdot\left(1+\frac{1}{p_k}+\frac{1}{p_k^2}+\ldots\right)$$

(сколько членов написать в каждой скобке, мы выберем потом). В левой части получится не больше 1, потому что

$$(1-x)(1+x+x^2+\ldots+x^m) = 1-x^{m+1} \leqslant 1$$

поэтому левая часть не больше $1/B$. А число B можно сделать сколь угодно большим, если взять достаточно много простых чисел и достаточно много слагаемых в каждой скобке в B. В самом деле, в произведении будут члены вида $1/m$ при любом m, которое разлагается на простые множители до p_k, и выбирая достаточно большое k и достаточно много членов внутри скобок, можно получить

$$B \geqslant 1+\frac{1}{2}+\ldots+\frac{1}{N}+\text{ещё что-то}$$

для любого N, и остаётся доказать, что гармонический ряд расходится, то есть сумма справа может быть сколь угодно большой. Это следует из того, что

$$\frac{1}{k+1}+\frac{1}{k+2}+\ldots+\frac{1}{2k} \geqslant \frac{1}{2k}+\frac{1}{2k}+\ldots+\frac{1}{2k} \geqslant \frac{1}{2}.$$

(В этом рассуждение даже не важно, что всякое число единственным образом разлагается на простые множители, если бы это вдруг было не так, то было бы только больше членов в правой части.) $\triangleleft$

6. Алгоритм Евклида

Однозначность разложения на множители (основную теорему арифметики) можно доказывать разными способами. Мы получим её как следствие *алгоритма Евклида вычисления наибольшего общего делителя* двух целых чисел.

▷ Это, пожалуй, не самый короткий, но самый естественный путь. Евклид — это тот самый древнегреческий Евклид, который написал первый в мире учебник геометрии, *Начала* — и там была не только геометрия. В частности, этот алгоритм (конечно, не называемый «алгоритмом» — это гораздо более позднее слово в часть арабского математика аль-Хорезми) там тоже был (для отрезков). ◁

Слова «наибольший общий делитель» (в применении к двум целым числам) надо понимать буквально. У каждого числа есть делители, и некоторые делители будут общими для двух чисел. Из них нужно выбрать самый большой.

Наибольший общий делитель чисел a, b обычно обозначают $\gcd(a, b)$ (от слов “greatest common divisor”), или по-русски $\text{НОД}(a, b)$.

6.1 А почему самый большой вообще есть? Не может ли так случиться, что какой общий делитель ни возьми, есть ещё больший?

▷ Да, такое тоже может быть: если оба числа равны нулю, то любое число будет делителем, а среди всех чисел нет наибольшего. Поэтому мы не определяем $\text{НОД}(0, 0)$. Но в остальных случаях — если одно из двух чисел ненулевое — все делители не превосходят модуля этого числа, так что среди них есть и наибольший. ◁

• В принципе можно искать наибольший общий делитель двух чисел перебором — взять ненулевое (выгодно взять меньшее по модулю) число и пробовать все делители от 1 до этого числа (точнее, его модуля). Но иногда можно обойтись и без этого.

Числа a и b называют *взаимно простыми*, если $\text{НОД}(a, b) = 1$.

6.2 С какими числами взаимно просто простое число p?

▷ Если p — простое число, то у него только два делителя 1 и p. Значит, и общими делителями могут быть только 1 и p. При этом 1 (который всегда общий делитель) будет наибольшим, когда p не является общим делителем. Отсюда ответ: со всеми, которые не делятся на p. ◁

6.3 Чему, согласно нашему определению, равно НОД $(a, 0)$ при $a \neq 0$?

▷ Нуль делится на что угодно, поэтому общими делителями будут все делители a, и наибольший из них будет a (точнее, $|a|$, поскольку a может быть отрицательным). ◁

6.4 Найдите НОД $(1230, 1231)$ и НОД $(123, 1231)$

▷ У чисел 1230 и 1231 нет никаких общих делителей, кроме 1 (и -1, если считать и отрицательные). Почему? Если оба числа 1230 и 1231 делятся на какое-то d, то и их разность должна делиться на d, а она равна 1, так что остаётся только $d = \pm 1$.

Про вторую пару: НОД $(123, 1231) = 1$, потому что все делители 123 являются также и делителями 1230, значит общих делителей у 123 и 1231 может быть только меньше, чем у 1230 и 1231. ◁

6.5 Какие значения может принимать НОД $(n, n + 6)$ при разных n? Как это значение зависит от n? [Указание: важен остаток от деления n на 6.]

▷ Ключевое наблюдение (в продолжение решения предыдущей задачи): *у пары* $(n, n + 6)$ *те же общие делители, что и у пары* $(n, 6)$. (Речь только об об *общих* делителях: у числа $n + 6$ самого по себе могут быть и другие делители, которых нет ни у n, ни у 6.) Почему? Если какое-то число d делит и n, и $n + 6$, то оно делит и разность $(n + 6) - n = 6$, так что общие делители первой пары будут общими делителями второй. Напротив, если d делит и n, и 6, то d делит и их сумму $n + 6$, так что общие делители второй пары будут общими делителями первой. Значит, множество общих делителей не изменится, когда мы перейдём от первой пары ко второй.

Теперь про НОД $(n, 6)$: у 6 есть делители 1, 2, 3, 6 если n делится на 6, то 6, если n делится на 3, но не на 6, то НОД $(n, 6) = 3$ (это бывает, когда $n \equiv 3 \pmod 6$), если n делится на 2, но не на 3 и 6, то 2 (это бывает, когда $n \equiv 2 \pmod 6$ или $n \equiv 4 \pmod 6$), в остальных случаях 1.

n mod 6	0	1	2	3	4	5
НОД $(n, n + 6)$	6	1	2	3	2	1

◁

6.6 Докажите, что для любых целых a, b выполнено равенство

$$\text{НОД}(a, b) = \text{НОД}(a - b, b).$$

▷ В решении предыдущей задачи мы видели, что множество общих делителей у пар (a, b) и $(a - b, b)$ одно и тоже. В самом деле, если d делит a и b, то делит и разность $a - b$; если d делит $a - b$ и b, то делит и сумму $(a - b) + b = a$. ◁

6.7 Докажите, что $\text{НОД}(a, b) = \text{НОД}(a - 2b, b) = \text{НОД}(a + b, b) = \text{НОД}(a + b, 2a + 3b)$.

▷ Мы уже знаем из предыдущей задачи, что можно из одного элемента пары вычесть второй, и наибольший общий делитель не изменится. Значит, можно это сделать и дважды: переходя от a, b к $a - b, b$, а потом к $a - 2b, b$, мы не меняем наибольший общий делитель. Если смотреть на вычитание в обратном направлении, то будет прибавление к одному члены пары второго — и оно тоже не меняет наибольший общий делитель: $\text{НОД}(a, b) = \text{НОД}(a + b, b)$. Чтобы перейти от $(a + b, 2a + 3b)$ к (a, b), нужно нескольких шагов:

$$(a + b, 2a + 3b) \to (a + b, a + 2b) \to (a + b, b) \to (a, b)$$

(вычитание первого члена пары из второго, ещё одно, потом вычитание второго из первого) ◁

6.8 Докажите, что для любого целого a и любого положительного целого b выполнено равенство $\text{НОД}(a, b) = \text{НОД}(a \bmod b, b)$.

▷ Мы уже видели, что при вычитании второго члена пары из первого наибольший общий делитель не меняется. Значит, он не изменится, и если мы вычтем несколько раз — столько, сколько нужно, чтобы из a вышло $a \bmod b$. (Если a отрицательно, то надо не вычитать, а прибавлять, но это тоже можно.) ◁

6.9 Найдите $\text{НОД}(123456789, 987654321)$.

▷ Применяя предыдущую задачу, разделим второе число на первое с остатком:

$$987654321 = 8 \cdot 123456789 + 9$$

(как ни странно, остаток очень небольшой), поэтому надо найти наибольший общий делитель пары $(123456789, 9)$, а это будет 9 (по признаку делимости первый член пары делится на 9). ◁

Задача 8 позволяет довольно быстро искать наибольшие общие делители. Скажем,

$$\begin{aligned}\text{НОД}(34,157) = \text{НОД}(34,157 \bmod 34) = \text{НОД}(34,21) = \\ = \text{НОД}(34 \bmod 21, 21) = \text{НОД}(13,21) = \text{НОД}(13, 21 \bmod 13) = \\ = \text{НОД}(13,8) = \text{НОД}(13 \bmod 8, 8) = \text{НОД}(5,8) = \\ = \text{НОД}(5, 8 \bmod 5) = \text{НОД}(5,3) = \text{НОД}(5 \bmod 3, 3) = \\ = \text{НОД}(2,3) = \text{НОД}(2, 3 \bmod 2) = \text{НОД}(2,1) = 1.\end{aligned}$$

Этот способ и называется *алгоритмом Евклида*.

• Мы довели вычисление до НОД$(2,1)$, хотя уже задолго до этого легко было сообразить, что общих делителей нет, — просто чтобы «следовать букве алгоритма». Кстати, можно было бы сделать и ещё один шаг:

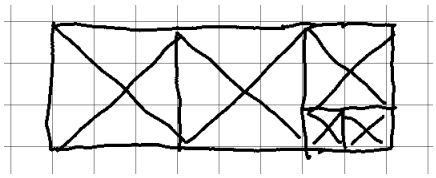
$$\text{НОД}(2,1) = \text{НОД}(2 \bmod 1, 1) = \text{НОД}(0,1) = 1.$$

В нашем примере почти всё время (кроме первого шага) деление с остатком сводится к однократному вычитанию, но так бывает не всегда. Может случиться, что числа (с самого начала или в середине вычислений) сильно различаются (одно много больше другого), и тогда деление с остатком заменяет большое число вычитаний.

▷ Программисты бы описали алгоритм Евклида как-нибудь так:

```
пока в паре большее число не делится на меньшее:
   заменить большее число остатком от деления на меньшее
ответ: меньшее число
```

(Точнее говоря, надо было бы написать «большее или равное» вместо «большее».) ◁



Алгоритм Евклида на квадратах

6.10 Машина действует так: получив прямоугольник размером $a \times b$ при $a < b$, она отрезает от него квадрат $a \times a$ — и остаётся прямоугольник $a \times (b - a)$, который снова засовывают в машину, если он не квадратный.

На какие квадраты будет разрезан прямоугольник 34×157? Как этот процесс связан с алгоритмом Евклида?

• Для произвольного прямоугольника никто не обещает, что процесс рано или поздно закончится (может быть, будут оставаться меньшие и меньшие прямоугольники, но не квадраты).

▷ Для этого конкретного прямоугольника: 4 квадрата 34×34 и останется прямоугольник 34×21, потом квадрат 21×21, останется 13×21, потом 13×13, останется 8×13, потом 8×8, останется 5×8, потом 5×5, останется 3×5, потом 3×3, останется 2×3, потом 2×2, останется 1×2, и наконец мы этот последний прямоугольник разрежем на квадраты 1×1.

сторона квадрата	34	21	13	8	5	3	2	1
сколько квадратов	4	1	1	1	1	1	1	2

Прямоугольник соответствует паре чисел (стороны прямоугольника). При отрезании квадрата из большего числа вычитается меньшее. Если оно после этого остаётся бóльшим, то отрезается ещё один такой же квадрат, и так далее — пока мы не получаем деление с остатком, разбитое в последовательность вычитаний. Так что получается, так сказать, «алгоритм Евклида в замедленной съёмке». ◁

6.11 При разрезании на квадраты описанным способом получились квадраты трёх размеров: 3 больших квадрата, 2 квадрата поменьше и 5 совсем маленьких. Найдите отношение сторон исходного прямоугольника.

▷ Будем смотреть с конца. Примем сторону совсем маленького квадрата за единицу. Раз их пять, то разрезали 1×5, значит, квадрат поменьше был 5×5 и на предыдущем шаге был прямоугольник 11×5 (ведь $1 + 2 \cdot 5 = 11$), и большой квадрат 11×11, их было 3, то есть изначально было 38×11 (ведь $5 + 3 \cdot 11 = 38$). Отношение сторон исходного прямоугольника: $38 : 11$. ◁

6.12 Найдите значение «непрерывной» (или, как ещё говорят, «цепной») дроби

$$3 + \cfrac{1}{2 + \cfrac{1}{5}}$$

(и сравните с предыдущей задачей).

▷ Такую дробь можно вычислять снизу вверх (= изнутри наружу) — а как ещё? получится $2 + 1/5 = 11/5$, потом $3 + 5/11 = 38/11$. Так что происходит всё то же самое, что в предыдущей задаче, но в обратном порядке (выделение целой части и перестановка числителя со знаменателем — это и есть один шаг алгоритма Евклида). ◁

6.13 Найдите целые положительные числа x, y, z, при которых

$$\frac{38}{11} = x + \cfrac{1}{y + \cfrac{1}{z}}$$

(укажите все возможные варианты).

▷ Тут один возможный ответ даёт предыдущая задача. Но единственный ли он? Да, и рассуждать можно так: число $y + \frac{1}{z}$ не меньше 1, поэтому дробь $\cfrac{1}{y + \cfrac{1}{z}}$ находится между 0 и 1, так что x определяется однозначно как целая часть $38/11$. По тем же причинам однозначно определяется y, и тем самым z. ◁

6.14 Докажите, что $\text{НОД}\,(2a, 2b) = 2\,\text{НОД}\,(a, b)$ и вообще

$$\text{НОД}\,(ca, cb) = c \cdot \text{НОД}\,(a, b)$$

при любых целых $a, b, c \neq 0$.

▷ Будем параллельно применять алгоритм Евклида к обеим парам чисел — или, если угодно, к обоим прямоугольникам, их изображающим. Тогда один прямоугольник будет вдвое (или в c раз) больше другого, если единица измерения общая, и процесс разрезания будет происходить синхронно. Значит, и результирующие маленькие квадраты будут отличаться в c раз. (А если выбрать единицы отличающимися в c раз, можно прямоугольники вообще сделать численно одинаковыми.) ◁

• Без алгоритма Евклида тут обойтись не так просто. Понятно, что если d — общий делитель a и b, то $2d$ — общий делитель $2a$ и $2b$, так что $\text{НОД}\,(2a, 2b) \geqslant 2\,\text{НОД}\,(a, b)$. Но как доказать обратное неравенство? Тут достаточно было бы доказать, что если d' — общий делитель $2a$ и $2b$, то либо d' чётный, либо d' — общий делитель a и b (и это верно, но надо использовать, что если нечётное число делит $2a$, то оно делит и a — что тоже обычно доказывается с помощью алгоритма Евклида, как мы вскоре и сделаем).

6.15* Докажите, что разрезание прямоугольника $a \times b$ на квадраты закончится в том и только том случае, если у его сторон есть *общая мера*. Здесь общей мерой называется отрезок, который укладывается и в a, и в b целое число раз.

• Именно в такой ситуации алгоритм Евклида (без такого названия, естественно) описан в «Началах» Евклида — только там не прямоугольник разрезается, а просто два отрезка, и меньший откладывается на большем.

▷ Если у сторон прямоугольника есть общая мера, примем её за единицу измерения. Тогда все квадраты, на которые мы разрезаем, будут с целыми сторонами, и прямоугольники будут уменьшаться (точнее можно сказать так: меньшая сторона прямоугольника будет уменьшаться), так что рано или поздно всё должно кончиться.

Напротив, если всё разрежется на конечное число квадратов, то идя с конца, видим, что сторона самого маленького квадрата целое число раз укладывается во всех сторонах ◁

6.16* Говорят, что стороны прямогольника находятся в отношении «золотого сечения», если после отрезания от него квадрата остаётся прямоугольник с тем же отношением сторон, что у исходного. Закончится ли алгоритм Евклида, если применить его к такому прямоугольнику? А если применить к прямоугольнику с отношением сторон $\sqrt{2} : 1$ (как у диагонали квадрата к его стороне)?

▷ Для золотого сечения — очевидно, нет, потому что новый прямоугольник будет с тем же отношением сторон, что и старый, поэтому и второй будет с тем же отношением сторон, и так далее.

Про прямоугольник с отношением $\sqrt{2}$: мы видели, что $\sqrt{2}$ иррациональный, поэтому общей меры нет, так что процесс будет бесконечным. Можно и более конкретно описать, что будет происходить: отношение после первого шага (отрезали один квадрат) будет $1/(\sqrt{2}-1) = \sqrt{2}+1$ (проверяется умножением), потом после отрезания одного квадрата будет снова $\sqrt{2}$, и так далее. Вообще для любого квадратного корня всё зациклится аналогичным образом (но это надо доказывать, так сразу это не ясно). ◁

6.17* Начав разрезать описанным способом прямоугольник на квадраты, мы получили два квадрата побольше, один поменьше и остался прямоугольник с тем же отношением сторон, что исходный (то есть дальше будет снова два квадрата, потом один ещё меньше, потом два ещё меньше и т.п.). Каково было отношение сторон исходного прямоугольника?

• Иногда эту задачу формулируют так: чему равна бесконечная периодическая цепная дробь

$$2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{2+\ldots}}}}$$

▷ Если отношение большей стороны к меньшей равно x, то

$$x = 2 + \cfrac{1}{1+\cfrac{1}{x}}$$

Свёртывая дробь, получаем $x = 2 + x/(x+1)$, или $x^2 + x = 2x + 2 + x$, то есть $x^2-2x-2 = 0$, или $(x-1)^2-3 = 0$, единственный положительный корень $1+\sqrt{3}$. Проверим на всякий случай: сначала два квадрата и отношение $1 : (\sqrt{3}-1) = \frac{1}{2} + \frac{\sqrt{3}}{2}$, целая часть 1, остаётся $1 : \frac{\sqrt{3}-1}{2} = \sqrt{3}+1$, как и требовалось. ◁

6.18 Докажите, что числа n^2 и $n-1$ взаимно просты при любом целом $n > 1$.

