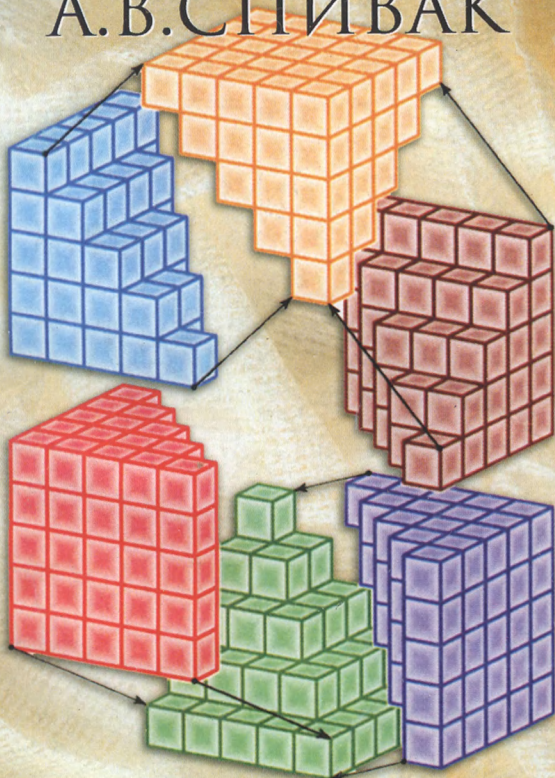


ВЫПУСК

102 Библиотека КВАНТ



А.В.СПИВАК



АРИФМЕТИКА

Б Ю Р О



КВАНТУМ



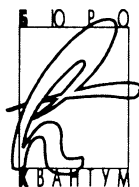
БИБЛИОТЕЧКА
КВАНТ
ВЫПУСК

102

Приложение к журналу
«Квант» № 4/2007

А.В.СПИВАК

АРИФМЕТИКА



Москва
2007

УДК 511.3(082)
ББК 22.130
С72

Серия
«Библиотечка «Квант»
основана в 1980 г.

РЕДАКЦИОННАЯ КОЛЛЕГИЯ:

Б.М.Болотовский, А.А.Варламов, В.Л.Гинзбург,
Г.С.Голицын, Ю.В.Гуляев, М.И.Каганов, С.С.Кротов,
С.П.Новиков, Ю.А.Осипьян (председатель),
В.В.Произволов, Н.Х.Розов, А.Л.Стасенко, В.Г.Сурдин,
В.М.Тихомиров, А.Р.Хохлов,
А.И.Черноуцан (ученый секретарь)

С72 Спивак А.В.

Арифметика. – М.: Бюро Квантум, 2007. – 160 с. (Библиотечка «Квант». Вып. 102. Приложение к журналу «Квант» № 4/2007.)

ISBN 5-85843-067-8

Книга по элементарной теории чисел состоит из статей, многие из которых были опубликованы в журнале «Квант». Алгоритм Евклида, основная теорема арифметики, ряды Фарея, периодические дроби, числа Фибоначчи, малая теорема Ферма, цепные дроби, квадратичный закон взаимности изучены весьма подробно, с большим количеством примеров и упражнений.

Может служить учебным пособием для математических классов и кружков. Адресована школьникам 7–11 классов, учителям, а также всем любителям математики.

ББК 22.130

ISBN 5–85843–067–8

© Бюро Квантум, 2007

СОДЕРЖАНИЕ

Предисловие	4
Индукция	5
Арбузная пошлина	18
Алгоритм Евклида	22
Основная теорема арифметики	35
Ряды Фарея	38
Периодические дроби	41
Малая теорема Ферма	54
Часть I. Примеры и три доказательства	54
Часть II. Функции Эйлера	63
Часть III. Длины периодов	75
Часть IV. Первообразные корни	87
Часть V. Функция и числа Кармайкла	93
Числа Фибоначчи	99
Цепные дроби	111
Квадратичный закон взаимности	130
Ответы, указания, решения	138

ПРЕДИСЛОВИЕ

В книгу вошли некоторые статьи журнала «Квант» и энциклопедии «Числа и фигуры» издательства «Росмэн». Столь глубоких, подробных и доступных школьнику изложений многих важных разделов арифметики до сих пор не было: речь пойдет о малой теореме Ферма, числах Фибоначчи, квадратичном законе взаимности.

Конечно, эти статьи не только не исчерпывают содержание современной науки о натуральных числах, но даже не дают представления о многих важнейших ее задачах и методах: за пределами этой книги остались как темы, которые невозможно изложить элементарно (а таких в арифметике, как и в любом другом разделе математики, абсолютное большинство), так и некоторые интересные задачи и теоремы, доступные школьнику. Невозможно в небольшой книге изложить все секреты царицы математики (так называл арифметику К.Ф.Гаусс) – хотя бы потому, что многие из этих секретов еще только предстоит открыть (математика в последние 400 лет развивается в высшей степени бурно!).

Каждая статья посвящена отдельной важной теме. Начинается изложение обычно с довольно простых вопросов, доступных семикласснику, а заканчивается довольно трудными – иной раз даже изысканными – темами. Поэтому эту книгу большинство школьников будут читать многократно, каждый раз продвигаясь дальше и дальше. Упражнений в книге очень много; скорее всего, при первом чтении удастся справиться лишь с небольшой долей упражнений: например, статьи «Периодические дроби» и «Малая теорема Ферма» – это целый мир, к которому надо очень долго привыкать!

Перед (или одновременно с) изучением последних двух статей сборника («Цепные дроби» и «Квадратичный закон взаимности») полезно изучить статьи «Уравнения Пелля» и «Суммы квадратов», опубликованные в журнале «Квант» (эти статьи войдут в один из следующих выпусков «Библиотечки»).

Автор статьи «Арбузная пошлина» – А.Котова, статьи «Малая теорема Ферма» – В.Сендеров и А. Спивак, остальных статей – А.Спивак. Многие упражнения заимствованы из «Задачника «Кванта»». По традиции журнала, номера таких задач отмечены буквой М.

*Выпросился остаться одну ночку; от одной
ночки две ночи, от двух ночек две недели, от
двух месяцев два года, а от двух годов жил
тридцать лет.*

Народная присказка

*Капитан Джонатан
Переплыл океан –
И в пути пеликана
Поймал капитан.*

*Пеликан Джонатана
Снес яйцо – и неожиданно
Стало у капитана
Целых два пеликана.*

*И второй пеликан
Снес яйцо, как ни странно:
Стало у Джонатана
Целых три пеликана.*

*Будет род пеликана
Прибывать беспрестанно,
Если только омет
Не спасет капитана!*

Робер Деснос (1900–1945),
французский поэт

Рассказ об индукции начну с анекдота.

— Взгляни на этого математика, — сказал логик. — Он замечает, что первые 99 чисел меньше сотни, и отсюда с помощью того, что он называет индукцией, заключает, что любые числа меньше сотни.

— Физик верит, — сказал математик, — что 60 делится на все числа. Он замечает, что 60 делится на 1, 2, 3, 4, 5 и 6. Он проверяет несколько других чисел, например, 10, 20 и 30, взятых, как он говорит, наугад. Так как 60 делится на них, он считает экспериментальные данные достаточными.

— Да, но взгляни на инженера, — возразил физик. — Он подозревает, что все нечетные числа простые. Во всяком случае, 1 можно рассматривать как простое число, доказывает он. Затем

идут 3, 5 и 7 – все, несомненно, простые. Затем идет 9 – досадный случай; по-видимому, 9 не является простым числом, но 11 и 13, конечно, простые. Возвращаясь к 9, говорит он, заключаем, что 9 должно быть ошибкой эксперимента.

