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*.

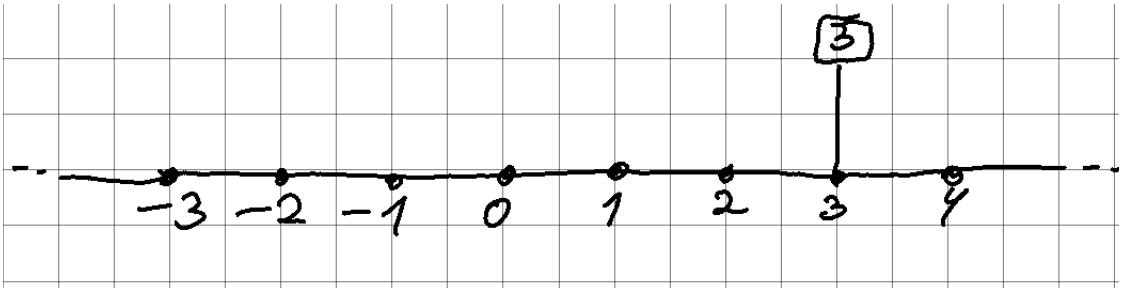
- Можно сказать так: в мешке чётное число n яблок, если их можно поделить поровну (для педантов: не разрезая яблок; величина яблока не учитывается, важно только их количество) между двумя людьми. Или так: если можно разложить яблоки парами. Эти два способа соответствуют умножению m на 2 (две группы по 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?

1.2 Будет ли нуль чётным числом, согласно нашему определению?

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)?

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

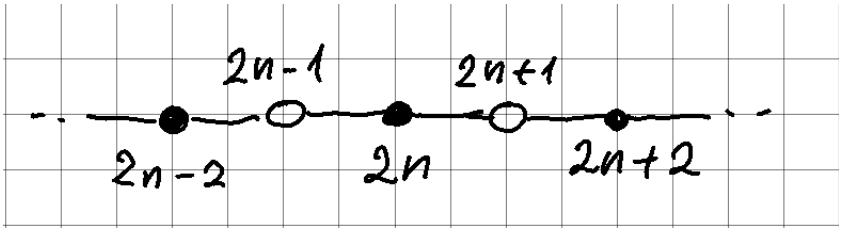


1.4 Отметьте чётные и нечётные числа на этом рисунке.

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?

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

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?

1.8 Всегда ли будет чётной сумма двух чётных чисел?

1.9 Докажите, что разность двух чётных чисел чётна.

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

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?

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.)

×	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?

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?

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?

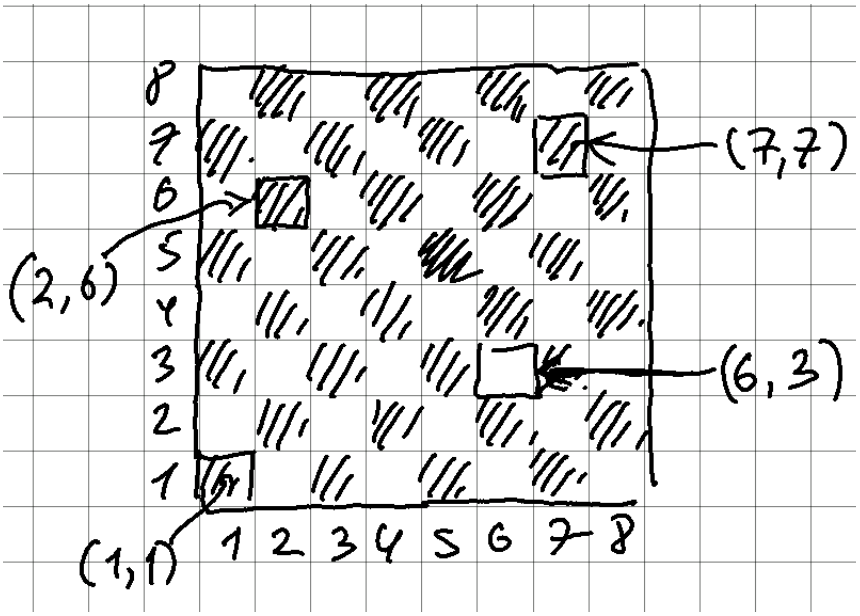
1.16* *Точным квадратом* называют квадрат целого числа (0, 1, 4, 9, 16,...). Может ли точный квадрат быть чётным, но не делиться нацело на 4?