▷ Можно вспомнить, что $n^2-1 = (n-1)(n+1)$, так что при делении n^2 на $n-1$ с остатком получится 1 (и частное $n+1$). Можно просто повторить рассуждения для этого случая, не ссылаясь на алгоритм Евклида: если d — общий делитель n^2, и $n-1$, то он делит и $n(n-1) = n^2 - n$, а значит, и n (как разность с n^2), а значит и 1 (как разность n и $n-1$). ◁

• Второе рассуждение лучше первого, потому что нет вопросов про то, с чего это мы позволяем себе применять алгоритм Евклида к отрицательным числам.

6.19* Докажите, что в последовательности

$$2+1, 2^2+1, 2^4+1, 2^8+1, 2^{16}+1, 2^{32}+1, \ldots$$

любые два числа (не обязательно соседние) взаимно просты. Как из этого вывести, что простых чисел бесконечно много?

▷ Произведение чисел этой последовательности до 2^n+1 равно $2^{2n}-1$ (удобно домножить формально на $(2-1)$ и потом применять формулу $(a-b)(a+b) = a^2 - b^2$ много раз), то есть на 2 меньше следующего члена $2^{2n}+1$. Значит, если

бы этот следующий член имел общий делитель с одним из предыдущих, то и разница 2 должна была бы на него делиться, а делителя 2 нет, потому что все числа нечётны).

Раз числа взаимно просты, то их разложения на простые множители не пересекаются (нет общих простых множителей), так что всего простых чисел должно быть бесконечно много. ◁

• Ещё одно доказательство получается из рассуждения с оценкой гармонического ряда, которое мы обсуждали в связи с плотностью простых чисел. Повторим его применительно к нашему случаю. Пусть есть всего k простых чисел $p_1, \ldots, p_k$. Каждая из k сумм

$$1+\frac{1}{p_1}+\frac{1}{p_1^2}+\frac{1}{p_1^3}+\ldots, \quad 1+\frac{1}{p_2}+\frac{1}{p_2^2}+\frac{1}{p_2^3}+\ldots, \quad \ldots, \quad 1+\frac{1}{p_k}+\frac{1}{p_k^2}+\frac{1}{p_k^3}+\ldots,$$

сколько слагаемых в ней ни бери, будет не больше такой суммы для наименьшего простого числа 2, то есть $1+\frac{1}{2}+\frac{1}{4}+\ldots$, а эта сумма при любом количестве слагаемых остаётся меньше 2 (сделаем шаг, потом полшага, останется полшага, потом четверть шага, останется четверть шага, и так далее). Поэтому произведение k таких сумм (при любом количестве слагаемых) будет не больше 2^k. С другой стороны, при раскрытии скобок и достаточно большом количестве слагаемых мы получим (среди прочего) все слагаемые в сумме

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\ldots\frac{1}{N},$$

даже и для больши́х N (надо просто взять побольше слагаемых). В самом деле, любое m можно разложить как произведение степеней простых, и найдя эти степени в знаменателях, перемножить, получится $1/m$. (Мы не пользуемся однозначностью — если бы даже её и не было, то $1/m$ появилось бы несколько раз.) Поэтому в наших предположениях (все простые среди $p_1, \ldots, p_m$) мы получаем, что

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\ldots\frac{1}{N} \leqslant 2^k$$

при любом k. Но если левую часть разбивать на скобки вида

$$\frac{1}{n+1}+\frac{1}{n+2}+\ldots+\frac{1}{2n},$$

то каждая скобка не меньше $1/2$ (в ней n членов, каждый не меньше $1/2n$), и потому при большом числе скобок получается противоречие.

7. Алгоритм Евклида: следствия

С помощью алгоритма Евклида можно доказать критерий разрешимости линейных уравнений в целых числах. Мы сейчас это объясним, но начнём с примеров.

7.1 В стране в ходу только две монеты: 8 флоринов и 15 флоринов. И у вас, и у кассира есть неограниченный запас монет обоих видов (для оплаты и для сдачи). Как заплатить 30 флоринов? 40 флоринов? 10 флоринов? 1 флорин? 13 флоринов? любое целое число флоринов?

▷ Заплатить 30 и 40 флоринов просто: два раза по 15 и пять раз по 8. Теперь можно заплатить 10, заплатив 40 ($=5\cdot 8$) и получив сдачи 30 ($=2\cdot 15$). Другими словами, $10 = 5\cdot 8 - 2\cdot 15$. Чтобы заплатить 1 флорин, можно заплатить 16 флоринов двумя монетами по 8 и получить сдачи 15. Другими словами, $1 = 2\cdot 8 - 1\cdot 15$. Теперь безо всяких вычислений можно понять, как заплатить любое целое число флоринов: надо просто много раз платить один флорин. Другими словами, можно умножить последнее равенство на любое число: $13 = (13\cdot 2)\cdot 8 - (13\cdot 1)\cdot 15 = 26\cdot 8 - 13\cdot 15$. ◁

7.2* Покажите, что можно заплатить кассиру любое число флоринов и в том случае, когда у вас есть только монеты в 15 флоринов, а у него только в 8 флоринов.

▷ Можно заметить, что $7\cdot 15 - 13\cdot 8 = 105 - 104 = 1$, и дальше можно повторять платежи. Но можно и заранее поменять 15-флориновые монеты на 8-флориновые у того же кассира (по курсу 8 за 15) в любом нужном количестве и свести задачу к предыдущей. ◁

7.3 Пусть теперь в ходу только две монеты: в 25 и 15 флоринов. Как заплатить 80 флоринов? 5 флоринов? 2005 флоринов? 7 флоринов? Какие суммы можно заплатить, а какие нет?

▷ Заплатить 80 можно как $50 + 30 = 2\cdot 25 + 2\cdot 15$. Чтобы заплатить 5, можно заплатить 50 и получить 45 сдачи: $5 = 2\cdot 25 - 3\cdot 15$. Теперь можно заплатить любое кратное 5 (заплатив 5 несколько раз), в том числе и 2005. А заплатить 7 нельзя, потому что все уплачиваемые суммы кратны 5 (поскольку обе монеты кратны 5, любая уплачиваемая сумма будет кратна 5, а 7 не делится на 5). Так что можно заплатить суммы, кратные 5, а не кратные — нельзя. ◁

В общем виде можно сказать так. Пусть даны два числа a и b. Мы рассматриваем числа вида $ma + nb$ при всевозможных целых m и n (суммы, которые можно уплатить, если есть только монеты a и b). Будем коротко называть такие числа «выразимыми» через a и b (полностью было бы «выразимыми в виде целочисленной линейной комбинации чисел a и b»). В предыдущих задачах мы установили, что

- любые целые числа выразимы через 8 и 15;
- целые числа, кратные 5, и только они, выразимы через 25 и 15.

Возникает общий вопрос: какие числа выразимы через данные два числа a и b? Ответ на него такой: *те* (*и только те*)*, которые кратны* НОД (a, b). Мы вскоре увидим, почему это так.

7.4 Фиксируем a и b и будем рассматривать выразимость через них. Покажите, что любое кратное выразимого числа выразимо. Покажите, что сумма и разность двух выразимых чисел выразими.

▷ Математики сформулировали бы утверждение этой задачи, сказав, что *выразимые числа образуют идеал*. (Терминология странная, но так получилось исторически.) ◁

▷ На языке монет: если можно уплатить u, то можно уплатить и любое кратное u (повторяя уплату). Если можно уплатить u и v, то можно уплатить $u + v$, сначала уплатив u, а потом уплатив v. Чтобы уплатить $u - v$, надо уплатить u, а потом получить сдачу v (уплата «в другую сторону»). ◁

7.5 Докажите, что число c выразимо через a и b в том и только том случае, когда c делится на $d =$ НОД (a, b).

• Эта формулировка означает, что надо доказать две вещи: (1) если c выразимо, то оно делится на d; (2) если c делится на d, то оно выразимо через a и b.

▷ Первая часть совсем простая: если обе монеты кратны какому-то d (наибольшему общему делителю, или даже просто общему делителю), то всё, что можно ими уплатить, тоже будет кратно d. Другими словами, поскольку a и b кратны $d =$ НОД (a, b), то и любая уплачиваемая сумма $ma + nb$ будет кратна d (как сумма или разность нескольких кратных d).

Вторая часть главная: почему d и любое кратное d выразимы (можно уплатить монетами a и b)? Достаточно доказать про d (потому что

если можно один раз уплатить d, то можно и повторять). Тут как раз и нужен алгоритм Евклида. В нём мы много раз вычитаем одно число пары из другого (деление с остатком можно считать многократным вычитанием). Начинаем мы с выразимых чисел a и b, и разность выразимых чисел всегда выразима, поэтому всё, что получится в ходе алгоритма, будет выразимо. В том числе и результат (то, что будет на последнем шаге), то есть наибольший общий делитель d. ◁

• Как это выглядит для нашего примера с 15 и 8? Алгоритм Евклида даёт последовательно $(15, 8) \to (7, 8) \to (7, 1)$, дальше 7 делится без остатка, так что мы останавливаемся и получаем НОД $(15, 8) = 1$.

Оба числа 15 и 8 выразимы через 15 и 8 (естественно), поэтому выразима их разность $7 = 15 - 8$. Раз числа 8 и 7 выразимы, то выразима их разность $1 = 8 - 7 = 8 - (15 - 8) = 2 \cdot 8 - 15$.

Утверждение предыдущей задачи формулируют ещё и так. Пусть a и b — произвольные целые числа (не равные оба нулю), и c — произвольное целое число.

Уравнение

$$ax + by = c$$

разрешимо в целых числах x, y тогда и только тогда, когда число c делится на НОД (a, b).

7.6 Имеет ли уравнение $23x + 89y = 5$ решения в целых числах? Найдите одно из них.

▷ Применяем алгоритм Евклида:

$(89, 23)$	$89 \bmod 23 = 20$	$20 = 89 - 3 \cdot 23$	$(23, 20)$
$(23, 20)$	$23 \bmod 20 = 3$	$3 = 23 - 1 \cdot 20$	$(20, 3)$
$(20, 3)$	$20 \bmod 3 = 2$	$2 = 20 - 6 \cdot 3$	$(3, 2)$
$(3, 2)$	$30 \bmod 2 = 1$	$1 = 3 - 1 \cdot 2$	$(2, 1)$

Теперь последовательно выражаем числа $20, 3, 2, 1$ в виде целочисленных линейных комбинаций 89 и 23 (и напоследок умножаем на 5):

$20 = 1 \cdot 89 - 3 \cdot 23$

$3 = 1 \cdot 23 - 1 \cdot 20 = 1 \cdot 23 - 1 \cdot (89 - 3 \cdot 23) = 4 \cdot 23 - 1 \cdot 89$

$2 = 1 \cdot 20 - 6 \cdot 3 = 1 \cdot (1 \cdot 89 - 3 \cdot 23) - 6 \cdot (4 \cdot 23 - 1 \cdot 89) = 7 \cdot 89 - 27 \cdot 23$

$1 = 1 \cdot 3 - 1 \cdot 2 = 1 \cdot (4 \cdot 23 - 1 \cdot 89) - 1 \cdot (7 \cdot 89 - 27 \cdot 23) = 31 \cdot 23 - 8 \cdot 89$

$5 = (5 \cdot 31) \cdot 23 - (5 \cdot 8) \cdot 89 = 155 \cdot 23 - 40 \cdot 89.$

Конечно, это не единственное решение — например, можно было бы сложить выражения для 3 и 2 и получить $4 \cdot 23 - 1 \cdot 89 + 7 \cdot 89 - 27 \cdot 23 = 6 \cdot 89 - 23 \cdot 23$. Но мы следовали общей схеме: сначала выразить наибольший общий делитель, а потом любое его кратное. ◁

• В этой задаче требуется найти одно решение — но можно и найти общую формулу для всех решений. Мы вскоре вернёмся к этому вопросу.

7.7 Докажите, что для любых двух целых чисел a, b (не равных одновременно нулю) их наибольший общий делитель не просто *больше* любого другого делителя, но и *делится* на него.

▷ Пусть d — этот наибольший общий делитель, а d' — какой-то другой делитель. Мы доказали (как следствие алгоритма Евклида), что можно найти x, y, для которых $ax + by = d$. Раз x и y делятся на d', то и ax, by, и, наконец, $ax + by$ (то есть d) делятся на d'. ◁

• Посмотрим снова на уравнение $ax + by = c$. Там две переменные x и y, значения которых мы ищем, и они входят симметрично. Но можно посмотреть на дело иначе: мы сначала подбираем x, а потом y. На первом шаге нужны такие x, при которых y найдётся, то есть для которых $c - ax$ делится на b (потому что $y = (c - ax)/b$ должно быть целым). Таким образом, мы ищем x, при котором $ax \equiv c \pmod{b}$. И это возможно (как мы теперь знаем), когда c делится на НОД(a, b).

Важный частный случай, когда a и b взаимно просты, разбирается в следующей задаче.

7.8 Пусть числа a и b взаимно просты. Тогда число a *обратимо по модулю* b, то есть найдётся такое x, что $ax \equiv 1 \pmod{b}$. (Это число x — мы скоро увидим, что оно единственно по модулю b — называют *обратным к* a *по модулю* b.)

▷ Поскольку a и b взаимно просты (их наибольший общий делитель равен 1), найдутся целые x и y, для которых $ax + by = 1$, и $ax - 1 = by$ делится на b, то есть $ax \equiv 1 \pmod{b}$, что и требовалось доказать. ◁

7.9 Пусть $b = 10$. Найдите все взаимно простые с b среди остатков по модулю 10, и укажите для них обратные.

▷ Ответ можно посмотреть в таблице умножения по модулю 10, которая у нас была: взаимно просты 1[1], 3[7], 7[3], 9[9] (в квадратных скобках указаны обратные). ◁

7.10 Пусть a и b взаимно просты. Докажите, что для любого c существует x, при котором $ax \equiv c \pmod b$, и что такое x единственно (по модулю b).

• Эта задача говорит о решении линейных уравнений по модулю b, если коэффициент при неизвестной взаимно прост с b.

▷ Условие $ax \equiv c \pmod b$, означает, что $ax - c$ делится на b, то есть найдётся такое y, что $ax - c = by$, то есть $ax + by = c$. А это мы уже знаем.

Можно было объяснить и иначе: мы знаем, что есть обратный элемент z, при котором $az \equiv 1 \pmod b$. Теперь это сравнение можно умножить на c, и получится $azc \equiv c \pmod b$, то есть можно положить $x = zc$.

Теперь единственность: пусть $ax \equiv ax' \pmod b$. Мы знаем, что a имеет обратный элемент z по модулю b, и можно умножить на него. Получится $zax \equiv zax' \pmod b$, то есть $x \equiv x' \pmod b$ (ведь $za \equiv 1 \pmod b$). ◁

Простое число взаимно просто со всеми числами, не делящимися на него. Для этого случая получаем такие утверждения:

7.11 Пусть p — простое число. Докажите, что любой ненулевой остаток a по модулю p обратим: существует такое x, что $ax \equiv 1 \pmod p$. Докажите, что уравнение (сравнение) $ax \equiv c \pmod p$ при $a \not\equiv 0 \pmod p$ имеет решение при любом c, и это решение единственно по модулю p.

• В частности, и обратный элемент единствен (как решение сравнения $ax \equiv 1 \pmod p$).

▷ Это мы уже делали для произвольного модуля, взаимно простого с a (в частности, годится любое простое p, которое не делит a). ◁

7.12 Покажите, что если p — простое число, и $ab \equiv 0 \pmod p$ для каких-то целых чисел a и b, то или $a \equiv 0 \pmod p$, или $b \equiv 0 \pmod p$ (или оба).

• Это утверждение можно переформулировать так: *если произведение двух целых чисел (ab) делится на p, то хотя бы одно из этих чисел (a или b) делится на p*. Или так: *если два целых числа не делятся на простое p, то их произведение не делится на p*. Или даже так: *если произведение ab делится на p, и при этом a не делится на p, то b делится на p*. Все эти формулировки запрещают одно и то же: сомножители не делятся, а произведение делится.

▷ Пусть ab делится на p, то есть сравнимо с 0 по модулю p, а первый сомножитель a не делится на p. Тогда a, как мы видели в предыдущей

задаче, имеет обратный элемент по модулю p: есть такое x, что $ax \equiv 1 \pmod{p}$. Теперь перемножим три числа a, x, b и рассмотрим их произведение по модулю p. Если перемножать сначала ax, а потом умножить на b, то получится b. Но если перемножить сначала ab, а потом полученный 0 (по модулю p) умножить на x, то получится 0. Значит, $b \equiv 0 \pmod{p}$. ◁

• Рассуждения по модулю с непривычки могут казаться странными, поэтому можно изложить решение без сравнений по модулю. Покажем, что если p просто, a не делится на p, и ab делится на p, то b делится на p. Раз p просто и a не делится на p, то a взаимно просто с p. Поэтому (следствие из алгоритма Евклида) можно найти такие x и y, что $ax + py = 1$. Умножим это равенство на b, получим $abx + pby = b$. В левой части оба слагаемых делятся на p (в первом ab делится на p, во втором p есть в явном виде), поэтому их сумма b делится на p.

7.13 Куда надо смотреть в таблицах умножения по модулю p и что проверять, чтобы убедиться, что действительно — в соответствии с доказанным нами — каждый ненулевой элемент имеет единственный обратный? А как проверить, что при $a \not\equiv 0 \pmod{p}$ уравнение $ax \equiv b \pmod{p}$ имеет единственное (по модулю p) решение*

▷ Надо убедится, что во всех строках (и столбцах, но это одно и то же), кроме первой (где умножают на 0) остаток 1 встречается ровно один раз.