Индукция – один из важнейших способов рассуждения, применяемых в математике. Суть этого метода в том, что для доказательства некоторого утверждения A_n , где $n = 1, 2, 3, \dots$, сначала доказывают его для $n = 1$ (соответствующее утверждение называют базой индукции), а затем для каждого натурального n в предположении, что A_n истинно, доказывают истинность утверждения A_{n+1} (индукционный переход).

Ввел термин «математическая индукция» в 1838 году Огёст де Морган (1806–1871) – сын полковника английских войск в Индии, первый президент Лондонского королевского математического общества (основанного в 1865 г.), один из создателей математической логики. (Его имя носят формулы $A \cup B = \overline{A \cap B}$ и $\overline{A \cap B} = \overline{A} \cup \overline{B}$, где черта обозначает переход от множества к его дополнению.)

Быстроим в ряд костяшки домино. Толкнем первую – она, падая, повалит вторую, та – третью, и так далее. Представьте, что доминошки изображают утверждения $A_1, A_2, A_3, \dots, A_{100}, A_{101}, \dots$, а падение доминошки означает доказательство соответствующего утверждения. Тогда «толкнуть первую доминошку» – значит доказать, что утверждение A_1 истинно; а то, что каждая доминошка, падая, валит следующую, означает, что при любом k из утверждения A_k следует A_{k+1} . Цепь доказательств, начавшись с первого утверждения, прокатится по всему ряду: она дойдет и до сотого, и до тысячного, и вообще до любого натурального числа.

Рассмотрим несколько примеров. Придумаем 10 различных натуральных чисел, сумма которых кратна каждому из них. В задаче нет параметра n , поэтому поставим более общую задачу: для любого натурального числа $n > 2$ придумаем n различных натуральных чисел, сумма которых кратна каждому из них.

Для $n = 3$ годятся числа 1, 2 и 3: их сумма равна 6 и кратна любому из них. Это **база** индукции – утверждение, с которого начинается цепь рассуждений.

Теперь выполним **индукционный переход**: научимся от ряда из n чисел переходить к $n + 1$ числам. Если сумма $a_1 + a_2 + \dots + a_n$ кратна любому из слагаемых, то можно добавить к числам a_1, a_2, \dots, a_n их сумму $a_1 + a_2 + \dots + a_n$. Таким образом из трех чисел 1, 2, 3 получим четыре числа 1, 2, 3, 6, а из них – пять чисел 1, 2, 3, 6, 12. Так можно действовать и дальше, увеличивая и

увеличивая количество чисел. В частности, для $n = 10$ получим: 1, 2, 3, 6, 12, 24, 48, 96, 192, 384.

Разумеется, нельзя утверждать, что найденный пример единственный: например, отпавляясь от равенства

$$\frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{24} + \frac{1}{120} = 1,$$

находим шесть чисел 40, 30, 24, 20, 5 и 1, сумма которых равна 120 и кратна любому из них. Известным уже способом из этих шести чисел можно получить десять, добавив числа 120, 240, 480 и 960.

Следующий пример – задача о разделе добычи. Вообразите, что три пирата захватили корабль с разнообразнейшим добром. Каждый уверен, что он бы поделил добычу на равные части, но остальные ему не доверяют. Если бы пиратов было двое, то выйти из положения было бы легко: один делит добычу на две части, а другой берет ту, которая ему кажется большей. Сможете организовать раздел добычи, чтобы ни один из троих пиратов не чувствовал себя обделенным? Учтите: добыча настолько разнородна и вкусы пиратов настолько несхожи, что объективного способа сравнения отдельных частей не существует!

Пусть первый пират разделит добычу на три, по его мнению, равные части, а второй и третий укажут те части, которые им кажутся большими. Если они укажут на разные части, то каждый берет ту часть, которую он считает большей, а первый берет оставшуюся (ему все равно!).

Если же они укажут на одну часть, пусть поделят ее между собой. Затем второго и третьего попросим указать на ту из оставшихся частей, которая кажется большей. Если они покажут на одну и ту же часть, то вновь делят ее между собой, а первый берет оставшуюся часть. Если же они укажут на разные части, пусть каждый из них делит понравившуюся часть с первым пиратом. Все честно!

А если пиратов не 3, а больше? Нам поможет индукция. Предположим, что n пиратов придумали способ справедливого раздела добычи. Пусть их стало на одного больше. Разделим всю добычу между n пиратами и затем предложим каждому из них разделить свою долю на $n + 1$ равных частей (по его мнению, равных). Пусть теперь $(n + 1)$ -й пират возьмет у каждого из них по одной части. У каждого из n пиратов останется, по его мнению, $n / (n + 1)$ его прежней доли; прежняя доля составляла, по его мнению, не менее $1/n$ всей добычи; $\frac{n}{n+1} \cdot \frac{1}{n} = \frac{1}{n+1}$.

Не сможет жаловаться и $(n + 1)$ -й пират, так как он взял у каждого из своих товарищей не менее $1/(n + 1)$ доли (по его мнению). Вообразите, как это выглядит для 15 пиратов. Придется делить все на 14 персон, а перед этим – на 13, на 12, ... , начать же придется с удивительного для непривычных к высокой абстракции злобных пиратов раздела на двоих! Если вам дадут довести эту процедуру до конца – все (но только в самый последний момент!) станут довольны.

Менее опасен для вас другой способ. Усадите пиратов вокруг круглого стола и предложите первому взять долю добычи. Пусть второй, если ему кажется, что первый взял слишком много, уменьшит ее до справедливой. (Если второй считает, что первый взял не больше положенного, пусть он ничего не трогает.) Затем пусть то же сделает третий, четвертый и так далее. Возьмет эту долю (полностью выходя из дележа) пират, последним ее коснувшийся. Именно *последний коснувшийся*: это правило не позволяет пиратам обманывать друг друга.

Можно было обойтись и без круглого стола: разложив всю добычу в узкую длинную ленту, медленно нести вдоль нее, от начала к концу, острый-преострый нож. Как только нож отделит от добычи, по мнению какого-то пирата, $1/n$ часть, этот пират должен закричать и взять эту часть себе. (Если одновременно закричали несколько пиратов – пусть эту часть возьмет кто-то один из них; кто именно – не имеет значения.) Очевидно, никто не сможет утверждать, что взявшему свою долю пирату досталось слишком много: надо было вовремя кричать!

Следующий пример. Пусть на кольцевой дороге стоят несколько одинаковых автомашин; если бы весь бензин из их баков слили в одну, то она смогла бы проехать по всей кольцевой дороге. Докажем, что хотя бы одна из этих машин может объехать все кольцо по часовой стрелке, забирая по пути бензин у остальных машин.

База – случай 1 машины – тривиальна. Предположим, что утверждение верно для n машин. Рассмотрим случай $n + 1$ машины. Хотя бы у одной из них (пусть это машина A) бензина хватит, чтобы доехать до ближайшей (по часовой стрелке!) машины: иначе суммарное количество бензина было бы явно недостаточно. Уберем на обочину машину, до которой может доехать A , а весь бензин из нее перельем в A . Общее количество бензина не изменилось, а число машин уменьшилось. По предположению индукции, хотя бы одна машина может объехать кольцо по часовой стрелке, забирая по пути бензин у остальных

машин. Эта же машина может, очевидно, объехать кольцо и в начальной ситуации.

Упражнения

1. Сумма первых n нечетных чисел равна n^2 (На рисунке 1 это равенство проиллюстрировано для $n = 5$.) Докажите это по индукции.

2. Нетрудно проверить, что 2 делится на 2^1 , 3 4 делится на 2^2 , 4 5 6 – на 2^3 , 2^2 , 5 6 7 8 – на 2^4 , а 6 7 8 9 10 – на 2^5 . Сформулируйте и докажите общее утверждение.