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)

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.)



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

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,..., $A_{12}A_{13}$, $A_{13}A_1$.

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

• 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 $\langle\ldots\rangle$, то она чётна, и (2) если сумма чётна, то в ней чётное число $\langle\ldots\rangle$.

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

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.

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?

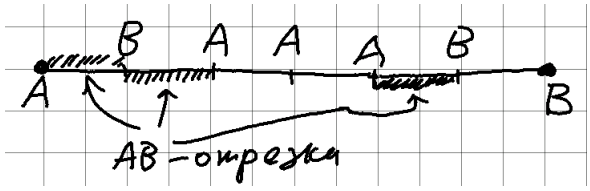
1.25* Чтобы узнать, чётно ли целое положительное число, достаточно посмотреть на его последнюю цифру. Почему?

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

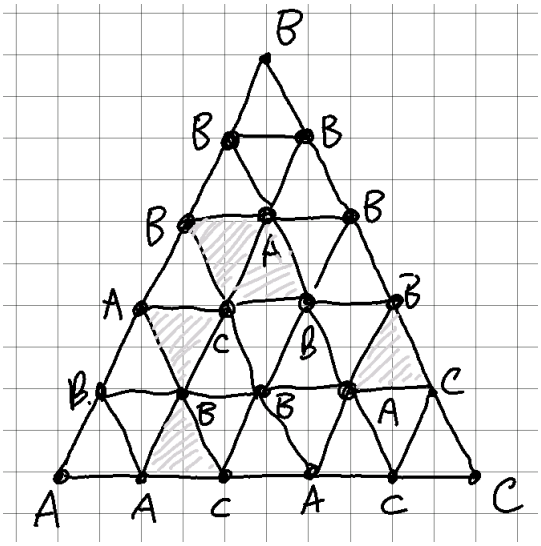
1.27* Запишем степени двойки (1, 2, 4, 8, 16, 32, ...) и степени тройки (1, 3, 9, 27, 81, ...). Может ли в этих двух последовательностях чисел встретиться какое-то общее число, кроме 1?

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

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.



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.



• 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*).

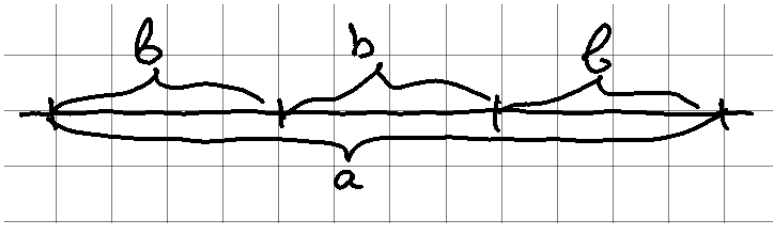
2. Делимость

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.

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

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?

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?

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?

• 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.

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?

• 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.

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?

• 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.

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 $a + b$.

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?

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?

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 $a^n - b^n$.

• 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.

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

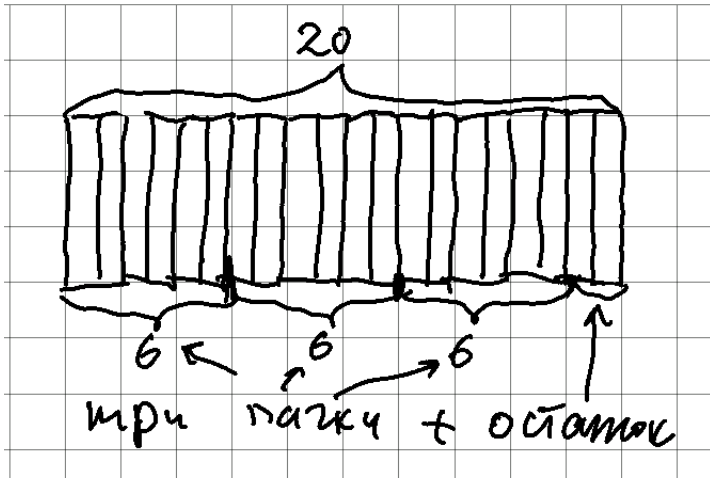
2.17* Имеется n различных целых положительных чисел. Докажите, что любое целое положительное число, которое делится на все эти числа, хотя бы в n раз больше наименьшего из них.