Во втором случае надо проверить, что в каждой из строк, кроме нулевой первой, *все* остатки по модулю p встречаются ровно один раз. (Другими словами, все строки получаются из $0, 1, 2, \ldots, p-1$ некоторой перестановкой.) ◁

7.14 Найдите обратное к числу 23 по модулю 89.

▷ Мы уже искали решения уравнения $23x + 89y = 1$, и нашли $x = 31$ и $y = 8$. Так что по модулю 89 обратным к 23 будет 31 (и обратное, как мы уже видели, единственно). ◁

7.15 Решите уравнение $23x \equiv 5 \pmod{89}$ (найдите все его целые решения и объясните, почему других нет).

▷ И это мы уже делали в форме решения $23x + 89y = 5$, и тогда нашли $x = 155$. Поскольку мы решаем уравнение по модулю 89, то годится любое число, которое сравнимо с 155 по этому модулю, например $66 = 155 - 89$. Общий вид таких чисел $155 + 89k$ (или $66 + 89l$, если начать с 66). Есть ли другие? мы уже знаем, что уравнение $ax \equiv c \pmod{p}$

имеет единственное решение по модулю p, если модуль p простой (а 89 — простое число). Так что других решений (кроме чисел вида $155 + 89k$) нет. ◁

Мы уже говорили, что уравнение $ax + by = c$ (при целых коэффициентах a, b, c) имеет решение в целых числах x, y тогда и только тогда, когда c делится на $d = \text{НОД}(a, b)$. Как найти все его решения? Разделим уравнение на d. Тогда получится уравнение $a'x + b'y = c'$, где $a' = a/d$, $b' = b/d$ и $c' = c/d$. Коэффициенты a' и b' в левой части — целые взаимно простые числа (почему?). Если число c' справа нецелое, то решений нет. Если целое, то есть, и одно решение x_0, y_0 можно найти с помощью алгоритма Евклида. Мы уже видели, что значение x' единственно по модулю b', так что все решения можно найти как $x_k = x_0 + kb'$, и соответственно $y_k = y_0 - ka'$.

Напишем какое-то целое число и будем прибавлять к нему какое-то другое целое число много раз (скажем, 3, 8, 13, 18, ...). Получится *арифметическая прогрессия*, а то число, которое прибавляют, называют её *разностью* (потому что такова разность двух соседних членов).

• На числовой оси арифметическую прогрессию можно представлять себе так: мы начинаем с некоторого числа и откладываем много раз какое-то другое число (разность).

7.16 Даны две арифметические прогрессии из целых чисел. Первые члены их могут быть любыми, а разности — положительные взаимно простые целые числа. Покажите, что найдётся целое число, которое входит в обе прогрессии.

▷ Арифметическая прогрессия, которая начинается с a_1, а потом увеличение на b_1, содержит члены вида $a_1 + b_1x$. Вторая прогрессия содержит члены $a_2 + b_2y$. Мы ищем *неотрицательные* x и y, для которых $a_1 + b_1x = a_2 + b_2y$, или $b_1x - b_2y = a_2 - a_1$. Мы уже знаем, что в силу взаимной простоты b_1 и b_2 такие числа x и y найдутся, но как их сделать неотрицательными? Если добавить к x число b_1, а к y число b_2, то решение останется решением (изменения сократятся). Будем так делать, пока x и y не станут неотрицательными. ◁

7.17 Путник начинает движение у столба 0 на кольцевом шоссе длиной в a километров и каждый день проходит b километров. У всех ли километровых столбов ему придётся заночевать — и если не у всех, то у каких именно?

▷ Вопрос можно переформулировать так: какие остатки при делении на b могут давать числа, кратные a? Другими словами, при каких r от 0 до $b-1$ уравнение $ax \equiv r \pmod b$ имеет решение? Это бывает, когда найдутся x и y, при которых $ax+by=r$, а на этот вопрос мы ответ знаем: когда r кратно НОД(a,b).

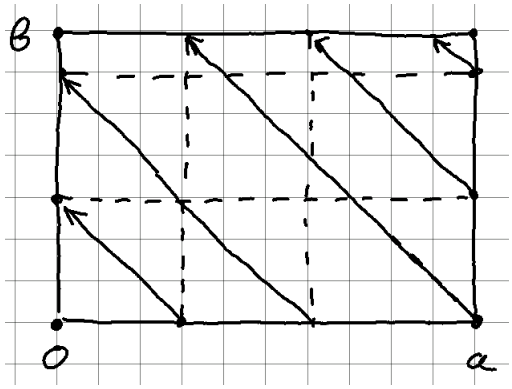
Так что при взаимно простых a и b все столбы будут использованы для ночёвки, а если НОД$(a,b)=rf>1$, то будет каждый r-й столб (все столбы с номерами, кратными r). ◁

7.18 Есть две бочки с большим запасом воды и два ведра, в a литров и b литров, причём a и b — взаимно простые целые числа. Как перелить из одной бочки в другую один литр?

▷ Одно ведро позволяет перелить ax литров, если переливать x раз (отрицательные x соответствуют переливанию в другом направлении). Второе даёт by литров, всего $ax+by$ литров, так что нам надо решить уравнение $ax+by=1$. А это, как мы знаем, возможно, поскольку НОД$(x,y)=1$. ◁

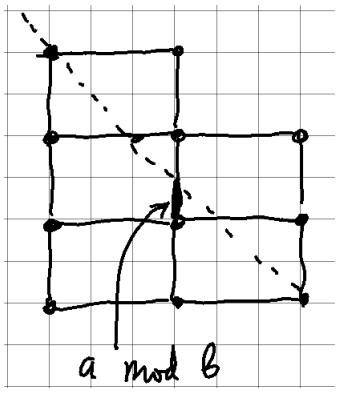
7.19* Пусть теперь имеется одна бочка (из которой можно черпать и куда можно сливать воду) и два ведра в a и b литров, причём a и b — взаимно простые целые числа, и $a>b$. Покажите, что можно отмерить (получить в ведре b) любое целое число литров от 0 до b. (Использовать какие-то другие ёмкости, кроме этих двух вёдер и бочки, нельзя.)

▷ Тут полезно нарисовать, как говорят, *фазовое пространство* нашей системы. В каждый момент ситуация описывается двумя числами: сколько воды в одном ведре (обозначим это количество x) и в другом (y). При этом $0 \leqslant x \leqslant a$ и $0 \leqslant y \leqslant b$. Как в этих терминах описываются наши возможные действия? Если ведро пустое, то его можно наполнить, а если полное — вылить. Это значит, что мы можем с края прямоугольника перейти на другой край (перпендикулярно краю и параллельно другой стороне). Кроме того, мы можем переливать из одного ведра в другое (это соответствует движению под углом 45° к осям).



Начав с $(0, 0)$, мы перепрыгиваем в $(a, 0)$ (наливаем воду в большое ведро), затем двигаемся вверх–налево до $(a - b, b)$, потом перепрыгиваем вниз (выливаем воду из малого ведра), потом снова вверх–налево (в нашем случае вода в большом ведре кончается, а в малом $a - b$), наливаем воду в большое ведро и так далее. Нам надо показать, что продолжая двигаться по этой линии (с пунктирными перепрыгиваниями), мы побываем во всех целых точках на вертикальной оси (от 0 до b).

Чтобы это понять, удобно заменить прыжки переходом в другую копию прямоугольника (топологи сказали бы, что отождествление точек левого и правого края превращает прямоугольник в цилиндр, а после этого отождествление верхнего и нижнего — в тор, а затем мы накрываем этот тор плоскостью).



На рисунке это показано для прямоугольника поменьше и его разложенных по всей плоскости копий. Теперь можно сказать так: когда линия пересекает прямоугольник справа налево, мы смещаемся влево на a и вверх на a, то есть попадаем в точки $a \bmod b$, $2a \bmod b$ и так далее (сдвиг на кратное b соответствует переходу в другую копию, так что можно вычитать). А мы уже знаем, что среди

$ax \mod b$ при НОД $(a, b) = 1$ есть все остатки (потому что a обратимо в остатках по модулю b). ◁

• Если это рассуждение кажется непонятным, полезно проследить, что будет в примере с нашего первого рисунка ($a = 10$, $b = 7$), что в каком порядке будет переливаться, наливаться, выливаться и что будет оставаться в малом ведре, когда большое пустое.

7.20* Будем откладывать на окружности, начав с некоторой точки, одну и ту же (по величине) дугу много раз, и отмечать полученные точки. (Начав с какой-то точки круга, мы делаем равные шаги и никогда не останавливаемся.) Покажите, что возможно одно из двух: либо мы через несколько шагов вернёмся в исходную точку, либо наши отметки будут, как говорят, *плотны на окружности* — это значит, что на любой дуге (ненулевой длины) будут наши отметки.

▷ Будем откладывать и откладывать точки. Если в какой-то момент мы придём в уже посещённую точку, то между ними будет целое число оборотов, так что дальше всё будет повторяться (первый случай). Если же нет, то точек будет становиться всё больше и больше, а расстояние между ближайшими точками всё меньше и меньше: если точек n, то одна из дуг между ними будет меньше $1/n$. Посмотрим на переход по этой дуге: ещё через столько же шагов мы снова сдвинемся на то же расстояние, меньшее $1/n$. Значит, мы будем двигаться шагами, равными этой малой дуге, и таким образом рано или поздно попадём в любую дугу длины больше $1/n$. Поскольку n произвольно, то в любую дугу мы рано или поздно попадём. ◁

• На самом деле можно показать, что не только наши отметки будут плотны на окружности, но ещё они равномерно распределены: это означает, грубо говоря, что средняя доля отметок, попадающих в некоторую дугу, пропорциональна длине этой дуги. Но это уже доказать сложнее (наиболее естественное доказательство использует разложение непрерывных функций в ряд Фурье, точнее, их приближение тригонометрическими многочленами).

7.21* Возьмём произвольное положительное число α (не обязательно целое) и будем смотреть на числа $\alpha, 2\alpha, 3\alpha, \ldots$. Покажите, что возможно только два варианта: либо какое-то из них будет целым (и тогда α — отношение двух целых чисел, то есть рациональное число), либо среди них будет число, которое в десятичной записи будет иметь после запятой сто нулей.

• В этой задаче сто нулей можно заменить на любую группу цифр.

▷ Эта задача сводится к предыдущей: мы двигаемся по окружности длины 1 шагами в α. Либо мы вернёмся в исходную точку (и тогда α рационально), либо нет. Во втором случае мы попадём в любую дугу, то есть, в частности, в отрезок от 0 до 0,000 … 01 (сто нулей), что и означает, что у некоторого целого кратного α будет 100 нулей после запятой.

По тем же причинам (отрезок такой же длины, но с другого места) можно получить любую группу цифр после запятой. ◁

• В этой главе мы извлекали следствия из такого факта (который, в свою очередь, получается как результат алгоритма Евклида): уравнение $ax + by =$ НОД(a, b) имеет решение в целых числах x и y. Его можно доказать и неконструктивно. Вот как это делается. Рассмотрим числа, выразимые через a и b. Возьмём среди них наименьшее положительное число d. Покажем, что это будет общий делитель a и b, который делится на любой другой общий делитель. Второе понятно: если d' делит a и b, то оно делит и любое выразимое число, в частности, наименьшее выразимое d. Теперь первое: почему a, скажем, делится на d? Разделим a на d с остатком: $a = qd + r$, где $0 \leqslant r < d$. Здесь числа a и qd выразимы, поэтому $r = a - qd$ выразимо, что невозможно при $r \neq 0$, так как d было *наименьшим* выразимым положительным числом (а остаток при делении на d всегда меньше d). Значит, d будет наибольшим общим делителем, то есть НОД$(a, b) = d$ выразим.

7.22* Пусть a, b — положительные целые числа. Рассмотрим их *общие кратные*, то есть числа, делящиеся и на a, и на b. (Таково, например, ab.) Пусть m — их *наименьшее* общее кратное. Покажите, что оно будет делителем любого общего кратного a и b.

• Это легко будет следовать из теоремы о единственности разложения на множители, как мы увидим, но и без неё это доказывается довольно просто.

▷ Пусть m' — какое-то другое общее кратное (будем считать, что положительное, иначе изменим знак). Поскольку m было наименьшим, то $m < m'$. Поделим m' с остатком на m: пусть $m' = qm + r$, где $0 \leqslant r < m$. Тогда $r = m' - qm$ будет общим кратным a и b (как разность двух общих кратных), но $r < m$, а m было наименьшим. Значит, $r = 0$, что и требовалось доказать. ◁

7.23 Докажите, что если a делится на b и на c, причём b и c взаимно просты, то a делится на bc.

▷ Мы увидим скоро, что это сразу видно, если воспользоваться единственностью разложения на простые множители. Но можно доказать и так: раз b и c взаимно просты, можно найти такие x и y, что $bx + cy = 1$. Тогда $a = a(bx + cy) = abx + acy$. Оба сладаемых делятся на bc. Скажем,

abx делится на bc, потому что ax делится на c (а это потому, что a делится на c). Аналогично и для acy. Значит, и сумма, равная a, делится на bc. ◁

7.24 Мы хотим найти целое число, которое даёт остаток 3 при делении на 4 и остаток 6 при делении на 9. Какое уравнение в целых числах надо для этого решать и есть ли у него решения?

▷ Числа, которые дают остаток 3 при делении на 4, имеют вид $4k+3$, а числа, которые дают остаток 6 при делении на 9, имеют вид $9l+6$. Поэтому, чтобы найти общее число, мы должны решить уравнение $4k+3 = 9l+6$, или $4k-9l = 3$. Мы уже знаем, что оно имеет решение, поскольку 4 и 9 взаимно просты. Впрочем, тут оно сразу видно: $k = 3$, $l = 1$, $4k+3 = 9l+6 = 15$, так что искомое число 15. ◁

7.25 Пусть a и b — взаимно простые целые числа, а m и n — произвольные (тоже целые) числа. Докажите, что можно найти число u, для которого

$$u \equiv m \pmod{a} \quad \text{и} \quad u \equiv n \pmod{b}.$$

▷ Как и в прошлой задаче, здесь надо решать уравнение $m+ak = n+bl$ (считая переменными k и l: при данных a, b, m, n мы ищем подходящие k и l). Это уравнение можно переписать как $ak - bl = n - m$, и оно имеет решение, так как a и b взаимно просты. (Точнее, a и $-b$ взаимно просты.) ◁

На это утверждение можно посмотреть иначе. Пусть b и c взаимно просты. Если мы знаем остаток от деления какого-то числа x на bc, то можно восстановить (даже не зная x) остатки от деления на b и c, надо просто поделить остаток $x \bmod bc$ на b и на c.

Предыдущая задача показывает, что *при этом может получиться любая пара остатков* (всего таких пар bc, как и остатков по модулю bc). При этом разные остатки (не сравнимые по модулю bc) дадут разные пары: если x и x' сравнимы по модулям b и c одновременно, то $x - x'$ делится на b и на c. А раз b и c взаимно просты, то $x - x'$ делится и на bc (задача 23).

Математики говорят, что *возникает взаимно-однозначное соответствие*

$$x \bmod bc \leftrightarrow (x \bmod b, x \bmod c)$$

между остатками по модулю bc и парами остатков по взаимно простым модулям b и c, и называют это утверждение *китайской теоремой об остатках*).

▷ История этого названия, как всегда довольно запутанная. Если верить википедии, то ещё в третьем веке новой эры китайский математик Сунь цзы разобрал в своём сочинении один из примеров такого рода (см. следующую задачу 26), и потом это много раз переоткрывалось, обобщалось, доказывалось и т.п. ◁

7.26* Есть неизвестное число предметов. Если считать их тройками, останутся два, если пятёрками, останутся три, и если семёрками, то останутся два. Сколько всего предметов?

• В этой задаче модуля не два, а три (3, 5, 7), но они попарно взаимно просты, и утверждение обобщается и на этот случай.

▷ Тут надо найти x, для которого $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$. Раз уж совпали остатки по модулям 3 и 7, удобно начать с них: $x - 2$ делится на 21, то есть $x = 21k + 2$. Теперь по модулю 5 получаем $21k + 2 \equiv 3 \pmod 5$, или $k + 2 \equiv 3 \pmod 5$, так что $k \equiv 1 \pmod 5$. Минимальный ответ $k = 1$, то есть число 23, дальше $128 = 6 \cdot 21 + 2$, и так далее. ◁

7.27* Докажите такое обобщение китайской теоремы об остатках (на несколько модулей): если $b_1, \ldots, b_n$ — попарно взаимно простые целые числа, а $c_1, \ldots, c_n$ — произвольные остатки по модулям $b_1, \ldots, b_n$ соответственно, то система сравнений

$$x \equiv c_1 \pmod{b_1}, \quad x \equiv c_2 \pmod{b_2}, \ \ldots, \quad x \equiv c_n \pmod{b_n}$$

имеет решение x, и притом это x ровно одно по модулю $b_1 \cdot \ldots \cdot b_n$.

▷ Уже доказанное (про два остатка) позволяет заменить «$x \equiv c_1 \pmod{b_1}$ и $x \equiv c_2 \pmod{b_2}$» на $x \equiv c_{12} \pmod{b_1 b_2}$, и уменьшить число сравнений. Надо только отметить, что $b_1 b_2$ взаимно просто с любым b_k из остальных, потому что это произведение двух взаимно простых с ним чисел. После этого повторяем рассуждение, пока не останется одно сравнение. ◁

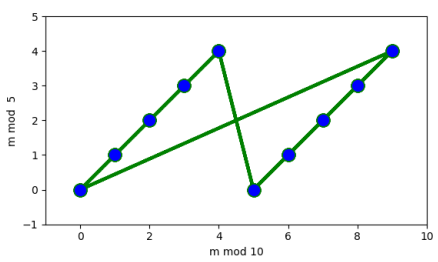
7.28* Иногда шахматную доску «сворачивают в тор»: если фигура выходит за границу, то её возвращают с другой стороны (сдвигая по горизонтали на ширину доски и/или по вертикали на высоту доски).