3. Двухзначное число 12 делится на 4, трехзначное число 112 – на 8, четырехзначное число 2112 – на 16. Вообще, для любого натурального числа n существует составленное из цифр 1 и 2 число, делящееся на 2^n . Докажите это.

4. Любую дробь m/n , где m, n – натуральные числа, $1 < m < n$, можно представить в виде суммы нескольких дробей вида $1/q$ таких, что знаменатель каждой следующей дроби делится на знаменатель предыдущей. Докажите это. (Например, $\frac{3}{43} = \frac{1}{15} + \frac{1}{330} + \frac{1}{14190}$.)

5. Квадрат нельзя разрезать на n квадратов тогда и только тогда, когда $n = 2, 3$ или 5 . Докажите это.

Не всегда переход следует осуществлять от n к $n + 1$. Иногда приходится использовать другие формы индукции. Например, докажем, что число $n!$ при любом натуральном n представимо в виде произведения двух натуральных чисел, различающихся не более чем вдвое. **База** – два равенства: $1! = 1 \cdot 1$ и $2! = 1 \cdot 2$.

Индукционный переход проведем не от n к $n + 1$, а от n к $n + 2$. Пусть $n! = ab$, где a, b – натуральные числа, $1 \leq a \leq b \leq 2a$.

Тогда $(n + 2)! = a(n + 2) \cdot b(n + 1)$, при-

чем $\frac{a}{b} \cdot \frac{n+2}{n+1} < 1 \cdot 2 = 2$ и $\frac{b}{a} \cdot \frac{n+1}{n+2} < 2 \cdot 1 = 2$.

Выясним, на какое наибольшее число частей могут разделить плоскость 15 прямых. Нарисовать 15 прямых нетрудно (рис.2). А вот разобраться, сколько там частей, вовсе не легко: некоторые прямые пересекаются за пределами чертежа, а мелкие части почти

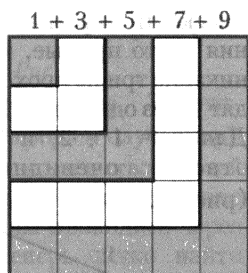


Рис.1

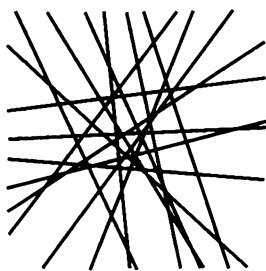


Рис.2

неразличимы. Можно, конечно, выйти на стадион с 15 веревками и провести «исследование на местности», но вдруг веревки запутаются? И куда мы пойдём, если вместо 15 прямых будет 150?

Лучше решим задачу Я. Штейнера об n прямых – найдем формулу для количества $f(n)$ частей, на которые разбивают плоскость n прямых общего положения (прямые общего положения – это прямые, никакие две из которых не параллельны и никакие три не проходят через одну точку).

Для $n = 1, 2$, и 3 ответы очевидны (рис.3–5): $f(1) = 2$,

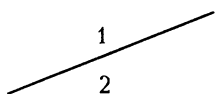


Рис. 3

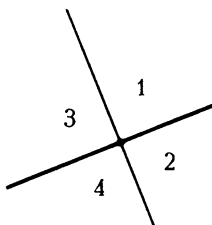


Рис. 4

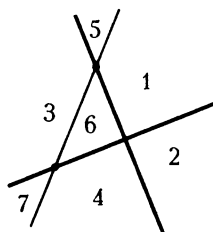


Рис. 5

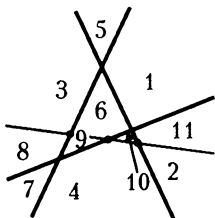


Рис. 6

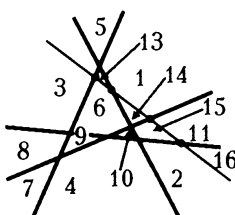


Рис. 7

$f(2) = 4$ и $f(3) = 7$. Чуть сложнее увидеть, что $f(4) = 11$ (рис.6) и $f(5) = 16$ (рис. 7). Запишем найденные значения в таблицу:

n	1	2	3	4	5
$f(n)$	2	4	7	11	16

Видите закономерность? $4 = 2 + 2$, $7 = 3 + 4$, $11 = 4 + 7$, $16 = 5 + 11$ – числа правого столбца равны сумме соседей слева и сверху. Формулой это можно записать так:

$$f(n) = n + f(n-1). \quad (*)$$

Чтобы доказать эту формулу, посмотрим, что происходит, когда к $n-1$ прямым добавляем еще одну. Например, на рисунке 8 к пяти прямым добавлена шестая прямая. Она пересекает не

все части, на которые пять прямых разрезают плоскость, а только шесть частей. Это не случайно: поскольку шестая прямая пересекает каждую из других прямых, всего возникает пять точек пересечения, которые делят прямую на шесть частей – два луча и четыре отрезка. Каждый из отрезков и лучей, на которые шестую прямую делят точки ее пересечения с пятью другими, является

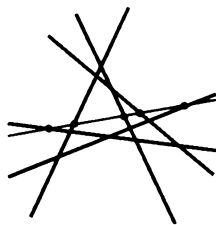


Рис. 8

следом от разрезания некоторой части на две. Значит, $f(6) = f(5) + 6$. Аналогично обстоит дело и в общем случае: при добавлении n -й прямой к $n - 1$ прямым количество частей увеличивается на n (как вы помните, среди прямых не должно быть параллельных и никакие три не должны проходить через одну точку). Формула (*) доказана. Теперь легко найти $f(15) = 121$, продолжив таблицу.

Величину $f(150) = 11326$ можно вычислить так же, но нельзя ли побыстрее? Можно! Кроме рекуррентной (выражающей следующее значение через предыдущие) формулы (*) есть явная формула

$$f(n) = \frac{n(n+1)}{2} + 1. \quad (**)$$

Докажем ее по индукции.

База очевидна: $f(1) = 2 = \frac{1 \cdot (1+1)}{2} + 1$.

Переход состоит в том, что если $f(n-1) = \frac{(n-1)n}{2} + 1$, то

$$f(n) = n + f(n-1) = n + \frac{(n-1)n}{2} + 1 = \frac{n(n+1)}{2} + 1.$$

Заметьте, как легко! Правда, возникает вопрос: как можно было догадаться, что для $f(n)$ выполнена именно формула (**)?

Сумма $S(n) = 1 + 2 + 3 + \dots + n$ первых n натуральных чисел встречалась всякому, кто интересуется математикой. Эта сумма удовлетворяет соотношению

$$S(n) - S(n-1) = n.$$

Для $S(n)$ есть явная формула:

$$S(n) = \frac{n(n+1)}{2}, \quad (***)$$

вывести которую можно при помощи индукции, а можно и без индукции, записав сумму $S(n)$ два раза: сначала расположив слагаемые по возрастанию, а потом в обратном порядке, по убыванию:

$$\begin{aligned} S(n) &= 1 + 2 + 3 + \dots + (n-2) + (n-1) + n, \\ S(n) &= n + (n-1) + (n-2) + \dots + 3 + 2 + 1, \end{aligned}$$

и сложив эти равенства почленно:

$$2S(n) = (n+1) + (n+1) + (n+1) + \dots + (n+1) + (n+1) + (n+1) = n(n+1).$$

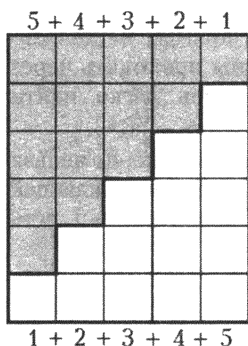


Рис. 9

Разделив на 2, получим формулу для $S(n)$. (На рисунке 9 это рассуждение проиллюстрировано геометрически: для $n = 5$ показано, как прямоугольник размером $n \times (n+1)$ можно разбить на две равные фигуры, каждая из которых состоит из $1 + 2 + 3 + \dots + n$ клеток.)