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

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

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.)

- Раньше в школах учили делить «уголком»:

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

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.

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

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

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?

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

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).

• 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 $3x$?

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

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?

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

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?

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.)

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)?

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?

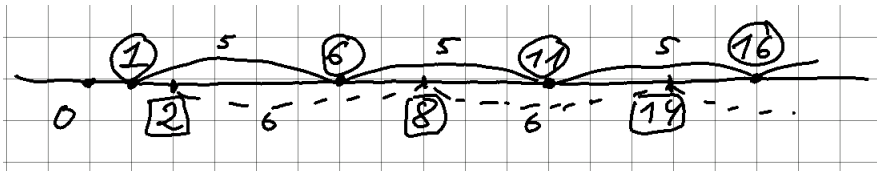
3.17* Останется ли утверждение предыдущей задачи верным, если второе условие записать как $0 < r \leqslant b$?

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

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?

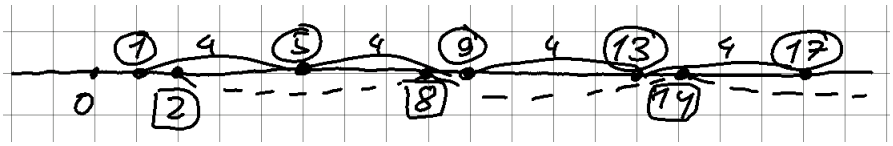
• Вообще взятие остатка по модулю k — это, если можно так выразиться, наматывание числовой оси на окружность длины k.

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)?



• 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)?



• 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)?

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.)

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.)

• 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

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

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

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 $a \equiv c \pmod n$.

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 $ac \equiv bd \pmod n$.

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 $a/c = b/d \pmod n$?

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

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

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).

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

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

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 $a \equiv b \pmod{c}$?

• 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].)

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.)

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.)

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?

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

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.)

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.)

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 $\sqrt{3}$. ◁

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?

▷ 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 $(-3) \cdot (-1)$.

• 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.)

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?

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

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

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

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

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

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

• 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.

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

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.

• 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.)

▷ 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.

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?

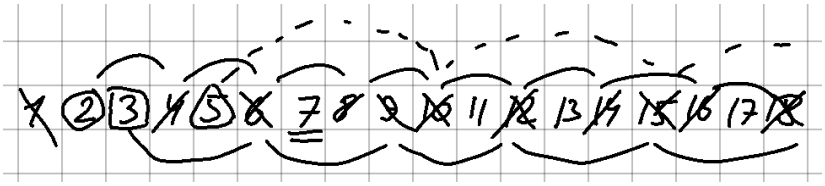
5.16 Дано положительное целое число n (можно взять, скажем, 1000). (а) Докажите, что есть число, которое делится на все числа от 2 до n. (б) Докажите, что есть число, большее 1, которое даёт остаток 1 при делении на все числа от 2 до n. (в) Докажите, что есть число, большее 1, которое не делится ни на одно из чисел от 2 до n.

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».

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

Как составить таблицу простых чисел? Можно написать все числа $1, 2, 3, 4, 5, 6, \ldots$ 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?

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).

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 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?

• 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 НОД$(a, b) = 1$.

6.2 С какими числами взаимно просто простое число p?

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

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

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.]

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

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

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

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

6.9 Найдите НОД$(123456789, 987654321)$.

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:

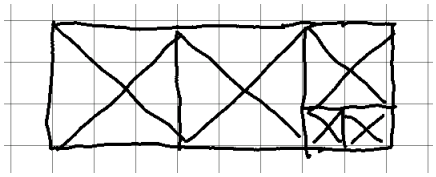
$$\text{НОД}(2, 1) = \text{НОД}(2 \bmod 1, 1) = \text{НОД}(0, 1) = 1.$$

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).

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.

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

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

(и сравните с предыдущей задачей).

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).

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 $a, b, c \neq 0$.

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.

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)?

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

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

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

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?