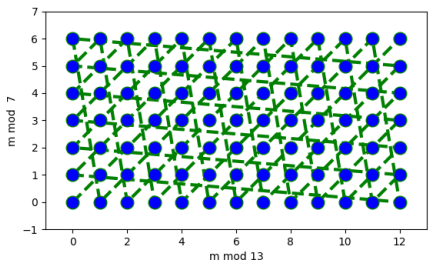
Докажите, что на свёрнутой в тор доске $a \times b$ со взаимно простыми a и b шахматный король, который начинает с какой-то клетки и всё время идёт вправо-вверх по диагонали, побывает во всех клетках по разу и вернётся в исходную клетку.

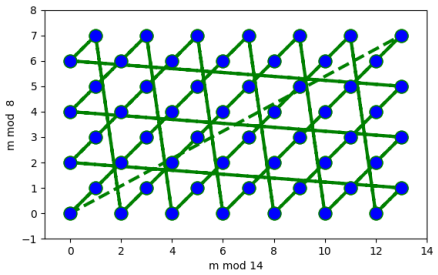
• На одном из следующих рисунков как раз и показан путь короля. (На каком?)

▷ Шахматный король ведёт себя в точности как остатки $(x \bmod a, x \bmod b)$ при увеличении x на 1, так что достаточно сослаться на китайскую теорему об остатках. ◁

Китайскую теорему об остатках (и условие взаимной простоты) можно проиллюстрировать картинками, на которых изображены возможные пары остатков $(x \bmod a, x \bmod b)$ для трёх пар модулей: $(10, 5)$, $(13, 7)$ и $(14, 8)$. Линии соединяют пары остатков для соседних значений x.







В первом случае остаток при делении на 5 однозначно определяется остатком при делении на 10 (является *функцией* от него). Во втором случае — как и положено для взаимно простых модулей — возможны все пары остатков. Третий случай промежуточный: в нём модули не кратны друг другу, но и не взаимно просты, поэтому возможны многие пары остатков, но не все.

7.29* Какая доля всех пар остатков реализуется на последней картинке? Общий вопрос: если мы рассмотрим все пары остатков по модулям a, b, то какая их доля реализуется как $(x \bmod a, x \bmod b)$?

▷ На картинке они идут в шахматном порядке, так что реализуется половина. В общем случае ответ будет $1/\text{НОД}(a,b)$. В самом деле, появление пары (u,v) означает, что уравнение $u+ax = v+by$ имеет решение. Его можно переписать как $ax - by = v - u$, так что $v-u$ должно делиться на $\text{НОД}(a,b)$, и в каждой вертикали (или горизонтали) будет как раз доля $1/\text{НОД}(a,b)$. ◁

7.30* Покажите, что уравнение $ax+by+cz = 1$ с целыми коэффициентами a, b, c имеет решение (с целыми значениями переменных x, y, z) тогда и только тогда, когда у a, b, c нет общего делителя, кроме 1.

• В терминах платежей: монетами в a, b и c флоринов можно уплатить 1 флорин (и потому любое целое число) в том и только том случае, когда нет (целого положительного) числа, которому кратны все три монеты.

▷ Если общий делитель $d > 1$ есть, то левая часть в $ax + by + cz$ кратна d, а правая нет. Обратное чуть сложнее. Прежде всего заметим, что в виде $ax + by$ можно представить все числа, кратные $\text{НОД}(a,b)$, поэтому достаточно решить уравнение $\text{НОД}(a,b)t + cz = 1$ относительно t и z. Если его нельзя решить, то у $\text{НОД}(a,b)$ и c есть общий делитель, который будет делителем всех трёх чисел a, b, c. ◁

7.31* Игрок тасует колоду из 52 карт (рубашкой вверх) так: он берёт стопку из 10 верхних карт и меняет её местами с оставшимися картами (так что теперь сверху 42 другие карты, внизу снятые 10, по-прежнему все карты рубашкой вверх). Затем он делает то же самое ещё раз, потом ещё раз и так до бесконечности. Сколько карт побывают в низу колоды (будут в какой-то момент на последнем месте в колоде)?

▷ Описанное преобразование — сдвиг на 10 в цикле из 52 карт, поэтому получатся все сдвиги, кратные $\text{НОД}(10, 52) = 2$. Значит, в низу колоды побывает ровно половина всех карт. ◁

8. Однозначность разложения и её следствия

Сейчас уже всё готово для доказательства теоремы об единственности разложения на простые множители. Основная лемма тут (уже доказанная): *произведение двух чисел, не делящихся на простое p, тоже не делится на p*. То же самое верно и для большего числа сомножителей.

8.1 Докажите, что это верно для любого числа сомножителей: если число p простое ни один из сомножителей в произведении не делится на p, то и всё произведение не делится на p.

• Другими словами, если произведение делится на p, то хотя бы один сомножитель делится на p. Или так: не может быть, чтобы все сомножители не делились, а произведение делилось. (Речь везде идёт, конечно, о произведении целых чисел.)

▷ Будем постепенно добавлять сомножители в произведение, сохраняя не-делимость на p. Вообще если известно, что произведение двух «хороших» чисел «хорошее» — что бы ни называлось «хорошим» — то и произведение любого количества хороших чисел будет хорошим (домножение произведения на хорошее число сохраняет хорошесть). ◁

Мы уже говорили про однозначность разложения на простые множители: если какое-то положительное целое число двумя способами представлено в виде произведения простых множителей, то есть

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_l,$$

то эти разложения отличаются лишь перестановкой множителей (в них входят одни и те же множители в разном порядке; в частности, $k = l$.

8.2 Докажите это утверждение, пользуясь предыдущей задачей.

▷ Пусть есть два разложения целого положительного числа на простые множители. Если входящие в них простые числа пересекаются (есть простое число, входящее в оба), то сократим на все такие множители. Если после сокращения вообще ничего не останется (с обеих сторон будет 1), то, значит, разложения были одинаковые, только порядок разный (потому что состояли из тех самых множителей, на которые мы сократили). Может ли быть иначе? В этом случае получится два разложения одного числа, в которых нет общих множителей:

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_l,$$

(мы написали снова a, но это может быть уже меньшее число после сокращения). Теперь это очевидно противоречит доказанному: левая часть делится на p_1, а правая часть (ей равная) состоит из простых чисел, не равных p_1 и потому не делящихся на p_1 — и, значит, их произведение не делится на p_1 (как говорит предыдущая задача). ◁

8.3 Пусть p, q — два различных простых числа. Покажите, что в последовательностях $1, p, p^2, p^3, \ldots$ и $1, q, q^2, q^3, \ldots$ нет общих чисел, кроме 1.

▷ Общее число имело бы два разных разложения. ◁

8.4* Пусть a и b — два целых положительных (не обязательно простых) числа. Покажите, что если $a^n = b^m$ при некоторых целых $m, n > 0$, то оба числа a и b являются степенями некоторого одного числа x.

▷ Можно считать (как говорят, *не ограничивая общности* — это значит, что всегда можно свести дело к этому случаю), что m и n взаимно просты. (Иначе можно взять наибольший общий делитель и извлечь корень). Посмотрим теперь на разложение числа $u = a^n = b^m$. Поскольку разложение u единственно, то одно и то же разложение получится, если начать с a и если начать с b. Какова кратность какого-то простого числа p в этом разложении? она должна делиться на m, и одновременно на n, то есть должна делиться на mn (взаимная простота), поэтому из u можно извлечь нацело корень степени mn, и этот корень $x = \sqrt[mn]{u}$ будет давать $x^m = a$ и $x^n = b$. ◁

Если какой-то множитель повторяется в разложении несколько раз, его можно написать в соответствующей степени, если он совсем не входит, его можно написать в нулевой степени ($p^0 = 1$). Поэтому теорему о разложении на множители можно пересказать так: всякое число n однозначно представляется в виде

$$N = 2^{n_2} \cdot 3^{n_3} \cdot 5^{n_5} \cdot \ldots$$

где $k_2, k_3, k_5, \ldots$ — неотрицательные целые числа, среди которых лишь конечное число ненулевых (так что реально в произведении конечное число множителей). Для случая $N = 1$ можно считать, что все n_i равны нулю (все сомножители единицы).

Глядя на степени простых чисел в разложении (другими словами, их *кратности* — сколько раз они входят в разложение), можно многое сказать о делимости, наибольшем общем делителе и так далее. В следующих задачи сформулированы такие утверждения.

8.5 Два положительных целых числа a и b разложены в произведение простых. Как, глядя на эти разложения, определить, делится ли a на b?

▷ Чтобы убедиться, что a делится на b, надо проверить, что все числа, входящие в разложение b, входят и в a, причём не меньшее число раз (с не меньшей кратностью). Это почти очевидно, но скажем подробно. Надо проверить две вещи.

Пусть a делится на b. Покажем, что кратности простых чисел в a не меньше, чем в b. Раз a делится на b, то $a = bc$ для некоторого целого c (тоже положительного). Разложим b и c на простые множители. Соединяя эти разложения, получим разложение для a, в котором кратности не меньше, чем в разложении для b. Но поскольку разложение единственно, это и будет данное нам разложение на a.

Наоборот, пусть в a кратности не меньше, чем в b. Тогда излишек (множители из a, которые не попали в b) образует c, и $a = bc$. ◁

8.6 Сколько делителей у числа $2^5 \cdot 3$?

▷ Из предыдущей задачи видно, что они все имеют вид $2^a 3^b$, где $0 \leqslant a \leqslant 5, 0 \leqslant b \leqslant 1$. Таким образом, для 2^a есть шесть вариантов $2^0, 2^1, \ldots, 2^5$, и каждый из них можно умножать на 3, а можно и не умножать, всего 12 вариантов. ◁

8.7* Сколько делителей у целого числа $2^n 3^m 5^k$?

▷ Делители имеют вид $2^{n_1} 3^{m_1} 5^{k_1}$, где $0 \leqslant n_1 \leqslant n$, $0 \leqslant m_1 \leqslant m$ и $0 \leqslant k_1 \leqslant k$. Для n_1 есть $n+1$ вариантов, затем $m+1$ и $k+1$, всего комбинаций $(n+1)(m+1)(k+1)$. ◁

8.8* Найдите наименьшее число, имеющее ровно 18 делителей.

▷ Вспоминая разложение $18 = 3 \cdot 3 \cdot 2$, видим, что годится любое число $p^2 q^2 r$, где p, q, r — простые числа. Наименьшее будет при $p = 2$, $q = 3$, $r = 5$, то есть 180. Ещё есть разложение 18 (то есть числа вида p^{19}, а также $2 \cdot 9$, то есть числа pq^8, или $3 \cdot 6$, то есть числа $p^2 q^5$. Но в каждом из трёх вариантов наименьшее число будет больше. (Для последнего: $3^2 \cdot 2^5 = 9 \cdot 32 = 288$, для остальных ещё больше.) ◁

8.9 Как определить по разложению числа на множители, будет ли оно точным квадратом?

▷ Все простые множители должны входить в него чётное число раз. ◁

8.10* Докажите с помощью предыдущих задач (если вы этого еще не сделали другим способом раньше), что целое положительное число n имеет нечётное число делителей тогда и только тогда, когда оно является точным квадратом.

▷ В задаче 7 мы видели, что число делителей равно произведению кратностей в разложении, увеличенных на 1. Чтобы это произведение было нечётным, необходимо и достаточно, чтобы все кратности были чётны. ◁

8.11 Как, глядя на разложение на множители двух целых положительных чисел, узнать, будут ли они взаимно простыми?

▷ Посмотреть, есть ли у них общие простые делители в разложениях: если есть, то они явно не взаимно просты, если нет, то простых общих делителей нет (здесь используется однозначность разложения!), поэтому и никаких нет (любой общий делитель можно разложить на простые). ◁

8.12 Как, глядя на разложение на множители целого положительного числа, определить, сколько у него на конце нулей в десятичной записи?

▷ Что такое число нулей на конце? это максимальная степень $10^n = 2^n 5^n$, на которую число делится. Значит, надо посмотреть, сколько в разложении двоек и сколько пятёрок, и взять минимум из этих двух кратностей. ◁

8.13 Как, глядя на разложение на множители двух целых положительных чисел a и b, найти их наибольший общий делитель? Почему сразу ясно, что он делится на любой другой общий делитель?

▷ В общий делитель каждое простое число должно входить с кратностью не больше чем в a и не больше чем в b. Делитель будет наибольшим, если эта кратность максимальна.

Другими словами, общие делители чисел

$$N = 2^{n_2} 3^{n_3} 5^{n_5} \quad \text{и} \quad M = 2^{m_1} 3^{m_2} 5^{m_5}$$

имеют вид $2^{k_2} 3^{k_3} 5^{k_5} \ldots$, где k_p не превосходит n_p и m_p. Наибольший общий делитель получится, если $k_p = \min(n_p, m_p)$. (Через $\min(u, v)$ обозначается минимум из двух чисел u и v — то из них, которое меньше, или любое, если они равны.) ◁

• Глядя на эту задачу, можно было бы подумать, что алгоритм Евклида не особо и нужен: можно разложить числа на множители и потом найти их

наибольший общий делитель описанным способом. С точки зрения практики это совсем не так: раскладывать на множители большие числа гораздо сложнее. Число из нескольких тысяч цифр на современных компьютерах разложить часто не удаётся — а найти наибольший общий делитель двух чисел такого размера с помощью алгоритма Евклида можно практически мгновенно.

8.14 Используя предыдущую задачу, покажите, что для целых положительных a, b, k выполняется равенство $\text{НОД}(ka, kb) = \text{НОД}(a, b)$. (Раньше мы видели другое доказательство, с помощью алгоритма Евклида.)

▷ Кратность какого-то простого p в ka и kb получается из кратностей в a и b добавлением кратности в k, поэтому и минимум тоже увеличится на кратность p в k. Что соответствует умножению $\text{НОД}(a, b)$ на k. ◁

8.15 Как найти наименьшее общее кратное двух чисел, зная их разложение на множители? Почему любое общее кратное делится на наименьшее общее кратное?

▷ Если m — общее кратное a и b, то любое простое p входит в разложение m не меньше раз, чем в a и чем в b, и наоборот. Поэтому надо взять максимум из кратностей p в сомножителях. ◁

Будем обозначать наименьшее общее кратное двух целых положительных чисел a и b через $\text{НОК}(a, b)$. (В английских текстах иногда используют обозначение $\text{lcm}(a, b)$, сокращение от least common multiple.)

8.16 Докажите, что для любых целых положительных a и b выполняется равенство

$$\text{НОД}(a, b) \cdot \text{НОК}(a, b) = ab$$

▷ Это следует из сказанного выше про кратности и очевидного соотношения $\min(u, v) + \max(u, v) = u + v$. ◁

• Когда складывают две простые дроби, часто ищут наименьшее кратное их знаменателей (чтобы привести дроби к общему знаменателю).

8.17 В каких случаях наибольшее кратное двух чисел равно их произведению?

▷ Если числа взаимно просты (это следует, например, из предыдущей задачи). ◁

Наибольший общий делитель и наименьшее общее кратное можно определить не только для двух, но и для трёх (и более) чисел (посмотрев

на все общие делители, то есть числа, являющиеся делителями всех трёх, и выбрав наибольший, и т.п.).

8.18* Докажите, что для любых целых положительных a, b и c выполняется равенство

$$\text{НОК}(a,b,c) = \frac{a \cdot b \cdot c \cdot \text{НОД}(a,b,c)}{\text{НОД}(a,b) \cdot \text{НОД}(a,c) \cdot \text{НОД}(b,c)}.$$

• Эта формула аналогична так называемой *формуле включений и исключений* для числа элементов в множествах: $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.

▷ Достаточно проверить, что для любого простого p кратности в левой и правой части одинаковы. Это сводится к проверке тождества

$$\max(u,v,w) = u + v + w + \min(u,v,w) - \min(u,v) - \min(u,w) - \min(v,w).$$

От перестановок это тождество не меняется, поэтому достаточно его проверить для $u \leqslant v \leqslant w$, а тогда это будет

$$w = u + v + w + u - u - u - v,$$

и всё сокращается. ◁

• В этом решении есть пробел: а почему дробь в правой части целая и вообще можно считать кратности? Можно заметить, что сомножители в знаменателе делят a, c и b соответственно и потому числитель их сокращает. А можно перенести знаменатель в левую часть, тогда вопрос отпадает и рассуждение действует, а потом поделить.

8.19 Используя теорему об однозначности разложения на множители (и уже выведенные из неё следствия), докажите заново уже встречавшиеся нам утверждения: (а) если ab делится на k и a взаимно просто с k, то b делится на k; (б) если a делится на каждое из двух взаимно простых чисел b и c, то a делится на их произведение bc.

▷ (а) Если ab делится на k, то разложение ab содержит разложение k, но в a нет тех множителей, которые есть в k, так что все они приходятся на b. (б) В разложении a есть разложение b и есть разложение c, при этом они не пересекаются, так как b и c не имеют общих множителей. ◁

8.20 Докажите, что если для некоторого целых положительных a и n уравнение $x^n = a$ имеет рациональное решение (найдётся рациональное x, для которого $x^n = a$), то найдётся и целое решение этого уравнения.

▷ Пусть $(u/v)^n = a$ для целых u и $v \neq 0$. Можно считать $v > 0$ (изменим знак у u и v, если нужно). Можно считать также, что $u > 0$. В самом деле, если n нечётно, то это автоматически так, а если чётно, то знак можно поменять. Теперь разложим u и v на множители (и сократим общие, если они есть). Если в знаменателе что-то останется, то оно никуда не денется и после возведения в степень, так что u^n/v^n — тоже несократимая дробь. Получаем два разных разложения $u^n = av^n$, что противоречит теореме о единственности разложения на множители. ◁

8.21* Покажите, что кратность любого простого множителя p в разложении на множители числа $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ равна

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots$$

Здесь $\lfloor u \rfloor$ обозначает целую часть (наибольшее целое, не превосходящее u); сумма в правой части обрывается, когда все дальнейшие слагаемые становятся равны нулю (потому что очередные степени p все больше n).