В следующем примере главное – догадаться, какую формулу надо доказывать по индукции. Давайте найдем явную формулу для суммы кубов первых n натуральных чисел. Начинаем: $1^3 = 1$, $1^3 +$

$$+ 2^3 = 9, \quad 1^3 + 2^3 + 3^3 = 36, \quad 1^3 + 2^3 + 3^3 + 4^3 = 100, \quad 1^3 + 2^3 + 3^3 + 4^3 + 5^3 = 225, \quad 1^3 + 2^3 + 3^3 + 4^3 + 5^3 + 6^3 = 441.$$

Что же это за числа: 1, 9, 36, 100, 225, 441? Это квадраты! И не просто квадраты, а квадраты сумм первых n натуральных чисел: $1 = 1^2$, $9 = (1+2)^2$, $36 = (1+2+3)^2$, $100 = (1+2+3+4)^2$, $225 = (1+2+3+4+5)^2$, $441 = (1+2+3+4+5+6)^2$.

Возникает гипотеза: сумма кубов первых n натуральных чисел равна квадрату суммы этих чисел. Вспомнив формулу (**), мы можем сформулировать гипотезу в более удобном для применения индукции виде:

$$1^3 + 2^3 + 3^3 + \dots + n^3 = \left(\frac{n(n+1)}{2} \right)^2.$$

Докажем ее.

База: $1^3 = \left(\frac{1(1+1)}{2} \right)^2$. **Переход:** предположим, что для неко-

торого натурального числа n формула верна. Тогда

$$\begin{aligned} (1^3 + 2^3 + 3^3 + \dots + n^3) + (n+1)^3 &= \left(\frac{n(n+1)}{2} \right)^2 + (n+1)^3 = \\ &= \frac{(n+1)^2}{4} (n^2 + 4n + 4) = \frac{(n+1)^2 (n+2)^2}{4} = \left(\frac{(n+1)(n+2)}{2} \right)^2. \end{aligned}$$

Понимаете, что произошло? Сумму кубов первых $n+1$ натуральных чисел мы представили как сумму суммы кубов n чисел и числа $(n+1)^3$. А дальше – всего лишь алгебраические преобразования!

Упражнения

6. Каждая из сумм $1, 3 + 5, 7 + 9 + 11, 13 + 15 + 17 + 19, \dots$ равна кубу количества слагаемых. Докажите это.

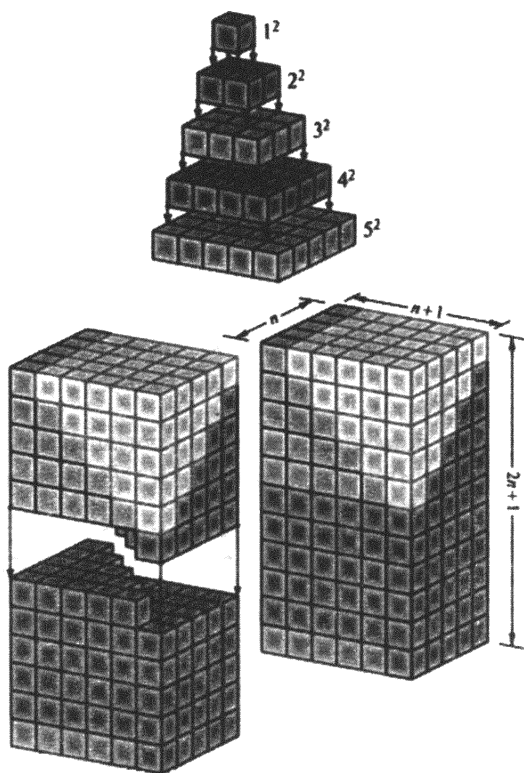


Рис. 10

7. а) Докажите по индукции равенство

$$1^2 + 2^2 + 3^2 + \dots + n^2 = n(n+1)(2n+1)/6.$$

б) Рассматривая обложку этой книги и рисунок 10, убедитесь, что из $1^2 + 2^2 + 3^2 + \dots + n^2$ кубиков можно сложить ступенчатую пирамиду, из трех таких пирамид – «почти куб», а из двух «почти кубов» – параллелепипед $n \times (n+1) \times (2n+1)$.

Тождество $3k(k+1) = k(k+1)(k+2) - (k-1)k(k+1)$ позволяет найти

$$\begin{aligned} \sum_{k=1}^n k(k+1) &= \frac{1}{3}(1 \cdot 2 \cdot 3 - 0 \cdot 1 \cdot 2 + 2 \cdot 3 \cdot 4 - 1 \cdot 2 \cdot 3 + 3 \cdot 4 \cdot 5 - \\ &\quad - 2 \cdot 3 \cdot 4 + \dots + (n-1)n(n+1) - \\ &\quad - (n-2)(n-1)n + n(n+1)(n+2) - (n-1)n(n+1)) = \\ &= \frac{n(n+1)(n+2)}{3}. \end{aligned}$$

Чему равна сумма четвертых степеней? А сумма пятых степеней? Помогают следующие легко запоминаемые формулы:

$$\sum_{k=1}^n k = \frac{n(n+1)}{2}, \quad \sum_{k=1}^n k(k+1) = \frac{n(n+1)(n+2)}{3},$$

$$\sum_{k=1}^n k(k+1)(k+2) = \frac{n(n+1)(n+2)(n+3)}{4},$$

и вообще, $\sum_{k=1}^n k^{\bar{s}} = \frac{n^{\overline{s+1}}}{s+1}$, где $k^{\bar{s}}$ – это произведение $k \cdot (k+1) \cdot \dots \cdot (k+s-1)$.

Теперь сумму четвертых степеней вычислить несложно: поскольку $k^4 = k(k+1)(k+2)(k+3) - 6k^3 - 11k^2 - 6k$, имеем:

$$\begin{aligned} \sum_{k=1}^n k^4 &= \sum_{k=1}^n k(k+1)(k+2)(k+3) - 6 \sum_{k=1}^n k^3 - 11 \sum_{k=1}^n k^2 - 6 \sum_{k=1}^n k = \\ &= \frac{n(n+1)(n+2)(n+3)(n+4)}{5} - 6 \cdot \frac{n^2(n+1)^2}{4} - \\ &\quad - 11 \cdot \frac{n(n+1)(2n+1)}{6} - 6 \cdot \frac{n(n+1)}{2}. \end{aligned}$$

Воспользовавшись формулой $\frac{1}{k(k+1)} = \frac{1}{k} - \frac{1}{k+1}$, полу-

чаем

$$\begin{aligned}\sum_{k=1}^n \frac{1}{k(k+1)} &= \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \dots + \frac{1}{(n-1)n} + \frac{1}{(n+1)n} = \\ &= 1 - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \frac{1}{3} - \frac{1}{4} + \dots + \frac{1}{n-1} - \frac{1}{n} + \frac{1}{n} - \frac{1}{n+1} = \\ &= 1 - \frac{1}{n+1} = \frac{n}{n+1}.\end{aligned}$$

А равенство

$$\frac{1}{k(k+1)(k+2)} = \frac{1}{2} \left(\frac{1}{k(k+1)} - \frac{1}{(k+1)(k+2)} \right)$$

помогает найти сумму $\sum_{k=1}^n \frac{1}{k(k+1)(k+2)}$. Разумеется, формулы

$$\sum_{k=1}^n \frac{1}{k(k+1)} = \frac{n}{n+1} \quad \text{и} \quad \sum_{k=1}^n \frac{1}{k(k+1)(k+2)} = \frac{1}{2} \left(\frac{1}{2} - \frac{1}{(n+1)(n+2)} \right)$$

легко доказать по индукции, как только они выписаны. Изложенный выше способ замечателен тем, что не требует предварительного знания ответа.