• 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?

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.

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?

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.) ◁

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

• 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.

• 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 $\text{НОД}(15, 8) = 1$.

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 $\text{НОД}(a, b)$.

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

• 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.

• 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 $\text{НОД}(a, b)$.

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.)

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

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 $ax \equiv 1 \pmod{p}$).

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.

• 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*

7.14 Найдите обратное к числу 23 по модулю 89.

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

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?

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?

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.)

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.

• 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.

• В этой главе мы извлекали следствия из такого факта (который, в свою очередь, получается как результат алгоритма Евклида): уравнение $ax + by = \text{НОД}(a, b)$ 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.

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

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

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

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.

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

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

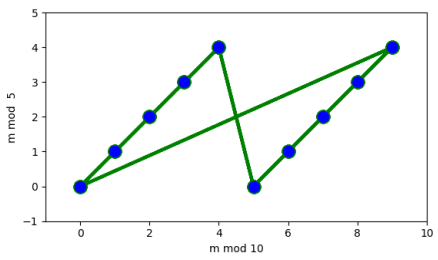
имеет решение x, и притом это x ровно одно по модулю $b_1 \cdot \ldots \cdot b_n$.

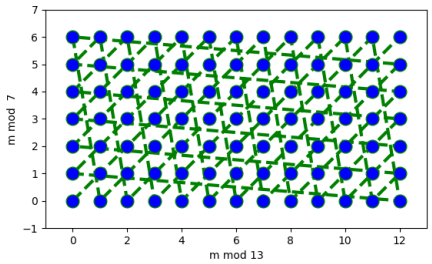
7.28* Иногда шахматную доску «сворачивают в тор»: если фигура выходит за границу, то её возвращают с другой стороны (сдвигая по горизонтали на ширину доски и/или по вертикали на высоту доски).

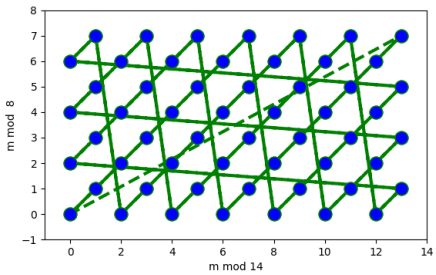
Докажите, что на свёрнутой в тор доске $a \times b$ со взаимно простыми a и b шахматный король, который начинает с какой-то клетки и всё время идёт вправо-вверх по диагонали, побывает во всех клетках по разу и вернётся в исходную клетку.

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

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 $(x \bmod a, x \bmod b)$?

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.

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)?

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.)

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.

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.

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.

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?

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

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

8.8* Найдите наименьшее число, имеющее ровно 18 делителей.

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

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.

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

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

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?

• 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.)

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

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

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

• 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?

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: $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.

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.

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.

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).

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 $n!$).

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.

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 $4620 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$.

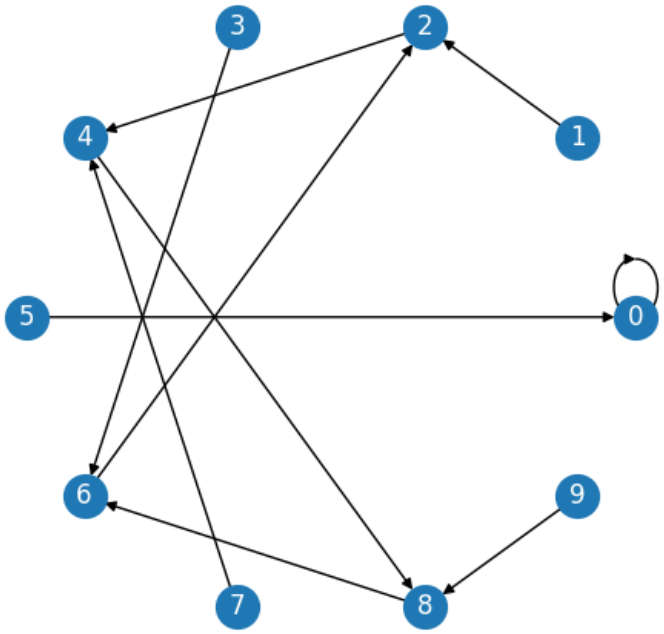
• Указанное в этой задаче свойство функций σ и τ иногда называют *мультипликативностью*. Оно останется верным, если мы рассмотрим сумму любых степеней делителей, скажем, сумму их квадратов. (Для степени 0 получается τ, для степени 1 получается σ.)