▷ Множители p в разложении для $n!$ появляются, когда сомножитель в $1 \cdot 2 \cdot \ldots \cdot n$ кратен p. Таких кратных сомножителей как раз $\lfloor n/p \rfloor$ (а именно, $p, 2p, \ldots kp$, где k — максимальное целое, меньшее или равное n/p). Но могут быть и сомножители, в которых p входит несколько раз: $p^2, 2p^2, \ldots, kp^2$ при $k = \lfloor n/p^2 \rfloor$. Как подсчитать общий вклад? Есть такой способ считать сумму нескольких целых положительных чисел: подсчитать все числа по разу, потом ещё раз пересчитать числа, большие или равные 2, потом ещё добавить числа, большие или равные 3, и так далее. Тогда число, равное u, будет как раз u раз и посчитано. Этот способ подсчёта и даёт утверждение задачи. ◁

8.22* Следуя предыдущей задаче, покажите, что для любого целого $n \geqslant 2$ произведение любых последовательных n чисел делится на $n!$ (сравнив кратного произвольного простого p в этом произведении и в $n!$).

▷ В соответствии с методом подсчёта в предущей задачи достаточно убедиться, что среди $1, 2, \ldots, n$ не больше кратных p^k, чем в любых подряд идущих

n чисел. Количество кратных зависит от того места натурального ряда, с которого мы начинаем считать, то меньше всего их будет в том случае, когда мы начинаем точно сразу после очередного кратного (как с $1, 2, 3, \ldots, n$, которые сразу следуют за 0). ◁

8.23* Покажите, что среди степеней двойки $1, 2, 4, 8, \ldots$ и степеней тройки $1, 3, 9, 27, \ldots$ не только нет общих чисел, кроме 1, но нет и соседних чисел, кроме четырёх пар: $(1, 2)$, $(2, 3)$, $(3, 4)$ и $(8, 9)$. (Это установил ещё в XIV веке Леви бен Гершон — который помимо математики занимался талмудом, астрономией и многим другим.)

• Верно гораздо более сильное утверждение: если рассматривать степени целых чисел (кроме первой, то есть квадраты, кубы и т.д.), то среди них не найдётся двух идущих подряд чисел, кроме 8 и 9. Эта *гипотеза Каталана*, сформулированная аж в 1844 году, была доказана только сравнительно недавно (2002, Михайлеску), и доказательство сложное.

▷ Надо искать решения уравнений $2^m = 3^n + 1$ и $3^m = 2^n + 1$. Начнём с первого. Начиная с 8. левая часть делится на 8, значит, и правая часть должна делиться, то есть $3^n \equiv 7 \pmod 8$, а так не бывает (остатки у степеней 3 по модулю 8 чередуются: $1, 3, 1, 3, \ldots$. Среди меньших 8 (кроме указанных вариантов) решений очевидно нет.

Второе: $3^m = 2^n + 1$. Снова рассуждая по модулю 8, видим, что m должно быть чётно, так что достаточно доказать, что непредвиденных решений у уравнение $3^{2k} = 2^n + 1$ нет. Переписав его как $3^{2k} - 1 = 2^n$ и разложив левую часть как $(3^k - 1)(3^k + 1)$, видим, что обе скобки должны быть степенями двойки, и отличаться на 2, так что это может быть только 2 и 4, снова ничего непредвиденного не получается. ◁

8.24* Для целого положительного числа n можно подсчитать количество его делителей, которое мы обозначим $\tau(n)$, и сумму всех его делителей, которую мы обозначим $\sigma(n)$. Покажите, что если (целые положительные) числа a и b взаимно просты, то $\tau(ab) = \tau(a)\tau(b)$ и $\sigma(ab) = \sigma(a)\sigma(b)$. Найдите $\tau(4620)$ и $\sigma(4620)$, используя разложение $4620 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$.

• Указанное в этой задаче свойство функций σ и τ иногда называют *мультипликативностью*. Оно останется верным, если мы рассмотрим сумму любых степеней делителей, скажем, сумму их квадратов. (Для степени 0 получается τ, для степени 1 получается σ.)

▷

Выпишем все делители чисел a и b: пусть это будут $u_1, \dots, u_k$ и $v_1, \dots, v_l$ соответственно. Если перемножить какие-то u_i и v_j, то произведение $u_i v_j$ будет делителем числа ab. Поскольку a и b взаимно просты, так получатся все делители ab, и каждый по одному разу. В самом деле, любой делитель ab разлагается на простые множители, и можно разделить эти множители на те, которые встречаются в a, и те, которые встречаются в b. Отсюда сразу следует, что $t(ab)$ (число делителей ab) равно числу пар (делитель a, делитель b), то есть $\tau(a)\tau(b)$.

Для σ: раскроем скобки в произведение $\sigma(a)\sigma(b) = (u_1 + \dots + u_k)(v_1 + \dots + v_l)$, получится сумма kl слагаемых вида $u_i v_j$, то есть как раз сумма всех делителей числа ab.

То же рассуждение годится и для суммы s-х степеней делителей при любом s.

Теперь легко посчитать ответ для нашего примера:

$$\tau(2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11) = \tau(2^2)\tau(3)\tau(5)\tau(7)\tau(11) = 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 48$$

(это мы уже обсуждали). Для суммы:

$$\sigma(2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11) = \sigma(2^2)\sigma(3)\sigma(5)\sigma(7)\sigma(11) = \\ = (1+2+4)(1+3)(1+5)(1+7)(1+11) = 7 \cdot 4 \cdot 6 \cdot 8 \cdot 12 = 16\,128.$$

$\triangleleft$

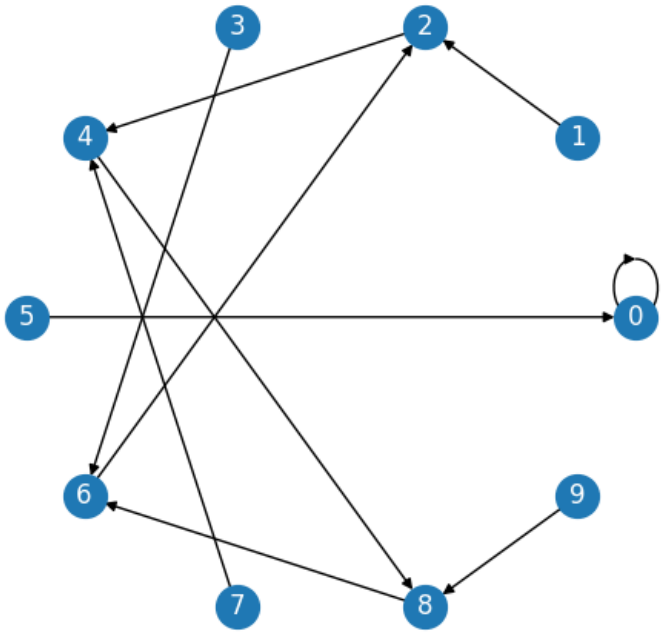
8.25* Пусть n — целое положительное число, которое не делится ни на 2, ни на 5. Докажите, что существует число вида 111 ... 111 (несколько единиц подряд в десятичной записи), которое делится на n.

• В качестве первого шага можно доказать, что некоторое число вида 1111 ... 111000 ... 000 делится на n (тут даже не важно, на что n не делится).

$\triangleright$ В бесконечной последовательности $1, 11, 111, 1111, \dots$ есть два числа, дающие одинаковые остатки при делении на n, поэтому их разница делится на n. Если n взаимно просто с 10, то нули на конце можно убирать без нарушения делимости. $\triangleleft$

9. Малая теорема Ферма

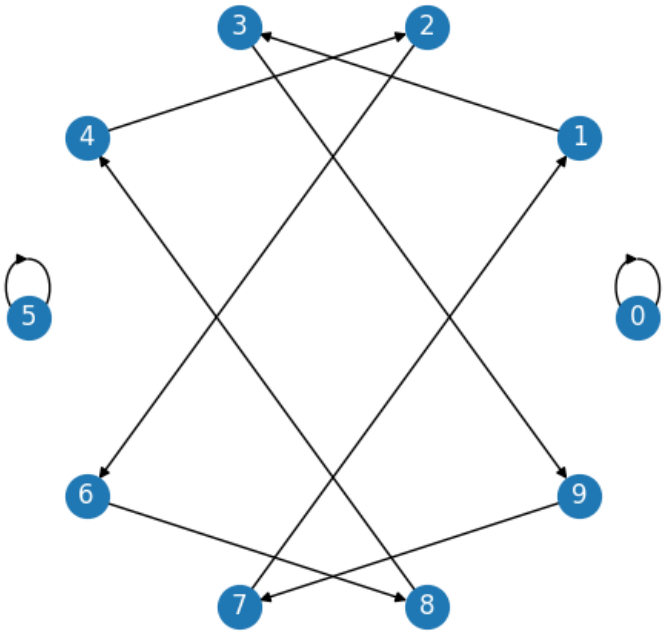
Мы уже обращали внимание на то, что последние цифры степеней двойки (и вообще любого числа) с какого-то момента повторяются по циклу: 1, 2, 4, 8, 6, 2, 4, 8, 6, 2, 4, 8, 6 … (первая единица в цикл не входит, а дальше повторения по четыре). Сейчас мы посмотрим на это подробнее, для чего нарисуем схему переходов.



На этой схеме из каждого остатка по модулю 10 идёт стрелка, соответствующая умножению его на 2 (по модулю 10)

9.1 Найдите на этой картинке упомянутый цикл.

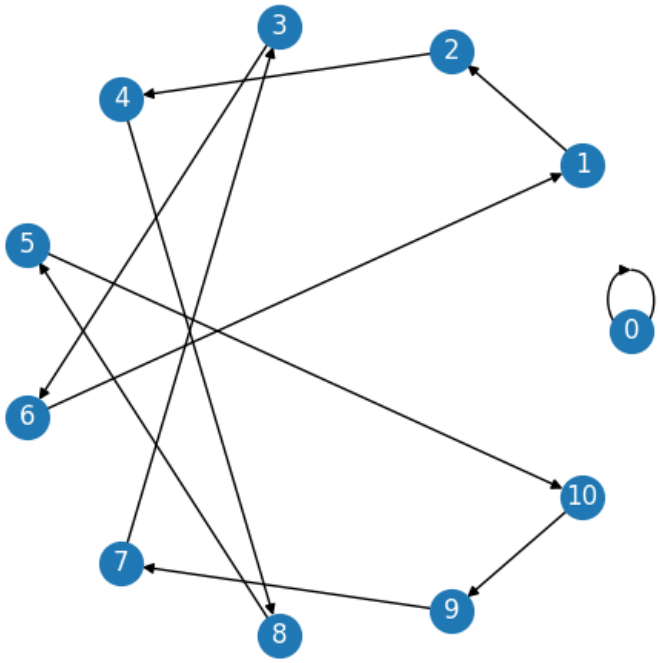
▷ Надо пройти по стрелкам, начиная с 1. ◁



9.2 Сколько циклов и какой длины есть в графе умножения остатков по модулю 10 на 3 на рисунке? Как будут меняться последние цифры степеней тройки?

▷ Видны два цикла длины 1 (если число кончается на 0 или на 5, то умножение на 3 не меняет последней цифры) и два цикла длины 4. Один из них соответствует последним цифрам степеней тройки: 1, 3, 9, 7, 1, 3, 9, 7, 1 … и далее по циклу. ◁

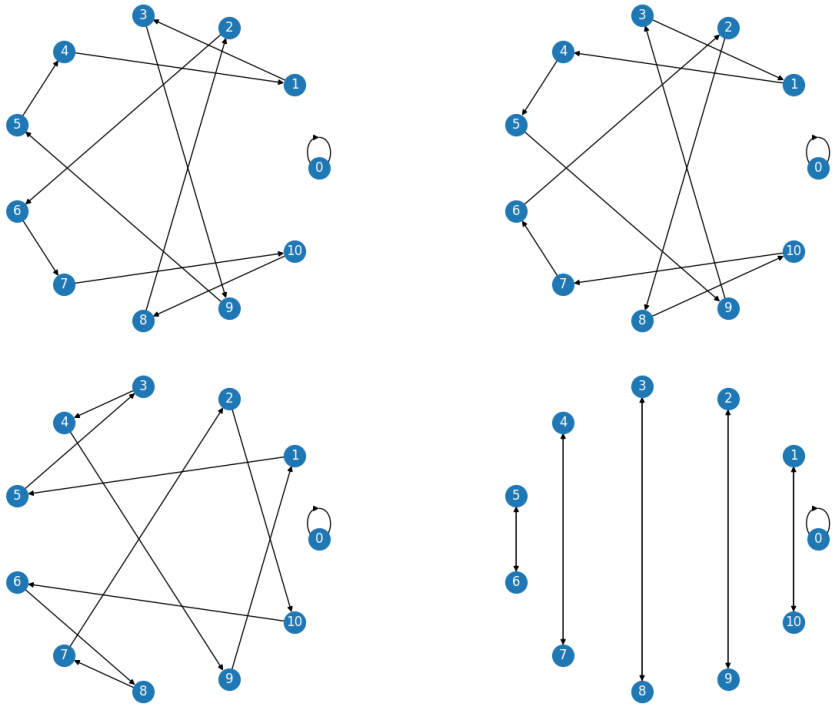
Мы уже обсуждали, что простые модули ведут себя более регулярно (все остатки, кроме нуля, обратимы, можно сокращать и т.п.). Вот один из графов умножения для простого модуля 11.



9.3 На что мы умножаем на этом рисунке? Какой будет период в последовательности остатков? Найдите $2^{179} \bmod 11$, глядя на эту картинку.

▷ Чтобы узнать, на что мы умножаем, надо посмотреть, куда переходит стрелка из 1, так что умножаем мы на 2. Там получается один цикл длины 10 (помимо цикла длины 1 из одного нуля, который есть всегда), так что 2^{180} по модулю 11 равно $2^0 = 1$, а 2^{179} будет предыдущим по циклу, то есть 6. ◁

По тому же модулю 11 можно нарисовать графы умножения на другие числа (слева направо множители 3 и 4 в верхнем ряду, 5 и 10 в нижнем).



9.4 Рассматривая эти картинки, можно заметить некоторые закономерности и понять, отчего так получается. Почему, скажем, две верхние картинки так похожи друг на друга (надо присмотреться, чтобы заметить, что стрелки ведут в противоположные стороны)? Почему последняя картинка состоит из отрезков (циклов длины 2, туда-сюда?

▷ Если сначала умножить на 3, а потом на 4 (или в другом порядке), то мы умножим на $12 \equiv 1 \pmod 1$1, то есть вернёмся в исходную точку. Поэтому стрелки обратны.

Умножая на 10, мы всё равно что умножаем на -1 (поскольку $-1 \equiv 10 \pmod 1$)1, а второе умножение на -1 возвращает в исходную точку. ◁

Теперь докажем некоторые общие свойства графов умножения на данное a по простому модулю p.

9.5 Докажите, что из каждой вершины выходит одна стрелка и в каждую вершину входит одна стрелка.

▷ То, что выходит одна стрелка, доказывать не требуется — так мы рисовали стрелки (из x ведёт стрелка в ax и только). А вот то, что в каждое y входит ровно одна стрелка, надо доказать. Другими словами, надо

доказать, что для любого y (и любого простого p и любого a, не равного 0 по модулю p уравнение $ax \equiv y$ (относительно x) имеет единственное решение. А это мы уже видели (умножая слева на обратный элемент a^{-1}, мы получаем, что $x = a^{-1}y$). ◁

9.6 Покажите, что стрелки разбиваются на несколько циклов.

• Стрелка, ведущая из вершину в неё саму же, считается циклом длины 1 (из одной вершины).

▷ Это следует из предыдущей задачи. Пойдём по стрелкам — рано или поздно мы должны попасть в вершину, где уже были. Но это может быть только начальная вершина (потому что иначе в неё будет две стрелки: одна уже нарисована ранее, одна новая. Значит, цикл замкнётся (и эти вершины уже больше ни с кем не связаны, так как все выходящие и входящие стрелки есть). ◁

9.7 У нас был граф умножения на 2 по модулю 10, и там вершина 1 не входила в цикл. Не противоречит ли это утверждению предыдущей задачи? Где не проходят наши рассуждения?

▷ Нет, потому что 2 не взаимно просто с 10 и не имеет обратного, поэтому в вершину могут входить несколько стрелок (скажем, в вершину 2 входят стрелки из 1 и 6). ◁

9.8 Покажите, что для простого модуля p в графе умножения на $a \neq 0 \pmod p$ все циклы имеют одинаковую длину (кроме тривиального цикла из одного нуля)

▷ Для этого полезно записать элементы цикла, начинающиеся с какого-то $b \neq 0$, с помощью формулы:

$$b \to ba \to ba^2 \to ba^3 \to \ldots$$

Цикл зациклится, когда мы дойдём (впервые) до $ba^m = b$. При каком m это случится? Можно сократить на b (умножить на обратный к b) и увидеть, что нам нужно минимальное m, при котором $a^m = 1$ (точнее следовало бы написать $a^m \equiv 1 \pmod p$, поскольку равенство и умножение понимаются по модулю p). А это m не зависит от b, так что все циклы одинаковы. ◁

Минимальное m, для которого $a^m \equiv 1 \pmod p$ (при простом p и $a \not\equiv 0 \pmod p$), называется *порядком* элемента a по модулю p.

Теперь всё готово для доказательства *малой теоремы Ферма*.

9.9 Докажите, что если p — простое число и $a \not\equiv 0 \pmod{p}$, то $x^{p-1} \equiv 1 \pmod{p}$.