Одна из интересных особенностей индукции состоит в том, что более точное утверждение иногда легче доказать, чем более слабое. Например, пусть $P_n = \frac{1 \cdot 3 \cdot 5 \cdot \dots \cdot (2n-1)}{2 \cdot 4 \cdot 6 \cdot \dots \cdot (2n)}$. Докажем не-

равенство $P_n < \frac{1}{\sqrt{n}}$.

База: $P_1 = \frac{1}{2} < \frac{1}{\sqrt{1}}$. Теперь попытаемся провести индукцион-

ный переход, т.е. из неравенства $P_n < \frac{1}{\sqrt{n}}$ попробуем вывести

неравенство $P_{n+1} < \frac{1}{\sqrt{n+1}}$. Очевидно,

$$P_{n+1} = P_n \cdot \frac{2n+1}{2n+2} < \frac{1}{\sqrt{n}} \cdot \frac{2n+1}{2n+2}.$$

Если бы правая часть не превосходила $\frac{1}{\sqrt{n+1}}$, то индукционный переход состоялся бы. Но увы: возводя интересующие нас

выражения в квадрат, получаем: $\frac{(2n+1)^2}{4n(n+1)^2}$ и $\frac{1}{n+1}$. Приведа к

общему знаменателю, приходим к сравнению чисел $4n^2 + 4n + 1$ и $4n(n+1)$. Очевидно, первое больше, а нам хотелось обратного!

Переход не состоялся. Это не значит, что неравенство $P_n < \frac{1}{\sqrt{n}}$ неверно. Не годится лишь наш метод доказательства. Докажем

более точное неравенство $P_n < \frac{1}{\sqrt{n+1}}$.

База индукции: $P_1 = \frac{1}{2} < \frac{1}{\sqrt{2}}$. **Переход:**

$$P_{n+1} = P_n \cdot \frac{2n+1}{2n+2} < \frac{1}{\sqrt{n+1}} \cdot \frac{2n+1}{2n+2}.$$

Неравенство $\frac{2n+1}{2\sqrt{n+1}(n+1)} < \frac{1}{\sqrt{n+2}}$ после возведения обеих частей в квадрат и перехода к общему знаменателю превращается в неравенство $(n+2)(4n^2 + 4n + 1) < 4(n+1)^3$. Раскроем скобки:

$$4n^3 + 8n^2 + 4n^2 + 8n + n + 2 < 4n^3 + 12n^2 + 12n + 4,$$

т.е. $0 < 3n + 2$. Получилось! Причина в том, что в доказательстве более сильного утверждения мы опирались на более сильное предположение индукции. На первый взгляд это удивительно, но так часто бывает: чем точнее утверждение, тем легче его доказать!

Довольно точные оценки величины P_n можно получить и без индукции. А именно, $P_n^2 = \frac{1 \cdot 3}{2^2} \cdot \frac{3 \cdot 5}{4^2} \cdot \dots \cdot \frac{(2n-1) \cdot (2n+1)}{(2n)^2} \cdot \frac{1}{2n+1}$.

Оставляя первый множитель $\frac{3}{4}$ без изменения, заменяя последний множитель $\frac{1}{2n+1}$ на большее число $\frac{1}{2n}$ и заменяя все другие множители на 1, в силу неравенства $(2k-1)(2k+1) < (2k)^2$ получаем неравенство $P_n^2 < \frac{3}{4} \cdot \frac{1}{2n}$, откуда $P_n < \sqrt{\frac{3}{8n}}$.

Аналогично можно получить оценку снизу:

$$P_n^2 = \frac{1}{2} \cdot \frac{3^2}{2 \cdot 4} \cdot \frac{5^2}{4 \cdot 6} \cdot \dots \cdot \frac{(2n-1)^2}{(2n-2)(2n)} \cdot \frac{1}{2n} > \frac{1}{2} \cdot \frac{1}{2n},$$

откуда $P_n > \frac{1}{2\sqrt{n}}$.

При помощи интегрального исчисления можно доказать формулу Валлиса: $\lim_{n \rightarrow \infty} P_n \sqrt{n} = \frac{1}{\sqrt{\pi}} = 0,5642\dots$

Упражнение 8. Найдите ошибку в следующем рассуждении, которое доказывает, что через любые n точек можно провести прямую линию.

«Доказательство». Применим индукцию. При $n = 1$ и $n = 2$ все правильно.

Осталось доказать это для больших значений n . Допустим, что утверждение верно при некотором $n = k$, и покажем, что в этом случае оно сохранит силу и при $n = k + 1$. Пусть произвольно заданы точки $M_1, M_2, \dots, M_k, M_{k+1}$. В силу предположения индукции, через k точек M_1, M_2, \dots, M_k проходит некоторая прямая l . В силу того же предположения через k точек M_2, \dots, M_k, M_{k+1} также проходит некоторая прямая l' .

Эти две прямые имеют по крайней мере две общие точки M_2 и M_k . Но две точки определяют единственную прямую. Поэтому прямые l и l' совпадают. Следовательно, прямая l , проходящая через точки M_1, M_2, \dots, M_k , проходит и через точку M_{k+1} .

...Наступило утро, и городские ворота со скрипом распахнулись. Зазвенели бубенцы, закричали погонщики, и караваны, груженные драгоценными индийскими тканями, прекрасной медной и серебряной посудой, знаменитыми хорасанскими коврами и множеством других дорогих товаров, двинулись в город. За воротами стояли бухарские стражники с разбойничьими физиономиями. Они ухмылялись, предвкушая сбор пошлины, часть которой непременно оседала в их карманах.

Вслед за караваном богатого купца из Багдада в ворота въехала скромная скрипучая арба декханина Али, полная арбузов. На арбе сидели двое. Один – сам Али, все лето не разгибавший спины на своей бахче, а другой – Ходжа Насреддин, выручивший недавно Али из неприятной истории с поливом посевов. В благодарность за помощь Али чуть не силой заставил Насреддина принять от него часть урожая, и теперь они вместе везли арбузы на бухарский базар: 104 арбуза Али и 17 – Насреддин.

– Стойте! – сказал начальник стражи, и арба остановилась. – По какому делу вы едете в благородную Бухару?

Али открыл было рот, чтобы подробно объяснить, но Насреддин дернул его за рукав и быстро сказал:

– На базар, о доблестные воины!

– Что продавать будете?

– Арбузы!

– С вас деловая пошлина – ведь вы едете по делу; и торговая пошлина – ведь вы едете торговать; и арбузная пошлина – ведь вы ввозите в город арбузы.

– Но... – начал Али.

– Молчи! – шепнул Насреддин. – Каждое слово тут стоит денег, а у нас с тобой их нет.

– Нет денег? – взревел начальник стражи, отличавшийся очень острым слухом, когда речь шла о возможности пожить-ся. – Поворачивайте оглобли! Мы не впустим вас в город!

– Зато у нас есть арбузы, – поспешно заметил Насреддин. – Сколько стоят арбузы на бухарском базаре?

Стражники переглянулись. День был жарким, и дармовые

арбузы пришлось бы кстати. Поразмыслив с минуту и поглядев на облизывающихся стражников, начальник назвал цену.

Всего полчаса поторговавшись, начальник стражи и Насреддин пришли к соглашению.

– Значит, Али должен отдать тебе 19 арбузов, но он переплатит тебе 1 таньга, – сказал Насреддин. – Зато я должен тебе 3 арбуза и 1 таньга впридачу. У меня нет и одной таньга, но я великодушно освобождаю тебя от долга моему другу. По рукам?

– По рукам, – ответил начальник стражи и кивнул своим подчиненным. Стражники кинулись к арбе и принялись разгружать арбузы. Насреддин внимательно следил за ними.