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).

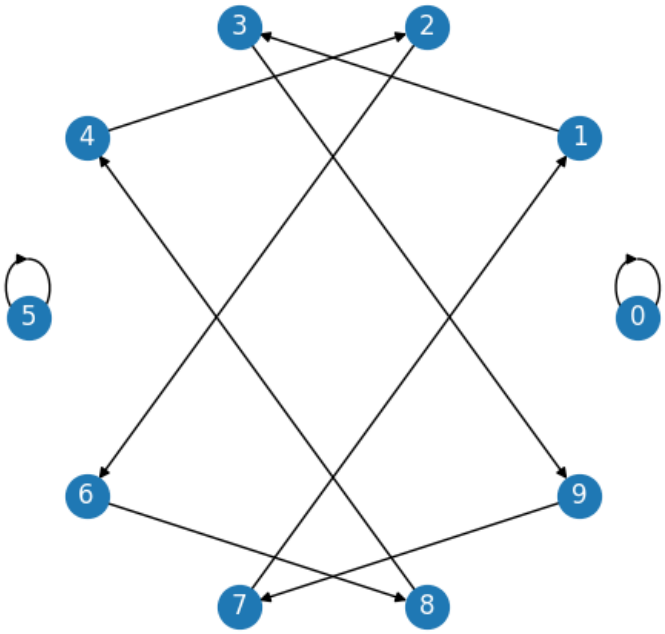
9. Малая теорема Ферма

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.



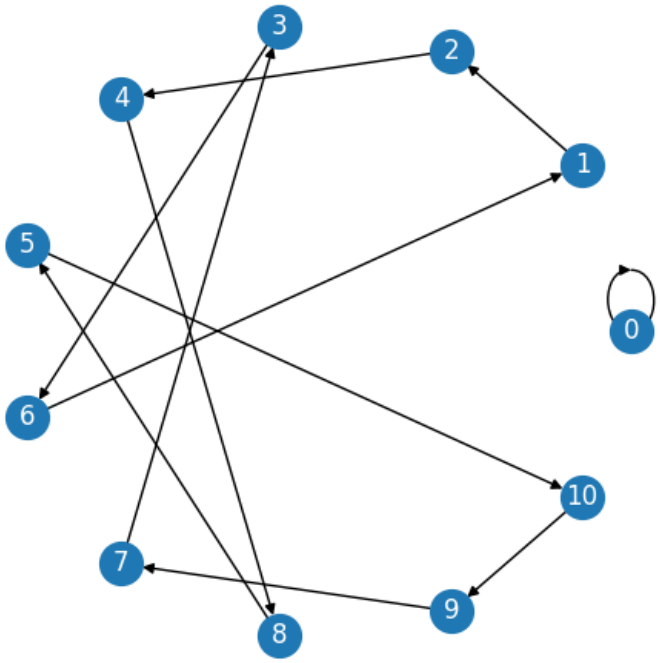
На этой схеме из каждого остатка по модулю 10 идёт стрелка, соответствующая умножению его на 2 (по модулю 10)

9.1 Найдите на этой картинке упомянутый цикл.



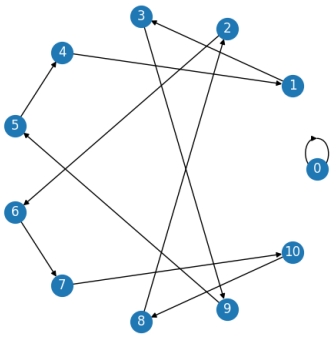
9.2 Сколько циклов и какой длины есть в графе умножения остатков по модулю 10 на 3 на рисунке? Как будут меняться последние цифры степеней тройки?