▷ Мы знаем, что граф умножения на a без нуля разбивается на циклы одинаковой длины, равной порядку m элемента a. Значит, $p-1$ (общее число элементов в циклах) делится на m (длину цикла). Поскольку $a^m \equiv 1$ и $p-1$ кратно m. то и $a^{p-1} \equiv 1 \pmod{p}$. ◁

▷ Это тот же самый Ферма, что и с $x^n + y^n \neq z^n$, но теорема другая («малая», а не «последняя» или «великая») — и тут Ферма, возможно, действительно знал доказательство, хотя и не опубликовал: в его письме от 1640 года говорится, что он мог бы послать доказательство, если не бы не опасался быть многословным. Доказательство было опубликовано Эйлером в 1736 году (почти что через сто лет). ◁

Умножив равенство $a^{p-1} \equiv 1 \pmod{p}$ ещё раз на a, мы замечаем, что $a^p \equiv a \pmod{p}$. Теперь оговорку про то, что a не делится на p, можно убрать (потому что для этого случая равенство верно по очевидным причинам), и мы можем сформулировать малую теорему Ферма так: *для любого простого p и для любого целого a разность $a^p - a$ делится на p.*

- Для этого утверждения можно предложить и другие доказательства.

9.10* Пусть p — простое число и $a \not\equiv 0 \pmod{p}$. Докажите, что произведение $A = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)$ по модулю p

(а) умножится на a^{p-1} и

(б) не изменится,

если все сомножители умножить на a, и выведите отсюда малую теорему Ферма.

▷ Первая часть очевидна (надо просто сгруппировать все множители a в начале). Вторая следует из того, что при такой замене (x на ax) мы пройдём из всех вершин по стрелкам, и по-прежнему останется произведение всех ненулевых остатков, хотя и в другом порядке. Ведь в каждую вершину входит ровно одна стрелка. Поскольку $a^{p-1}A \equiv A \pmod{p}$, то можно сократить на A (заметим, что A не равно нулю по модулю p как произведение ненулевых элемнетов) и получить $a^{p-1} \equiv 1 \pmod{p}$. ◁

В предыдущей задаче мы доказали теорему Ферма, но так и не узнали, чему равно это самое $A \equiv (p-1)! \pmod{p}$. На этот вопрос отвечает *теорема Вильсона*: при простых p выполнено сравнение $(p-1)! \equiv -1 \pmod{p}$. Другими словами, *при простых p число $(p-1)!+1$ делится на p.*

9.11* Докажите теорему Вильсона.

▷ Разобьём все ненулевые остатки по модулю p на пары, объединив остаток с обратным, то есть включив в одну пару x, y, если $xy = 1$. Есть два остатка, обратных самому себе (1 и $-1 = p-1$), они так и останутся без пары, а остальные сомножите, сгруппировавшись в пары, дадут -1, что и требовалось доказать.

Видите пробел в этом рассуждении? Сгруппировать в пары можно (обратный единственный, поэтому каждый элемент войдёт только в одну пару), но почему только два элемента обратны самому себе? Вдруг найдётся ещё какой-то x, для которого $x^2 = 1$ по модулю p? Но тогда $x^2 - 1 = (x-1)(x+1)$ делится на p, так что одна из скобок должна делиться на p. Отсюда видно, что других таких нет, и доказательство завершается.

Ещё одна поправка: если $p = 2$, то 1 и -1 это один и тот же остаток, так что нельзя сказать, что непарных остатков 2. Но и в этом случае $(2-1)! + 1 = 2$ делится на 2. ◁

▷ Видимо, формулировка этого утверждения известна давно (похоже, что её знал уже Ибн аль-Хайсам, X–XI век), а доказательство предложил Лагранж в 1771. Так что Вильсон, кажется, тут скорее не по делу (возможно, он переоткрыл её формулировку). ◁

9.12* Покажите, что для любого составного p утверждение теоремы Вильсона неверно.

▷ Пусть q — простой делитель p. Тогда q входит в произведение для $(p-1)!$, поэтому $(p-1)!$ делится на q, а $(p-1)! + 1$ даёт остаток 1 при делении на q и не делится на q (и тем более на p). ◁

Вот ещё два доказательства малой теоремы Ферма, правда, использующие некоторые сведения из комбинаторики.

9.13* При простом p и любых целых a и b выполнено такое утверждение:

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Выведите из него малую теорему Ферма.

▷ Вывести можно так: $(a+b+c)^p \equiv ((a+b)^p + c^p) \equiv a^p + b^p + c^p$, и аналогично для большего числа слагаемых. Поэтому и $(1+1+\ldots 1)^p \equiv 1^p + 1^p + \ldots + 1^p \pmod{p}$ при любом числе m слагаемых, поэтому $m^p \equiv m \pmod{p}$ (второй вариант формулировки теоремы).

А само утверждение следует из того, что все биномиальные коэффициенты $C_p^i = \frac{p!}{i!(p-i)!}$ содержат p в числителе, но не в знаменателе, поэтому после сокращения общих простых множителей p останется. ◁

▷ Отображение $x \mapsto x^p$ называют *гомоморфизмом Фробениуса* (для полей характеристики p). ◁

9.14* Пусть есть n разных букв. Мы их пишем (одну букву можно использовать и несколько раз, и вообще не использовать) в вершинах правильного p-угольника разными способами, причём не различаем способы, отличающиеся лишь поворотом. Покажите, что число разных способов равно $n + (n^p - n)/p$. Выведите отсюда теорему Ферма.

▷ Если бы вращать не разрешалось, то было бы n^p вариантов. Объединим варианты, отличающиеся вращениями, в одну группу. Будет n групп по одному варианту (во всех вершинах одна буква), а остальные группы будут по p вариантов (многоугольник можно повернуть p способами), откуда и получается ответ.

Видите пробел в этом рассуждении? Где мы использовали, скажем, что p простое? Надо проверить, что если использованы две разные буквы, то никакой поворот не переводит многоугольник в себя. Если бы переводил, то можно было бы его повторять, пока не получится поворот на одну вершину (поскольку по простому модулю всякий ненулевой остаток обратим).

Теорема Ферма вытекает из этого подсчёта, потому что число вариантов целое. ◁

• С помощью теоремы Ферма можно доказать, что некоторое число составное. Например, 12 составное, потому что $5^{11} \bmod 12 = 5$ (а не 1, как должно быть по теореме Ферма, будь 12 простым). Это выглядит глупо — мы доказываем очевидное с помощью неочевидного, но как ни странно, это имеет некоторый смысл. А именно, для больших чисел это может быть сильно проще, чем разлагать на множители. Скажем, можно проверить, что для $n = 2^{512}+1$ и $a = 3$ теорема Ферма не выполнена: используя домашний компьютер и несложную программу, можно почти мгновенно понять, что $a^{n-1} \bmod n$ равно

13387457852131866017809974335626508736765841341908171621341620739066502578 7-
93457441078230804865246011339933833061458906559278633032869468345609327807927612

(число разбито на две строки), так что $n = 2^{512} + 1$ составное, но чтобы разложить n на множители, домашнего компьютера может и не хватить. (А некоторые составные — по теореме Ферма — числа вообще никто раскладывать на множители не умеет.) На разнице между сложностью задач проверки простоты и разложения на множители основана вычислительная криптография.

Числа $2^1+1, 2^2+1, 2^4+1, 2^8+1, 2^{16}+1, 2^{32}+1,\ldots$ называются «числами Ферма». Он предположил, что они все простые, посмотрев на первые пять — но Эйлер обнаружил делитель 641 для числа $2^{32} + 1$, так что это число составное, Ферма ошибся. Пока что других простых чисел Ферма, кроме этих пяти, не обнаружено,

и вообще мало что известно. Бесконечно ли много простых среди чисел Ферма? Бесконечно ли много составных? Эти вопросы остаются открытыми.

Теорема Ферма касается простых модулей, но аналогичное утверждение есть и для составных; его называют *теоремой Эйлера*. Рассуждения остаются почти без изменений, но нужно рассматривать не все остатки по данному модулю n, а только взаимно простые с n. Вспомним их основные свойства.

9.15 (а) Докажите, что если $a \equiv b \pmod{n}$, то $\text{НОД}(a,n) = \text{НОД}(b,n)$. В частности, взамная простота с n определяется остатком по модулю m. (б) Докажите, что остаток a взаимно прост с модулем n тогда и только тогда, когда он обратим по модулю n (и в этом случае обратный тоже взаимно прост с n). (в) Докажите, что произведение двух взаимно простых с n остатков (по модулю n) взаимно просто с n.

▷ (а) Это мы знаем ещё из алгоритма Евклида: добавление кратного n не меняет наибольшего общего делителя с n. (б) Обратный к a остаток x по модулю n можно найти, решая уравнение $ax + ny = 1$. Наоборот, если $ax \equiv 1 \pmod{n}$, то $ax + ny = 1$ для некоторого n, поэтому a и n взаимно просты. (в) Мы знаем, что произведение двух чисел, взаимно простых с n, тоже взаимно просто с n (например, потому, что ни в том, ни в другом нет общих множителей с n). Можно заметить также, что произведение двух обратимых элементов обратимо (и обратным будет произведение обратных). ◁

Число остатков по модулю n, взаимно простых с n, называют *функцией Эйлера* от n и обозначают $\varphi(n)$.

9.16 Чему равно $\varphi(p)$ для простого p? Чему равно $\varphi(p^k)$ для степени простого числа p?

▷ В обоих случаях надо считать остатки (от 0 до $p-1$ или от 0 до p^k-1), не делящиеся на p (взаимно просты с p те числа, которые не делятся на p). Другими словами нужно пропускать каждое p-е число, начиная с нуля. В первом случае пропускается только 0, во втором случае $p^k/p = p^{k-1}$ чисел, остаётся $\varphi(p) = p-1$ и $\varphi(p^k) = p^k - p^{k-1}$ взаимно простых остатков. ◁

Теперь у нас всё готово для теоремы Эйлера.

9.17 Докажите теорему Эйлера: если остаток a взаимно прост с модулем n, то $a^{\varphi(n)} \equiv 1 \pmod{n}$.

• Если n простое, то все остатки, кроме нуля, с ним взаимно просты, а $\varphi(n) = n - 1$, так что получается в точности малая теорема Ферма.

▷ Нарисуем граф умножения на a по модулю n, но оставим в нём из вершин только взаимно простые с n. По-прежнему из каждой вершины ведёт по стрелке (потому что при умножении на a взаимная простота сохраняется, см. задачу 15). Остатки обратимы, поэтому решать уравнение $ax \equiv b \pmod{n}$ можно умножением на обратный. Значит, в каждую вершину входит только одна стрелка, и стрелки разбиваются на циклы. Как и раньше, цикл, начинающийся с b, имеет вид $b \to ba \to ba^2 \to \ldots$, и замыкается, когда $a^m = 1$ (здесь мы снова должны сослаться на обратимость), поэтому все циклы равной длины. Общее число вершин теперь $\varphi(n)$, поэтому $\varphi(n)$ делится на длину цикла, откуда и следует требуемое утверждение. ◁

9.18* Сколько решений имеет сравнение $x^2 \equiv 1 \pmod{pq}$, если p и q — различные простые числа? Найдите все решения при $p = 7$, $q = 5$.

▷ По китайской теореме об остатках нам надо искать отдельно решения этого сравнения по модулю p и по модулю q. Для простых модулей мы уже видели, что решений два: 1 и -1. (Если $x^2 - 1$ делится на p, то $(x-1)(x+1)$ делится на p.) Теперь два решения по одному модулю надо комбинировать с двумя решениями по другому модулю. Например, при $pq = 35$ получатся не только комбинации 1 и $-1 \equiv 34$, но и остаток x, для которого $x \equiv 1 \pmod{5}$ и $x \equiv -1 \pmod{7}$, то есть $x \equiv 6 \pmod{35}$, а также другой остаток x, для которого $x \equiv -1 \pmod{5}$ и $x \equiv 1 \pmod{7}$, то есть $x \equiv 29 \pmod{35}$. ◁

9.19* Докажите, что функция Эйлера мультипликативна: если m и n взаимно просты, то $\varphi(mn) = \varphi(m)\varphi(n)$.

▷ Тут полезна китайская теорема об остатках. Каждому остатку по модулю mn соответствует пара остатков: по модулю m и по модулю n, и наоборот (китайская теорема об остатках). При этом взаимно простым с mn остаткам соответствуют пары, в которых остатки взаимно просты с m и n соответственно: число не имеет общих делителей с mn тогда и только тогда, когда у него нет общих делителей ни с m, ни с n. А таких пар будет $\varphi(m)\varphi(n)$. ◁

Это рассуждение годится при $m, n > 1$. Вообще $\varphi(1)$ это некоторый особый случай, и мы положим $\varphi(1) = 1$ — для того, в частности, чтобы предыдущая задача была верна при всех m, n, включая 1.

9.20* Покажите, что для любого числа $n > 2$ выполняется тождество $\sum_{d|n} \varphi(d) = n$ (где сумма берётся по всем делителям числа n).

- Например, $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) = 1 + 1 + 2 + 2 = 6$. А для простого p мы получаем $\varphi(1) + \varphi(p) = 1 + (p - 1) = p$. Напомним, что мы считаем $\varphi(1)$ равным 1.

▷ Все остатки по модулю n можно разбить на группы, объединив в одну группу те, у которых равный наибольший общий делитель с n. Например, одну группу образуют остатки, взаимно простые с n, и в этой группе по определению $\varphi(n)$ остатков.

А сколько будет остатков x (будем считать, от 0 до $n - 1$), для которых НОД $(x, n) = 2$? Если n нечётно, то их совсем не будет. А если n чётно (и равно $2m$ при $m = n/2$)? Тогда эти остатки равны $2y$, где $0 \leqslant k < m$. Для всех таких $2y$ число 2 будет общим делителем с m, но не обязательно наибольшим: мы знаем, что НОД $(2y, 2m) = 2$ НОД (y, m), и поэтому нам нужны только те, для которых НОД $(y, m) = 1$. А их будет $\varphi(m)$.

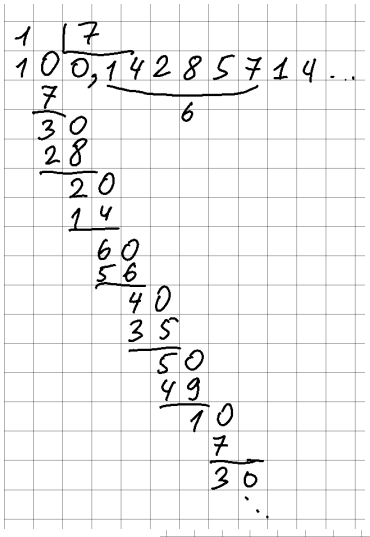
Аналогичное рассуждение показывает, что остатков x по модулю n, для которых НОД $(x, n) = d$,

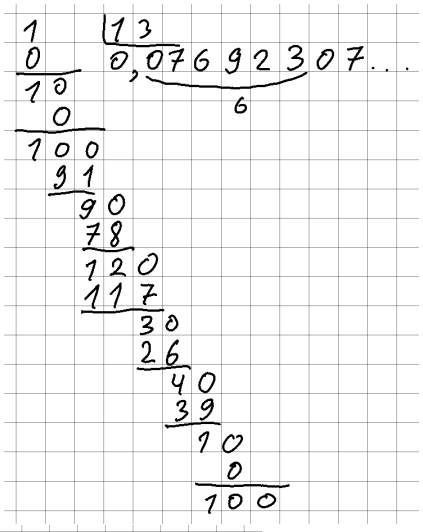
- ровно $\varphi(n/d)$, если d делит n;
- не существует, если d не делит n.

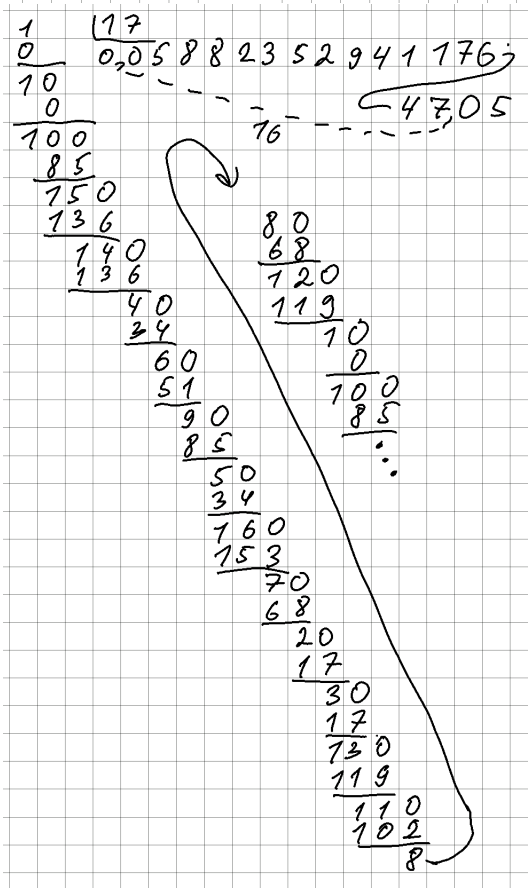
(Тут надо отдельно проверить случай $d = n$, потому что $\phi(1)$ определялось особо, но там ровно один остаток 0 годится.)

Осталось записать утверждение о том, что общее число остатков во всех группах равно n. ◁

С распространением калькуляторов благородное искусство деления уголком постепенно утрачивается, но когда-то оно было одним из базовых навыков в курсе арифметики. С его помощью можно было получать результат деления в виде бесконечной десятичной дроби.







9.21* Каким образом выполняется деление с остатком? Почему при делении целых чисел получается всегда периодическая дробь? Докажите, что в дроби $1/p$, где p — простое число, период начинается с самого начала (сразу после нуля), а длина этого периода является делителем $p-1$.