– Стой, почтенный, это уже лишний арбуз, мы уплатили пошлину сполна! – закричал он наконец, увидев, как один из стражников ухватился за двадцать третий арбуз. Стражник замешкался, Али подхлестнул ишака, и арба, переваливаясь, покатила подальше от ворот.

За спиной у друзей раздавалось чавканье: караул торопливо поглощал арбузы.

Вечером, распродав свой товар, Ходжа Насреддин и Али сидели в чайхане. Теперь у них было на что купить плов, так что они с удовольствием ужинали. Пузатый чайханщик принес каждому по чайнику и поставил на столик пиалы. И тут к друзьям подсел бородатый старик важного вида. Присмотревшись, Насреддин узнал его: они встречались прежде при довольно неприятных обстоятельствах. Это был знаменитый звездочет и мудрец Гуссейн Гуслия, главный математик эмира бухарского. К старости он стал слаб глазами и не узнал Насреддина, доставившего ему в свое время немало хлопот.

«Сейчас я поражу своей мудростью этих невежественных людей, – думал Гуссейн Гуслия. – Они расскажут об этом другим, слух дойдет и до эмира, и он будет ценить мою ученость еще больше».

– Я слышал ваш разговор со стражниками у бухарских ворот, – начал он, поглаживая длинную бороду. – Но я не слышал, какова должна была быть пошлина и сколько стоит один арбуз, – уж очень громко кричали доблестные стражи. Но я – великий ученый, и могу назвать цену арбуза, не побывав на базаре и никого не спрашивая.

– Что же, назови, – отозвался Ходжа Насреддин.

– 11 таньга! – провозгласил звездочет и с торжеством поглядел на собеседника. – Я великий мудрец эмира, сам

Гуссейн Гуслия, и вы должны признать мою несравненную мудрость...

– Ты не угадал, о великий Гуссейн Гуслия, – перебил его Насреддин.

– Как это «не угадал»? – возмутился старик. – Я знаю наизусть великую книгу Аль-Хорезми «Аль-джебр аль-мукабала», полную глубочайшей премудрости и недоступную невежественным умам. Вот смотри: если арбуз стоит x таньга, а за его провоз стражники берут y таньга, то цена 19 арбузов на 1 таньга больше, чем налог, который Али уплатил за свои 104 арбуза:

$$19x = 104y + 1.$$

А ты за свои 17 арбузов заплатил меньше, чем должен был, на 1 таньга, отдав 3 арбуза:

$$3x = 17y - 1.$$

Теперь, пользуясь наукой несравненного Аль-Хорезми, углубляться в которую нет нужды, ибо ты все равно ничего не поймешь, я нахожу x и y :

$$x = 11, y = 2.$$

Гуссейн Гуслия размахивал листом пергамента с расчетами, презрительно поглядывая на Насреддина.

– Мудрость твоя велика, – спокойно ответил Ходжа Насреддин. – Но, как сказал один умный человек, математика – это мельница, которая перемалывает то, что кладут на ее жернова. Я тоже не буду углубляться в премудрую науку Аль-Хорезми, ибо я не могу сравниться с тобой в учености, но знай, что вместо зерна ты бросил в жернова математики семена полыни, и доброй муки у тебя не вышло.

– Как это? – оскорбился звездочет. – Как можешь ты судить о верности моего решения, ты, презренный декханин, подобный невежеством своему ишаку?

– Так скажи мне, о Гуссейн Гуслия, с избытком одаренный познаниями, но чуточку обиженный умом, – спокойно ответил Насреддин, – зачем Али платить пошлину за те 19 арбузов, которые он отдал стражникам? Ведь их-то он не повез на базар. И я не обязан платить за 3 арбуза, съеденные у ворот доблестными воинами. Так что записать нужно так:

$$19x = (104 - 19)y + 1,$$

$$3x = (17 - 3)y - 1.$$

Теперь ты можешь привлечь ту достойную восхищения на-

уку, в которой тебе нет равных, и убедиться, что арбуз стоит 9 таньга.

Гуссейн Гуслия погрузился в вычисления и обнаружил, что непочтительный незнакомец прав.

– На этот раз я ошибся, – неохотно признался он. – Должен сказать тебе, что твои рассуждения достойны самого Ходжи Насреддина. И твое нахальство тоже!

Ходжа Насреддин долго смеялся. Хохотал Али. Чайханщик схватился за живот и тихо постанывал: «Ой, умру!» Гуссейн Гуслия некоторое время смотрел на них с недоумением, потом дернул себя за бороду и запричитал:

– Так это ты, о сын греха, это снова ты явился в Бухару, чтобы посмеяться над моими сединойми! Чтоб тебя забрал шайтан, чтоб тебе не знать покоя на том и этом свете, чтоб...

– Успокойся, почтенный, – сказал Ходжа Насреддин, утирая слезы. – Я всего лишь приехал продавать арбузы.

Алгоритм Евклида – это способ отыскания наибольшего общего делителя целых чисел, тесно связанный с алгоритмом разложения рациональных чисел в цепные дроби и с поиском решений линейных уравнений в целых числах.

По определению, $\text{НОД}(0; 0) = 0$, а для любой другой пары целых чисел a и b их наибольший общий делитель $\text{НОД}(a; b)$ – это наибольшее натуральное число d , на которое нацело делятся числа a и b . Основная идея алгоритма Евклида – равенство

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

которое верно для любых целых чисел a , b и q . Докажем его. С одной стороны, всякий общий делитель d чисел a и b является и делителем числа $a - bq$, ведь если $a = dx$ и $b = dy$ для некоторых целых чисел x и y , то $a - bq = dx - dyq = d(x - yq)$, а число $x - yq$ целое. С другой стороны, всякий общий делитель чисел $a - bq$ и b аналогичным образом является и делителем числа $a = (a - bq) + bq$. Следовательно, множество общих делителей чисел a и b совпадает с множеством общих делителей чисел $a - bq$ и b . А если совпадают множества, то совпадают и их наибольшие элементы. Равенство доказано.

Деление с остатком

При делении «уголком» (рис.1) числа $a = 20052005$ на $b = 43$ получаем частное 466325 и остаток 30 . Это можно записать формулой

$$\begin{array}{r} 20052005 \overline{) 43} \\ \underline{172} \\ 285 \\ \underline{258} \\ 272 \\ \underline{258} \\ 140 \\ \underline{129} \\ 110 \\ \underline{86} \\ 245 \\ \underline{215} \\ 30 \end{array}$$

$$20052005 = 43 \cdot 466325 + 30.$$

Если $a = bq + r$, где q, r – целые числа, причем $0 \leq r < b$, то число q называют неполным частным, а r – остатком.

Доказать возможность деления с остатком несложно. Достаточно заметить, что любое число a либо само есть кратное числа b , либо лежит между двумя последовательными кратными числа b , т.е.

$$bq < a < b(q + 1).$$

В первом случае $r = 0$. Во втором случае

Рис. 1

$0 < a - bq < b$, так что число $r = a - bq$ удовлетворяет условиям $0 < r < q$.

Деление с остатком не только возможно, но и производится единственным способом. В самом деле, если

$$a = bq_1 + r_1 = bq_2 + r_2,$$

где q_1, q_2, r_1 и r_2 – целые числа, причем $0 \leq r_1 < b$ и $0 \leq r_2 < b$, то

$$b(q_1 - q_2) = r_2 - r_1.$$

Очевидно, $-b < r_1 - r_2 < b$. Единственным числом, которое больше числа $-b$, меньше числа b и нацело делится на b (а делится потому, что оно равно произведению числа b на $q_1 - q_2$), является число 0. Значит, $r_2 - r_1 = 0$ и $q_1 = q_2$: деление с остатком производится единственным способом.

Упражнение 1. Найдите неполное частное и остаток от деления на 12 числа а) 123; б) -123 .