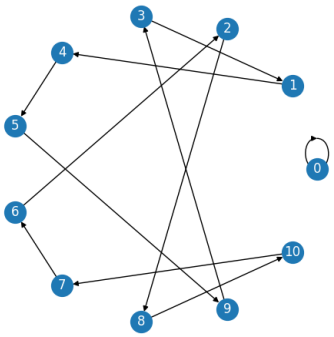
Мы уже обсуждали, что простые модули ведут себя более регулярно (все остатки, кроме нуля, обратимы, можно сокращать и т.п.). Вот один из графов умножения для простого модуля 11.

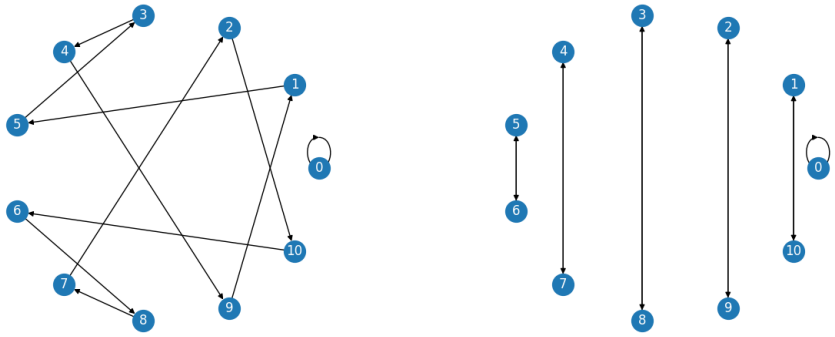


9.3 На что мы умножаем на этом рисунке? Какой будет период в последовательности остатков? Найдите $2^{179} \bmod 11$, глядя на эту картинку.

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?

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.

9.6 Покажите, что стрелки разбиваются на несколько циклов.

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

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?

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)

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 $x^{p-1} \equiv 1 \pmod{p}$.

▷ 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.

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.

▷ 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.

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.

▷ 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.

• 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.

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?

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.

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

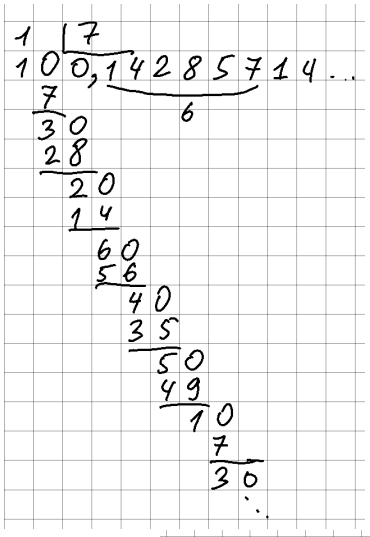
9.19* Докажите, что функция Эйлера мультипликативна: если m и n взаимно просты, то $\varphi(mn) = \varphi(m)\varphi(n)$.

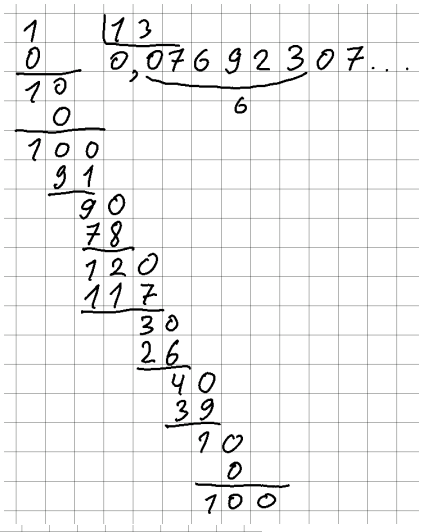
Это рассуждение годится при $m, n > 1$. Вообще $\varphi(1)$ это некоторый особый случай, и мы положим $\varphi(1) = 1$ — для того, в частности, чтобы предыдущая задача была верна при всех m, n, включая 1.