• В наших примерах 6 делит $7-1$ (для 1/7), а также 6 делит $13-1$ (для 1/13), наконец, 16 делит $17-1$ (для 1/17).

▷ Глядя на примеры, мы видим, что происходит вот что. Текущий остаток (под горизонтальной чертой, вначале 1) умножается на 10 (приписывается нуль). Затем полученное число делится на p (делитель, он справа в уголке), неполное частное добавляется к дроби, а с остатком процесс повторяется.

Ясно, что все остатки не больше делителя, так что их конечное число, и они должны начать повторяться. Как только повторится остаток, всё дальнейшее тоже повторится. Значит, получается периодическая дробь (в которой какая-то группа цифр повторяется вновь и вновь). Не обязательно эта группа начинается с нуля: например, $1/6 = 0{,}16666\ldots$.

Но если делитель — простое число, то период начинается с самого начала. Почему? Можно заметить, остаток каждый раз умножается на 10 по модулю p, поэтому движение будет по циклу в графе умножения на 10 по модулю p. Мы знаем, что для простого модуля все вершины разбиваются на циклы одинаковой длины, и длина эта является делителем $p-1$, и одновременно периодом нашей десятичной дроби.

Остаётся один последний вопрос: может быть, у дроби есть и меньший период? Ведь цифры в частном могут повториться, даже если остатки не повторяются. (Например, в 1/17 период равен 16, и многие цифры входят несколько раз — иногда даже подряд.) Тут можно сослаться на то, что у любой последовательности символов длина *наименьшего* периода является делителем длины любого периода (иначе разделим с остатком, и остаток будет меньше — а периоды тоже образуют идеал). Поэтому, даже если бы период в частном был бы меньше периода в остатках, то он был бы его делителем и ничего бы не нарушилось. Но на самом деле период в частном и период в остатках одинаковы. Проще всего (хотя и не вполне строго) это объяснить так: дробь с какого-то места является десятичным представлением соответствующего остатка, делённого на p, и если с двух мест дроби одинаковы, то и остатки одинаковы. ◁

9.22* Пусть p — простое число. Сумму дробей

$$\frac{1}{1}+\frac{1}{2}+\ldots+\frac{1}{p-1}$$

привели к общему знаменателю. Докажите, что числитель полученной дроби делится на p.

- Например, при $p = 5$ получается

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4} = \frac{2\cdot 3\cdot 4 + 1\cdot 3\cdot 4 + 1\cdot 2\cdot 4 + 1\cdot 2\cdot 3}{1\cdot 2\cdot 3\cdot 4} = \frac{24+12+8+6}{24} = \frac{50}{24} = \frac{25}{12},$$

и 25 делится на 5.

▷ Посмотрим на вычисления, сделанные при приведении к общему знаменателю. Мы умножаем числители и знаменатели дробей на ненулевые выражения (как в обычном смысле, так и по модулю p), потом их складываем, потом сокращаем на ненулевые выражения (ненулевые, поскольку в знаменателе нет кратных p). Поэтому на это можно смотреть как на корректное вычисление в остатках по модулю p. Слева получится сумма всех обратных величин к ненулевым остаткам, то есть сумма всех ненулевых остатков, которые группируются на пары, в сумме равные нулю (1 и $p-1$, 2 и $p-2$ и так далее; заметим, что $p-1$ чётное число). Поэтому и правая часть равна 0, то есть числитель дроби равен нулю по модулю p, что и требовалось доказать. ◁

10. Что дальше?

Теория чисел (или, как раньше говорили, *высшая арифметика*), пожалуй, в максимальной степени иллюстрирует разрыв между простотой вопроса и сложностью ответа на него: на некоторые естественные вопросы ответ неизвестен до сих пор, а ответ на другие потребовал сложных математических теорий. Мы разобрали только самые базовые понятия, связанные с целыми числами; в этом разделе мы упомянем некоторые другие результаты (разной сложности).

Распределение простых чисел

Мы знаем, что простых чисел бесконечно много, и что бывают сколь угодно длинные отрезки, состоящие только из составных чисел. Но это очень слабые утверждения, которые мало говорят о том, насколько редки простые числа среди всех натуральных чисел: известно много больше.

Постулат Бертрана утверждает, что между n и $2n$ всегда есть простое число. Эта гипотеза была сформулирована Бертраном в 1845 году и вскоре (в 1852) была доказана Чебышёвым. Он же показал, что доля простых чисел среди чисел от 1 до N примерно пропорциональна $1/\log N$. Впоследствии более точный вариант этого утверждения, называемый *асимптотическим законом распределения простых чисел*, был доказан (в 1896 году) Адамаром и Валле-Пуссеном с использованием дзета-функции Римана (и разных фактов из комлексного анализа).[1]

Таким образом, доля простых чисел постепенно убывает, но достаточно медленно. Мы уже обсуждали в одной из задач, что она становится сколь угодно малой (простое следствие результатов Чебышёва). Немного продолжив наши рассуждения, можно установить, что сумма обратных величин к простым числам, $\sum 1/p$, может быть сделана сколь угодно большой, если взять достаточно много простых чисел (так что простые числа не слишком редки).

Реально интервалы между соседними простыми числами много меньше, чем это гарантируется постулатом Бертрана, но тут много открытых

[1]Функция Римана определяется как $\zeta(s) = \sum_n 1/n^s$, изначально при действительных $s > 1$, но потом её можно продолжить на другие действительные (а также комплексные) числа; в теории чисел есть знаменитая *гипотеза Римана*, которая говорит, что все нули этой функции, кроме действительных, имеют действительную часть 1/2.

вопросов: скажем, *гипотеза Лежандра* о том, что между двумя квадратами (n^2 и $(n+1)^2$) всегда есть хотя бы одно простое число, остаётся (2022) недоказанной (и не опровергнутой).

Можно интересоваться простыми числами специального вида. Например, все простые числа (кроме единственного чётного простого числа 2) делятся на два вида: $4k+1$ и $4k+3$. Оказывается, что и тех, и других бесконечно много; вообще, *теорема Дирихле* говорит, что в любой арифметической прогрессии

$$a, a+d, a+2d, a+3d, \ldots$$

при любых целых взаимно простых a и d бесконечно много простых чисел. (Если a и d имеют общий делитель, то он делит все члены прогрессии, так что в этом случае простое число может быть только одно.) Доказательство этого факта (как и для асимптотического закона распределения простых чисел) использует математический анализ и достаточно сложное — но для некоторых конкретных прогрессий это доказывается легко.

10.1* Покажите, что существует бесконечно много простых чисел, дающих остаток 3 при делении на 4 (имеющих вид $4k+3$).

▷ Заметим, что произведение простых чисел вида $4k+1$ всегда даёт остаток 1 при делении на 4, поэтому в разложении нечетного числа вида $4k+3$ всегда есть простой множитель того же вида. Если бы простых чисел вида $4k+3$ было конечное число, то мы могли бы взять их произведение N, и затем прибавить 2 или 4 так, чтобы получилось число вида $4k+3$, не делящееся ни на одно из выбранных простых чисел (потому что N на все делится, а 2 или 4 — нет). В разложении этого числа появится ещё одно простое число вида $4k+3$, противоречие. ◁

Много других фактов о простых числах (особенно когда их складывают, а не перемножают) формулируются просто, но доказываются сложно (или вообще до сих пор не доказаны). Скажем, знаменитая *гипотеза Гольдбаха* говорит, что всякое чётное число представляется в виде суммы двух простых чисел — и до сих пор не доказана.

Более слабое утверждение о том, что *всякое нечётное число, большее 7, можно представить в виде суммы трёх простых чисел* (его называют *слабой гипотезой Гольдбаха*) было доказано Хельфготтом (в 2013); для всех достаточно больших чисел его доказал Виноградов в 1937 году.

Ещё одна знаменитая гипотеза о простых числах говорит, что существует бесконечно много пар простых чисел, отличающихся на 2 (как 3 и

5, 11 и 13 и т. п.); такие пары называют *близнецами*. Эта гипотеза тоже до сих пор не доказана и не опровергнута (хотя и доказано для некоторых c, что есть бесконечно много пар простых чисел, отличающихся не больше чем на c).

Новые методы и результаты о простых числах продолжают появляться. Например, в 2004 году была доказана *теорема Грина–Тао*, утверждающая, что существуют сколь угодно длинные арифметические прогрессии, состоящие из простых чисел.

Рациональные приближения

Всякое действительное число может быть сколь угодно хорошо приближено рациональными числами: если нам надо приблизить число α рациональными числами со знаменателем n, можно посмотреть, в какой промежуток между числами

$$\dots, -\frac{3}{n}, -\frac{2}{n}, -\frac{1}{n}, 0, \frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \dots$$

оно попадает, и взять (любой) конец этого интервала. Все интервалы имеют длину $1/n$, поэтому ошибка приближения (модуль разности) будет не больше $1/n$.

Поэтому приближения со знаменателем n и ошибкой порядка $1/n$ не удивительны: они существуют при любом n. Однако бывают и гораздо более удачные приближения, скажем, знаменитое приближение Архимеда $22/7 = 3{,}1428257\dots$ для числа $\pi = 3{,}141592\dots$; тут ошибка только в третьем знаке (чуть больше $1/1000$) вместо $1/7$. Такие более удачные приближения бывают для любых чисел: *теорема Дирихле* утверждает, что для любого (действительного) числа α и любого N можно найти дробь m/n со знаменателем, не превосходящим N (то есть $n \leqslant N$) и ошибкой приближения меньше $1/nN$ (что сильно лучше точности $1/n$, гарантированной для любого знаменателя). В отличие от других результатов, упомянутых в этом разделе, это доказывается сравнительно просто.

10.2* Пусть $\alpha > 0$ — действительное число, а $N > 1$ — целое число. Тогда существует дробь m/n с $n \leqslant N$, для которой

$$\left| \frac{m}{n} - \alpha \right| < \frac{1}{nN}.$$

▷ Рассмотрим числа $0, \alpha, 2\alpha, 3\alpha, \dots, N\alpha$ по модулю 1 (на отрезке $[0,1]$, свёрнутом в кольцо). Всего у нас $N+1$ точек, так что есть две разные точки, отличающиеся меньше чем на $1/N$ (как точки на кольце). С другой стороны, по прямой (до сворачивания) они отличаются на $n\alpha$ при каком-то целом n от 1 до N, так что $n\alpha$ почти что целое число m (с точностью $1/N$):

$$|m - n\alpha| < \frac{1}{N}, \quad \text{то есть} \quad \left|\frac{m}{n} - \alpha\right| < \frac{1}{nN},$$

что и требовалось доказать. ◁

Это доказательство показывает, что хорошие приближения есть, но как их искать? На этот вопрос отвечают *цепные дроби*. Любое число α можно разложить в цепную дробь, например

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \cfrac{1}{\dots}}}}}$$

Для этого мы выделяем из $\pi = 3{,}1415926\dots$ целую часть 3, остаётся число $0{,}1415926\dots$, меньшее 1, из обратного к нему $1/(\pi - 3) = 7{,}06251\dots$ выделяем целую часть 7, из обратного к остатку $1/0{,}06251\dots = 15.9965\dots$ выделяем целую часть 15, и так далее.

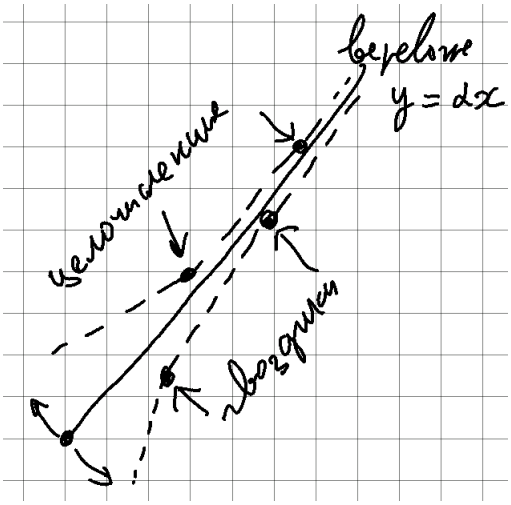
Затем, обрывая эту цепную дробь на конечном шаге, можно получать приближения

$$3 + \frac{1}{7} = \frac{22}{7}, \quad 3 + \cfrac{1}{7 + \cfrac{1}{15}} = \frac{333}{106}, \quad 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1}}} = \frac{355}{113}, \dots$$

которые приближают π лучше других дробей[2] (с теми же или меньшими знаменателями). Они называются *подходящими дробями* и имеют геометрический смысл, который можно описать так.

[2] К тому же 355/113 легко запомнить: надо написать 113355 и разбить посередине на числитель и знаменатель.

Вобьём гвоздики в точки с целыми координатами и протянем бесконечную верёвочку с наклоном α из точки $(0,0)$, то есть график $y = \alpha x$ при $x \geqslant 0$. Затем потянем за конец этой верёвочки в обе стороны — она упрётся в некоторые гвоздики. Эти самые гвоздики и будут соответствовать подходящим дробям при разложении α в цепную дробь (они будут чередоваться по разные стороны от прямой).



Для некоторых чисел приближения, гарантируемые теоремой Дирихле, близки к оптимальным. Таковы квадратичные иррациональности (корни квадратных уравнений с целыми коэффициентами), например, для $\sqrt{2}$ есть такая простая оценка:

10.3* Покажите, что число $\sqrt{2}$ не может слишком хорошо приближаться рациональными числами с небольшими знаменателями:

$$\left|\sqrt{2} - \frac{m}{n}\right| \geqslant \frac{1}{4n^2}$$

▷ Надо доказать, что $|m - n\sqrt{2}| \geqslant \frac{1}{4n}$. Заметим, что произведение

$$(m - n\sqrt{2})(m + n\sqrt{2}) = m^2 - 2n^2$$

будет ненулевым целым числом, и потому по модулю не меньше 1. Поэтому, если $m + n\sqrt{2}$ не превосходит $4n$, то всё доказано. Но если превосходит, то $m > 2n$, и $m/n > 2$, и разница между m/n и $\sqrt{2} = 1{,}41\ldots$ не меньше $1/2$, так что утверждение очевидно. ◁

С другой стороны, для него можно найти достаточно хорошие приближения; это можно сделать с помощью цепных дробей (Эйлер и Лагранж заметили ещё в XVIII веке, что квадратичные иррациональности соответствуют периодическим цепным дробям) или даже без них:

10.4* Покажите, что существует бесконечно много дробей m/n с целым числителем и знаменателем, для которых $m^2 - 2n^2 = 1$.

▷ Мы уже переписывали это уравнение в виде

$$(m - n\sqrt{2})(m + n\sqrt{2}) = 1.$$

Если есть два решения m_1, n_1 и m_2, n_2 этого уравнения, то можно их перемножить и получится

$$(m_1 - n_1\sqrt{2})(m_1 + n_1\sqrt{2})(m_2 - n_2\sqrt{2})(m_2 + n_2\sqrt{2}) = 1$$

Сгруппируем отдельно скобки с плюсами и минусами:

$$(m_1 + n_1\sqrt{2})(m_2 + n_2\sqrt{2}) = (m_1m_2 + 2n_1n_2) + (m_1n_2 + m_2n_1)\sqrt{2},$$
$$(m_1 - n_1\sqrt{2})(m_2 - n_2\sqrt{2}) = (m_1m_2 + 2n_1n_2) - (m_1n_2 + m_2n_1)\sqrt{2}.$$

Теперь можно заметить, что пара

$$m_3 = m_1m_2 + 2n_1n_2, \quad n_3 = m_1n_2 + m_2n_1$$

тоже будет решением этого уравнения. Другими словами, если «кодировать» решение (m, n) нашего уравнения числом $m + n\sqrt{2}$, то решения можно перемножать (и возводить в степень, умножая на себя многократно), и так получать сколько угодно решений. Например, можно начать с решения $3^2 - 2 \cdot 2^2 = 1$, кодируемого как $3 + 2\sqrt{2}$, и возвести его код в квадрат:

$$(3 + 2\sqrt{2})^2 = (3^2 + 2^2 \cdot 2) + 12\sqrt{2} = 17 + 12\sqrt{2},$$

и действительно

$$17^2 - 2 \cdot 14^2 = 289 - 288 = 1,$$

и $17/12 = 1{,}41666\ldots$ неплохо приближает $\sqrt{2} = 1{,}4142\ldots$. Возводя в куб, получаем

$$(17 + 12\sqrt{2})(3 + 2\sqrt{2}) = (51 + 2 \cdot 2 \cdot 12) + (17 \cdot 2 + 12 \cdot 3)\sqrt{2} = 99 + 70\sqrt{2},$$

и действительно $99^2 - 2 \cdot 70^2 = 981 - 980 = 1$, и так далее. ◁

• Для этих дробей разница между m^2 и $2n^2$ насколько мала, насколько это вообще возможно (равна 1), поэтому m/n хорошо приближает $\sqrt{2}$. Можно оценить, например, так: $m - n\sqrt{2} = 1/(m + n\sqrt{2}) < 1/n$ и $\frac{m}{n} - \sqrt{2} < 1/n^2$, почти как в теореме Дирихле.

Бывают и числа, которые приближаются дробями сильно лучше. Скажем, можно взять число

$$0,100\ldots00100\ldots00100\ldots001\ldots,$$

в десятичной записи которого единицы разделены большим (и быстро растущим, скажем, как факториалы) количеством нулей. Тогда, обрывая это число после очередной единицы, получаем приближение, в котором ошибка убывает быстрее любой степени знаменателя. Лиувиллль показал (1844), что такие хорошо приближаемые числа не только иррациональны (в нашем примере это следует из того, что дробь непериодическая), но и *трансцендентны*, то есть не являются корнями многочленов с целыми коэффициентами. Другими словами, теорема Лиувилля утверждает, что *алгебраические числа* (корни многочленов с целыми коэффициентами) не могут слишком хорошо приближаться рациональными числами. Гораздо более сильный результат (*теорема Рота*, 1955) в этом направлении говорит, что алгебраические числа не приближаются с ошибкой $1/n^c$ для $c > 2$: более точно, для всякого иррационального алгебраического числа α и для любого $c > 2$ существует лишь конечное число дробей m/n, для которых $|\alpha - m/n| < 1/n^c$.