Геометрический смысл деления с остатком

Пусть a и b – длины двух отрезков, $a > b$ (рис.2). Отложим b на a столько раз, сколько можно; получим остаток r_1 . Отложим r_1 на b сколько возможно раз, получим остаток r_2 , и так далее. Если, откладывая очередной отрезок длины r_n , мы не получим остатка (точнее, получим нулевой остаток $r_{n+1} = 0$), то отрезок длины r_n и есть наибольшая общая мера отрезков длин a и b .

Если числа a и b целые, то все остатки r_1, r_2, \dots также целые неотрицательные. В силу неравенств

$$b > r_1 > r_2 > \dots$$

процесс рано или поздно закончится. Последнее ненулевое число r_n и есть НОД($a; b$).

Если числа a и b не обязательно целые, то процесс откладывания может и не остановиться; тогда отрезки длин a и b называют несоизмеримыми, а отношение a/b – иррациональным числом. Например, диагональ правильного пятиугольника $ABCDE$ (рис. 3) несоизмерима с его стороной: поскольку $PCDE$ – ромб, то $PE = CD$, так что первый шаг алгоритма Евклида заменяет пару отрезков BE и BA на пару AB и BP .

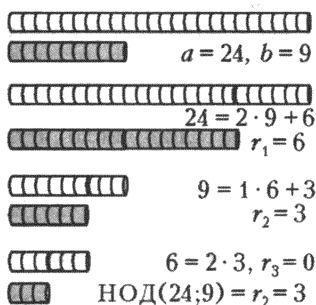


Рис.2

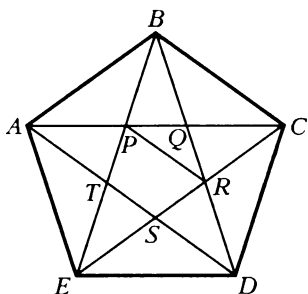


Рис. 3

Поскольку прямая EQ является осью симметрии пятиугольника $ABCDE$, то $PR \parallel AD$ и, следовательно, $\angle PRB = \angle ADB$. Так как пятиугольник $ABCDE$ симметричен и относительно прямой CT , то $\angle TDB = \angle TBD$. Следовательно, $BP = PR$. Поскольку $AB = CD = = BT = BP + PT$, то второй шаг алгоритма Евклида сводит задачу

нахождения общей меры диагонали и стороны правильного пятиугольника $ABCDE$ к задаче об общей мере отрезков $PB = PR$ и PT , т.е. к задаче об общей мере диагонали и стороны правильного пятиугольника $PQRST$.

Следующие два шага сведут задачу к поиску общей меры диагонали и стороны еще меньшего правильного пятиугольника. Значит, процесс будет длиться вечно, никогда не закончится!

Алгоритм Евклида в двоичной системе счисления

Особенно просто вычислять наибольший общий делитель, пользуясь двоичной системой счисления. Если двоичные записи двух чисел оканчиваются нулями, то они оба четные и мы используем формулу

$$\text{НОД}(2a; 2b) = 2\text{НОД}(a; b).$$

Если одно число четное, а другое нечетное, используем формулу

$$\text{НОД}(2a; 2b + 1) = \text{НОД}(a; 2b + 1).$$

А если оба нечетные, используем формулу

$$\text{НОД}(2a + 1; 2b + 1) = \text{НОД}(2a - 2b; 2b + 1) = 2\text{НОД}(a - b; 2b + 1).$$

Упражнения

2. Вычислите $\text{НОД}(3542; 2492)$, пользуясь двоичной системой счисления

3*. В три сосуда налито по целому числу литров воды. В любой сосуд разрешено перелить столько воды, сколько в нем уже содержится, из любого другого сосуда. Докажите, что несколькими такими переливаниями можно освободить один из сосудов. (Сосуды достаточно велики: каждый может вместить всю воду.)

Пример работы алгоритма Евклида

В привычной десятичной системе счисления вычислим НОД(6069; 663). Для этого разделим 6069 на 663 с остатком:

$$6069 = 663 \cdot 9 + 102.$$

Следовательно, $\text{НОД}(6069; 663) = \text{НОД}(663; 102)$. Поскольку $663 = 102 \cdot 6 + 51$, то $\text{НОД}(663; 102) = \text{НОД}(51; 102)$. Поскольку 102 делится на 51, получаем ответ: $\text{НОД}(6069; 663) = \text{НОД}(663; 102) = \text{НОД}(51; 102) = 51$.

Часто для краткости опускают буквы НОД, считая, что круглые скобки обозначают наибольший общий делитель чисел (не обязательно двух; в скобки можно заключить любое множество чисел). Наименьшее общее кратное $\text{НОК}[a; b]$ – наименьшее натуральное число, которое делится без остатка и на a , и на b , – тоже часто пишут без букв НОК.

Итак, алгоритм Евклида – это довольно быстро работающий метод нахождения наибольшего общего делителя двух чисел. Если даны два числа a и b , причем $a > b > 0$, то сначала делим a на b :

$$a = bq_1 + r_1,$$

где q_1 – неполное частное (которое не используется в дальнейших вычислениях), r_1 – остаток, $r_1 < b$. Если $r_1 > 0$, делим число b на r_1 и находим неполное частное q_2 и (только и интересующий нас) остаток r_2 . Если $r_2 > 0$, делим число r_1 на r_2 , при этом получаем остаток r_3 , меньший, чем r_2 , и так далее, пока какое-нибудь число r_{n-1} не разделится на r_n нацело (т.е. $r_{n+1} = 0$). Последний ненулевой остаток r_n и есть искомый наибольший делитель чисел a и b :

$$\begin{aligned}\text{НОД}(a; b) &= (b; r_1) = (r_1; r_2) = \dots = (r_{n-2}; r_{n-1}) = \\ &= (r_{n-1}; r_n) = (r_n; 0) = r_n.\end{aligned}$$

Линейные уравнения. Примеры

Алгоритм Евклида тесно связан с решением уравнений вида

$$ax - by = c$$

в целых числах, где a , b и c – данные целые числа, x и y – неизвестные.

Не любое уравнение такого вида имеет решения в целых числах. Например, равенство $2x - 246y = 345$ для целых чисел

x и y невозможно, поскольку левая часть делится на 2, а правая не делится.

Рассмотрим уравнение

$$69x - 91y = 1996.$$

Скорее всего, решения у него есть, но как их найти? Можно попытаться угадать пару чисел $(x; y)$, но вдруг не повезет? Быстрый и удобный способ дает алгоритм Евклида. Перепишем уравнение в виде

$$69x - 69y - 22y = 1996.$$

Обозначив $z = x - y$, получим

$$69z - 22y = 1996.$$

Один из коэффициентов полученного уравнения (69) остался от исходного уравнения, а другой (22) меньше, чем коэффициент исходного (91). Причина в том, что 22 – остаток от деления 91 на 69. Продолжим:

$$3z + 66z - 22y = 1996.$$

Обозначив $t = 3z - y$, придем к уравнению

$$3z + 22t = 1996.$$

Его решение легко угадать: $t = 1$, $z = (1996 - 22)/3 = 658$. Теперь легко вернуться к искомым x , y – достаточно посчитать сначала $y = 3z - t = 3 \cdot 658 - 2 = 1972$, потом $x = z + y = 1972 + 658 = 2630$.

Впрочем, можно было обойтись и совсем без угадывания, переписав уравнение в виде

$$3z + 21t + t = 1996,$$

обозначив $m = z + 7t$ и, таким образом, сведя дело к уравнению $3m + t = 1996$.

Если вместо m подставить любое целое число, то получим (тоже целое!) $t = 1996 - 3m$. Это позволяет нам найти $z = m - 7t = m - 7(1996 - 3m) = 22m - 13972$. Далее, $y = 3z - t = 3(22m - 13972) - (1996 - 3m) = 69m - 43912$. Наконец, $x = z + y = (22m - 13972) + (69m - 43912) = 91m - 57884$.