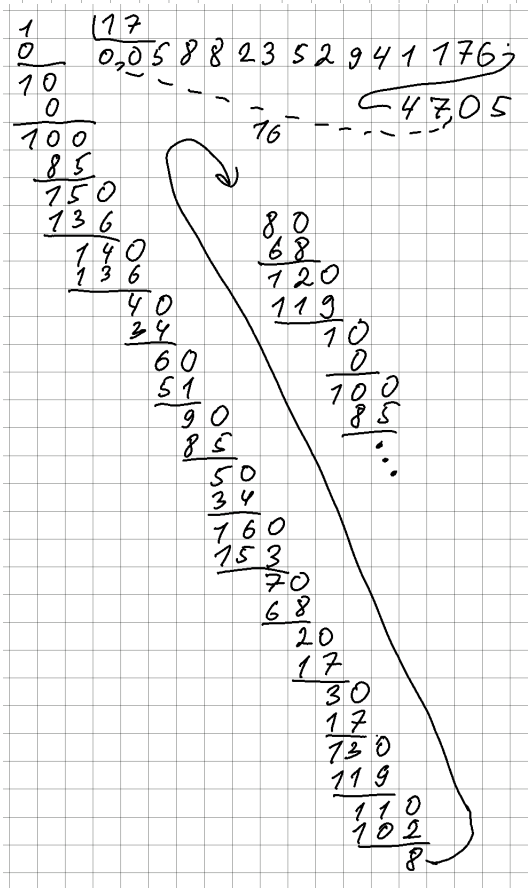
9.20* Покажите, что для любого числа $n > 2$ выполняется тождество $\sum_{d|n} \varphi(d) = n$ (где сумма берётся по всем делителям числа n).

• 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.

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).

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

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}=\frac{2\cdot3\cdot4+1\cdot3\cdot4+1\cdot2\cdot4+1\cdot2\cdot3}{1\cdot2\cdot3\cdot4}=\frac{24+12+8+6}{24}=\frac{50}{24}=\frac{25}{12},$$

и 25 делится на 5.

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 $4k+3$).

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 опровернута (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

$$\left| \frac{m}{n} - \alpha \right| < \frac{1}{nN}.$$

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

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \cfrac{1}{\dots}}}}}$$

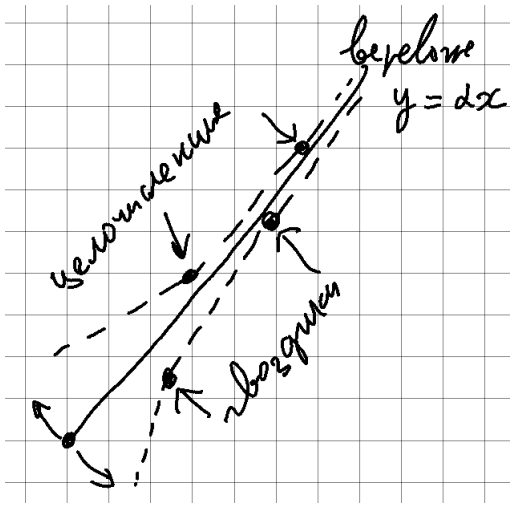
Для этого мы выделяем из $\pi = 3{,}1415926\ldots$ целую часть 3, остаётся число $0{,}1415926\ldots$, меньшее 1, из обратного к нему $1/(\pi - 3) = 7{,}06251\ldots$ выделяем целую часть 7, из обратного к остатку $1/0{,}06251\ldots = 15.9965\ldots$ выделяем целую часть 15, и так далее.

Затем, обрывая эту цепную дробь на конечном шаге, можно получать приближения

$$3 + \frac{1}{7} = \frac{22}{7}, \quad 3 + \cfrac{1}{7 + \cfrac{1}{15}} = \frac{333}{106}, \quad 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1}}} = \frac{355}{113}, \ldots$$

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.

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).



[2] К тому же 355/113 легко запомнить: надо написать 113355 и разбить посередине на числитель и знаменатель.

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:

$$\left|\sqrt{2} - \frac{m}{n}\right| \geqslant \frac{1}{4n^2}$$

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 $m^2 - 2n^2 = 1$.

• 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 $x^{(p-1)/2} \equiv 1 \pmod{p}$.

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 кри-

терия $x^{(p-1)/2} \equiv 1 \pmod{p}$ 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 $x = 3n$, $y = 4n$, $z = 5n$.

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.

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?

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]

[3]Замечательное геометрическое представление этого доказательства предложил Александр Спивак, см. `http://mmmf.msu.ru/lect/spivak/summa_sq.pdf`.

10.9* Используя целые гауссовы числа, покажите, что если два числа представимы в виде суммы двух квадратов, то представимо и их произведение.

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 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».