Квадратичные вычеты

Посмотрим на остатки (или, как иногда говорят, *вычеты*) по модулю p. Будем смотреть, что получается при их возведении в квадрат (какие остатки может давать квадрат целого числа при делении на p). Скажем, если $p = 11$, то возможны остатки $0, 1, 4, 9, 5, 3$. Их (кроме нуля) называют *квадратичными вычетами* по модулю 11, остальные (в данном случае $2, 6, 7, 8, 10$) называют *квадратичными невычетами*. (Нуль не считают ни вычетом, ни невычетом.)

10.5* Покажите, что из ненулевых остатков по простому нечётному модулю p квадратичных вычетов ровно половина (то есть $(p-1)/2$). Покажите, что произведение двух вычетов будет вычетом. Покажите, что произведение вычета и невычета — невычет. Покажите, что произведение

двух невычетов — вычет. Покажите, что если x — вычет, то $x^{(p-1)/2} \equiv 1 \pmod{p}$.

▷ Посмотрим на все ненулевые остатки и их квадраты. Поскольку $(-x)^2 = x^2$ (в том числе по модулю p), то остатки x и $p - x$ дают один и тот же квадрат, значит вычетов не больше половины. Но и не меньше, поскольку склеиваются только по два: если $x^2 \equiv y^2 \pmod{p}$, то $x^2 - y^2 = (x+y)(x-y)$ делится на p, так что одна из скобок делится на p.

Если $x = u^2$ и $y = v^2$ (по модулю p), то $xy = (uv)^2$, так что произведение вычетов будет вычетом. По аналогичным причинам и частное двух вычетов (по модулю p) будет вычетом: $x/y = (u/v)^2$. Отсюда следует, что произведение вычета и невычета будет невычетом (иначе невычет был бы частным двух вычетов). Осталось доказать, что произведение невычетов — вычет. В самом деле, если x — невычет, то отображение $z \mapsto xz$ будет перестановкой остатков, которая переводит все вычеты в невычеты, значит, все невычеты использованы (вычетов и невычетов, как мы знаем, поровну), и ничего не остаётся, как переводить невычеты в вычеты.

Если $x = y^2$, то $x^{(p-1)/2} = y^{p-1} = 1 \pmod{p}$ (теорема Ферма). ◁

• Известно, что многочлен степени k имеет не более k корней (в том числе и рассматриваемый по модулю p). Поэтому, раз $(p-1)/2$ невычетов являются корнями уравнения $x^{(p-1)/2} = 1 \pmod{p}$, то других корней у этого многочлена нет, так что условие $x^{(p-1)/2} = 1 \pmod{p}$ выполнено для вычетов и не выполнено для невычетов. Отсюда следует, что -1 является невычетом по нечётному простому модулю p тогда и только тогда, когда p имеет вид $4k+1$ (а не $4k+3$). Другими словами, если p имеет вид $4k+1$, то можно найти целые числа x и y, не делящиеся на p, для которых $x^2 + y^2$ делится на p.

Используя сведения о многочленах и числе их корней, можно (сравнительно несложно) доказать, что для любого p среди вычетов по модулю p имеется *примитивный корень*, то есть такое x, что в последовательности

$$1, x, x^2, x^3, \ldots, x^{p-2}$$

(следующий будет снова 1 по теореме Ферма) встречаются все ненулевые вычеты по модулю p. В терминах графов это значит, что граф умножения ненулевых остатков на x состоит из единственного цикла.

Гаусс (1801) доказал *квадратичный закон взаимности*, который связывает два свойства нечётных простых чисел p и q: когда q является квадратичным вычетом по модулю p, и когда p является квадратичным вычетом по модулю q. Оказывается, что при чётном $(p-1)(q-1)/4$ эти

свойства эквивалентны, а при нечётном — противоположны (выполнено ровно одно из двух). Случай чётного $p = 2$ разбирается отдельно: число 2 является квадратичным вычетом по модулю нечётного простого q, если q даёт остаток 1 или 7 при делении на 8 (и не является, если q даёт остаток 3 или 5).

Есть много доказательств этого утверждения, в том числе и элементарные (не использующие ничего, кроме известных нам свойств и критерия $x^{(p-1)/2} \equiv 1 \pmod{p}$ для квадратичных вычетов) и даже не очень сложные, но они требуют изобретательности и аккуратности при подсчётах, и мы их не приводим.

Диофантовы уравнения

Диофантовым уравнением называется алгебраическое уравнение с целыми коэффициентами, у которого требуется искать целые решения. Многие вопросы теории чисел связаны с такими уравнениям. Например, иррациональность числа $\sqrt{2}$ означает, что уравнение $x^2 - 2y^2 = 0$ не имеет решений в целых числах. А вот уравнение $x^2 - 2y^2 = 1$ имеет, как мы видели, бесконечно много решений в целых числах.

Знаменитая *великая теорема Ферма* утверждает, что диофантовы уравнения $x^3 + y^3 = z^3$, $x^4 + y^4 = z^4$ и вообще $x^n + y^n = z^n$ при $n \geqslant 3$ не имеют решений в целых числах, кроме тривиальных (когда одно из чисел x, y, z равно нулю). Несколько столетий это было знаменитой открытой проблемой (хотя Ферма в XVII веке и написал, что знает доказательство, только на полях книги, где он делал заметки, оно не помещается). Постепенно для разных значений n это удавалось доказать: для $n = 4$ это было уже у Ферма, для $n = 3$ это доказал (хотя и не сразу правильно) Эйлер в конце XVIII века. Дальнейший прогресс для конкретных показателей был достигнут в XIX веке (Лежандр, Дирихле, Жермен, Куммер и другие), и это потребовало развития алгебраических методов; в XX веке дальнейшее развитие алгебры и использование компьютеров позволило доказать теорему Ферма для всех не слишком больших n (сначала тысячи, потом и миллионы). Параллельно много людей («ферматистов», как их называли) предлагали свои доказательства для общего случая, и они оказывались неправильными. Наконец, в конце XX века Уайлз (используя весьма сложную алгебраическую технику) придумал полное доказательство.

При $n = 2$ решения есть: числа x, y, z, для которых $x^2 + y^2 = z^2$, называют *пифагоровыми тройками*, поскольку по теореме Пифагора они соответствуют прямоугольным треугольникам с целыми сторонами. Самый знаменитый такой треугольник (известный ещё в древнем Египте) имеет стороны $3, 4, 5$; в самом деле, $3^2 + 4^2 = 5^2$.

10.6* Докажите, что уравнение $x^2 + y^2 = z^2$ имеет бесконечно много решений, в которых числа x, y, z не имеют общего делителя.

• Без последней оговорки можно было бы взять $x = 3n$, $y = 4n$, $z = 5n$.

▷ Заметим, что $n^2 + (2n+1) = (n+1)^2$, и для бесконечно многих n нечётное число $2n + 1$ будет точным квадратом (ведь нечётных точных квадратов бесконечно много). Числа n и $n+1$ очевидно не имеют общего делителя при всех n. ◁

Есть и другие способы получать пифагоровы тройки. Ещё Евклиду была известна формула

$$x = m^2 - n^2, y = 2mn, z = m^2 + n^2.$$

10.7* Проверьте, что эта формула при целых $m > n$ даёт пифагорову тройку.

▷ Пользуемся формулами квадрата разности и суммы:

$$(m^2 - n^2)^2 + (2mn)^2 = m^4 - 2m^2n^2 + n^4 + 4m^2n^2 = m^4 + 2m^2n^2 + n^4 = (m^2 + n^2)^2.$$

◁

Пифагоровы тройки соответствуют решениям уравнения $x^2 + y^2 = 1$ в рациональных числах, то есть точкам с рациональными координатами на окружности. (Если $x^2 + y^2 = z^2$ для целых x, y, z, то $(x/z)^2 + (y/z)^2 = 1$.) Все рациональные точки на окружности можно получить, проводя через точку $(-1, 0)$ прямую с рациональным наклоном k, имеющую уравнение $y = k(1 + x)$, и беря вторую точку её пересечения с окружностью $x^2 + y^2 = 1$. (Если вторая точка рациональна, то наклон рационален как отношение рациональных чисел. Наоборот, если наклон рационален и одна из точек пересечения рациональна, то по теореме Виета и вторая будет рациональной.) Продолжая это рассуждение, можно установить, что приведённая формула позволяет получить все пифагоровы тройки.

Диофантовы уравнения встречаются часто, и было бы замечательно иметь общий способ выяснять, есть ли решения у данного уравнения. У нас был такой способ для линейных уравнений вида $ax + by = c$, может быть, и для произвольных уравнений это можно? В начале XX века

Гильберт, перечисляя важнейшие (по его мнению) математические задачи, под номером 10 сформулировал такой вопрос: *дано диофантово уравнение с любым числом переменных и целыми коэффициентами, придумать способ узнать за конечное число шагов, имеет ли оно решение в целых числах.* После возникновения (в 1930-е годы) теории алгоритмов этот вопрос можно было понять так: придумать алгоритм (как сейчас сказали бы, программу для компьютера), который бы по любому диофантову уравнению за конечное время выяснял, есть у него решения или нет. В 1970 на этот вопрос был получен отрицательный ответ: Матиясевич, продолжая работы Девиса, Патнама и Робинсон, доказал, что такого алгоритма не существует. Что в каком-то смысле даже и хорошо: люди, изучающие конкретные классы диофантовых уравнений, могут не опасаться, что потом появится алгоритм, который «сделает их усилия бессмысленными и заменит их тупой компьютерной программой».

Для некоторых уравнений вопрос о разрешимости совсем простой.

10.8* Для каких значений c уравнение $x^2 - y^2 = c$ имеет решения?

▷ Уравнение можно переписать как $(x - y)(x + y) = c$. Легко понять, что $(x - y)$ и $(x + y)$ могут быть любыми целыми числами одинаковой чётности (оба чётные или оба нечётные), поэтому решение существует, если c нечётно или c делится на 4 (и не существует, когда c чётно, но на 4 не делится). ◁

Аналогичное уравнение с суммой квадратов сложнее, потому что $x^2 + y^2$ на множители не разлагается. Вернее, разлагается, но нужен квадратный корень из -1:

$$a^2 + b^2 = (a + b\sqrt{-1})(a - b\sqrt{-1})$$

Такого корня, конечно, нет среди обычных чисел (квадрат любого числа неотрицателен), но в алгебре (и логике) есть способ обходить эту трудность: понять, как надо было бы с этим несуществующим объектом действовать, если бы он существовал. Можно складывать и перемножать формальные записи вида $a + b\sqrt{-1}$ по обычным алгебраическим правилам, скажем,

$$(a + b\sqrt{-1})(c + d\sqrt{-1}) = (ac - bd) + (ad + bc)\sqrt{-1},$$

получается формальная запись того же вида. Или можно просто сказать, чтобы не смущать людей призраками, что мы просто вводим операции сложения и умножения на парах целых чисел, полагая

$$(a, b) + (c, d) = (a + c, b + d) \quad \text{и} \quad (a, b) \cdot (c, d) = (ac - bd, ad + bc),$$

и проверяем, что они обладают обычными алгебраическими свойствами. Такие пары называют *целыми гауссовыми числами*, их можно разлагать на множители и даже доказать единственность разложения (правильно определив простые гауссовы числа и единственность). Используя это (и свойства квадратичных вычетов), можно понять, когда $x^2+y^2 = c$ имеет решение: это бывает, если *в разложении c на простые множители все множители вида $4k+3$ входят в чётной степени*.

Ключевым шагом тут является случай нечётного простого c: ещё в XVII веке Жирар и Ферма сформулировали ответ: уравнение $x^2 + y^2 = p$ имеет решение, когда простое число p имеет вид $4k + 1$. То, что при $p = 4k + 3$ решений нет, очевидно по модулю 4, но существование решений для $p = 4k + 1$ доказать не так просто, и были придуманы самые разные доказательства (Эйлер, Лагранж, Дедекинд и многие другие); короткое, элементарное и загадочное доказательство придумал Цагир в 1990.[3]

10.9* Используя целые гауссовы числа, покажите, что если два числа представимы в виде суммы двух квадратов, то представимо и их произведение.

▷ Если $m = a^2 + b^2$ и $n = c^2 + d^2$, то можно написать

$$m = (a + bi)(a - bi), \quad n = (c + di)(c - di)$$

(мы пишем i вместо $\sqrt{-1}$ для краткости), и поэтому

$$mn = (a + bi)(c + di)(a - bi)(c - di) = (s + ti)(s - ti) = s^2 + t^2,$$

где

$$(s + ti) = (a + bi)(c + di), \text{ то есть } s = (ac - bd),\ t = (ad + bc)^2.$$

Законность операций с мнимыми числами, конечно, надо обосновывать, но можно и просто проверить тождество

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

(Диофант, доказавший это тождество в III веке новой эры, ни про какие комплексные числа, естественно, не знал.) ◁

Можно спросить также, какие целые числа представимы в виде суммы *трёх* квадратов (те, которые не имеют вида $4^k(8l+7)$, теорема Лежандра) и в виде суммы *четырёх* квадратов (все). Последнее утверждение доказал Лагранж; он же установил, что уравнение $x^2 - Dy^2 = 1$ (которое

[3] Замечательное геометрическое представление этого доказательства предложил Александр Спивак, см. `http://mmmf.msu.ru/lect/spivak/summa_sq.pdf`.

по некоторому недоразумению назвают *уравнением Пелля*) имеет бесконечно много решений при любом D, не являющемся точным квадратом. (Если D — точный квадрат, то получается разность двух квадратов, и есть только тривиальное решение $x = 1$, $y = 0$.)

Разные открытые проблемы

Возвращаясь к исходному замечанию о том, как много в теории чисел простых вопросов с неизвестными ответами, приведём ещё три таких вопроса.

Совершенные числа

Целое положительное число называют *совершенным*, если оно равно сумме всех целых положительных делителей, не считая самого себя. Первые два таких числа $6 = 1 + 2 + 3$ и $28 = 1 + 2 + 4 + 7 + 14$, и известно ещё несколько десятков совершенных чисел. Но никто не знает, бесконечно ли их много, а также бывают ли нечётные совершенные числа.

Гипотеза Коллатца

Начнём с некоторого целого положительного числа n и будем многократно преобразовывать его по одному и тому же правилу: если чётно, делим на 2, если нечётно, умножаем на 3 и прибавляем единицу. Скажем,

$$3 \to 10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1 \to 4 \to 2 \to 1 \to \ldots$$

Гипотеза Коллатца утверждает, что мы всегда придём к циклу $1 \to 4 \to 2 \to 1 \to \ldots$, с какого бы числа мы не начали.

Нормальные числа

В десятичном разложении

$$\sqrt{2} = 1{,}41421356237309504880168872420969807856967187537694807 3\ldots$$

не видно никакой явной закономерности в десятичных знаках и можно предположить, что в этой последовательности встречаются все комбинации цифр, и даже в пределе одинаково часто (такие числа Борель назвал *нормальными*). Но никто не знает, так ли это.

11. Послесловие

Есть много сборников задач математических классов (и ещё больше сборников задач олимпиад) — какой смысл ещё одного и чем он отличается (по замыслу составителей) от имеющихся?

Часто сборники задач представляют собой подборку задач («листков»), дававшиеся в каком-то математическом классе[4], обычно без решений (потому что решения рассказывали школьники, и для раздачи их не готовили) и объяснений (которые, если это бывало нужно, делались на занятиях устно). Если использовать сборник задач для самостоятельных занятий (или для преподавания в другом классе), то полезно иметь больше задач разной трудности (и, в частности, больше простых — но не повторяющихся, как это часто бывает в задачниках — задач).

Сборники задач олимпиад (и «для подготовки к олимпиадам») отражают ограничения, связанные с подбором олимпиадных задач — поскольку считается, что они должны быть «в пределах школьной программы»[5], вместо естественных и важных понятий (будь то комплексные числа, сходимость и пределы или линейные пространства) изучаются всякие олимпиадные хитрости: подготовка к соревнованиям по фигурной гимнастике — не то же самое, что прогулки на природе. Кроме того, как и в задачах математических кружков, там обычно не предполагается систематического изложения (скорее авторы стараются, чтобы разные разделы были более или менее независимы).

В качестве образца жанра мы ориентировались на брошюры, возникшие из заданий ВЗМШ[6] («Функции и графики», «Метод координат», «Прямые и кривые», «Пределы» — задания Н. Б Васильева и В. Л. Гутенмахера про целые числа и по комбинаторике так и не были, видимо, изданы, но некоторые их варианты есть в сети `https://sites.google.com/site/vaguten/home/russkaa-vzms`). К сожалению, в них обсужда-

[4]Традиция такого преподавания в математических классах, когда раздаются задачи и несколько преподавателей обсуждают со школьниками их решения, убеждаясь, что школьник решил правильно и при необходимости помогая, была заложена Н. Н. Константиновым в начале 1960-х годов. Составители имели возможность работать в этой традиции и с благодарностью вспоминают Н.Н.

[5]При всём цинизме таких деклараций — ведь олимпиады при всей своей полезности уже давно стали «профессиональным спортом» и для читавших только школьный учебник и решавших задачи из школьного задачника они вряд ли посильны.

[6]Всесоюзная заочная математическая школа, основанная И. М. Гельфандом в середине 1960-х годов.

ется лишь небольшая часть того, что стоило бы изучать человеку, который заинтересовался математикой.

Для задач из нашего сборника вопрос об авторе, как правило, не имеет смысла (и даже если имеет, то в большинстве случаев узнать первоисточник нельзя) — но, разумеется, составители не претендуют на «авторство».