Мы нашли общее решение уравнения в целых числах:

$$\begin{cases} x = 91m - 57884, \\ y = 69m - 43912. \end{cases}$$

Подставьте в эти формулы вместо m любое целое число – получите некоторое частное решение. (Если боитесь, что мы

допустили арифметическую ошибку, проверьте тождество $69 \cdot (91m - 57884) - 91 \cdot (69m - 43912) = 1996$.) В найденном виде представимо любое решение $(x; y)$ интересующего нас уравнения.

Упражнение 4. Если натуральное число n не делится на 3, то существуют два последовательных натуральных числа, сумма цифр каждого из которых делится на n . Докажите это.

Точки с целыми координатами на прямой

Прямая на плоскости задается, как известно, уравнением первой степени. Любое такое уравнение можно привести к виду $ax - by = c$, где a, b, c — целые числа. Рассмотрим примеры.

$2x = 5$. Уравнение задает прямую, параллельную оси ординат (вертикальную прямую). Точек с целыми координатами на этой прямой нет, поскольку число $5/2$ не целое.

$y = x$. Это биссектриса первого («северо-восточного») и третьего («юго-западного») квадрантов. Точек с целыми координатами бесконечно много. Они расположены на равных расстояниях одна от другой. Каждому целому x соответствует целое $y = x$.

$4x = -5y$. Прямая проходит через начало координат. Числа 4 и -5 взаимно просты. Для того, чтобы $-5y$ делилось на 4, необходимо и достаточно, чтобы y делилось на 4, т.е. $y = 4t$, где $t \in \mathbb{Z}$. Подставляя в уравнение, получаем $4x = -5 \cdot 4t$, т.е. $x = -5t$. Значит, целочисленных точек бесконечно много. Они расположены на равных расстояниях и описываются формулой $(x; y) = (-5t; 4t)$.

$2y - 3x = 6$. Выразив y через x , получим $y = \frac{3}{2}x + 3$. Если x нечетно, то y — не целое. Если же $x = 2t$, то $y = 3t + 3$. Следовательно, на исследуемой прямой лежит бесконечно много точек с целыми координатами:

$$\begin{cases} x = 2t, \\ y = 3t + 3, \end{cases}$$

где t — любое целое число.

$5x - 7y = 2$. Легко подобрать пару целых чисел $(x; y) = (-1; -1)$. Немного подумав, найдем еще одну пару: $x = 6, y = 4$. Вообще, если увеличить x на 7, а y на 5, то выражение $5x - 7y$ не изменит своего значения:

$$5(x + 7) - 7(y + 5) = 5x + 5 \cdot 7 - 7y - 7 \cdot 5 = 5x - 7y.$$

Поэтому, зная одну пару целых чисел (x, y) , удовлетворяющих уравнению $5x - 7y = 2$, мы можем указать бесконечно много других пар:

$$\begin{cases} x = 7t - 1, \\ y = 5t - 1. \end{cases}$$

Проверка того, что все эти пары удовлетворяют уравнению, не составляет труда:

$$5(7t - 1) - 7(5t - 1) = 35t - 5 - 35t + 7 = 2.$$

Никаких других целочисленных решений исследуемое уравнение не имеет. Доказывать это можно разными способами. Например, запишем

$$\begin{cases} 5x - 7y = 2, \\ 5 \cdot (-1) - 7 \cdot (-1) = 2 \end{cases}$$

и приравняем левые части: $5x - 7y = 5 \cdot (-1) - 7 \cdot (-1)$, откуда $5(x + 1) = 7(y + 1)$. Теперь ясно, что левая часть должна делиться на 7. Следовательно, число $x + 1$ должно нацело делиться на 7, т.е. $x + 1 = 7t$, где t — целое. Осталось выполнить подстановку $5 \cdot 7t = 7(y + 1)$ и получить $y = 5t - 1$.

Разумеется, можно было решить уравнение $5x - 7y = 2$ и каким-нибудь другим способом. Рассмотренный нами способ интересен тем, что при помощи него можно решить уравнение $ax - by = c$ не только при $(a; b; c) = (5; 7; 2)$, но и в общем случае.

Линейные уравнения. Общий случай

Пусть при помощи алгоритма Евклида или любым другим способом на прямой $ax - by = c$ мы нашли одну точку с целыми координатами. Найдем все целочисленные точки этой прямой.

Теорема 1. Если числа a, b взаимно простые, a, x_0 и y_0 — целые числа, удовлетворяющие равенству $ax_0 - by_0 = c$, то пары чисел x, y , удовлетворяющие равенству $ax - by = c$, имеют вид

$$\begin{cases} x = x_0 + bt, \\ y = y_0 + at, \end{cases}$$

где t — целое.

Доказательство. В одну сторону утверждение очевидно:

$$a(x_0 + bt) - b(y_0 + at) = ax_0 + abt - by_0 - abt = ax_0 - by_0 = c.$$

В другую сторону рассуждение чуть сложнее: $ax - by = c = ax_0 - by_0$ и, следовательно, $a(x - x_0) = b(y - y_0)$. Поскольку числа a и b взаимно просты и $a(x - x_0)$ делится на b , то $x - x_0$ делится на b , т.е. $x - x_0 = bt$ для некоторого целого t . При этом

$$abt = b(y - y_0),$$

откуда $y = y_0 + at$, что и требовалось доказать.

Следующая теорема – необходимое и достаточное условие разрешимости линейного уравнения в целых числах.

Теорема 2. *Уравнение $ax - by = c$, где a, b, c – данные целые числа, x и y – неизвестные, имеет решения в целых числах тогда и только тогда, когда число c делится на наибольший общий делитель чисел a и b .*

Одно доказательство этой теоремы непосредственно вытекает из изложенного выше способа решения с помощью алгоритма Евклида. (Подумайте, как именно!) Второй – не менее замечательный – способ доказательства основан на следующей лемме.

Лемма. *Пусть a и b – целые числа, хотя бы одно из которых не равно 0. Обозначим буквой m наименьшее натуральное число, представимое в виде $m = ax - by$, где x, y – целые числа. Тогда $m = \text{НОД}(a; b)$.*

Доказательство. Обозначим $d = \text{НОД}(a; b)$. Тогда любое число вида $ax - by$, в том числе и m , делится на d . Осталось доказать, что не только m делится на d , но и d – на m . Для этого докажем, что как число a , так и число b делится на m . Рассуждаем «от противного». Пусть, например, a не делится на m . Разделим a на m с остатком:

$$a = mq + r,$$

где $0 < r < m$. Поскольку число m представимо в виде $m = aX - bY$, где X, Y – целые, то

$$r = a - mq = a - (aX - bY)q = a(1 - Xq) + bYq.$$

Таким образом, число r представимо в виде $r = ax - by$. Но $0 < r < m$, а m , как помните, – наименьшее натуральное число, представимое в таком виде. Лемма доказана. Утверждение теоремы 2 следует из нее.

Докажем теорему 2 еще одним – геометрическим – способом. Через l_c для любого целого числа c обозначим прямую, заданную уравнением $ax - by = c$. Рассмотрим параллелограмм с вершинами $(0; 0)$, $(0; -1)$, $(b; a - 1)$ и $(b; a)$. Длины двух вертикальных его сторон равны 1, а большие стороны лежат

на прямых l_0 и l_b . Внутри этого параллелограмма (не в вершинах) лежит ровно $b - 1$ целых точек: на каждой из вертикальных прямых $x = 1, x = 2, \dots, x = b - 1$ по одной. Параллелограмм пересекают как раз столько же $(b - 1)$ прямых: l_1, l_2, \dots, l_{b-1} . Поскольку более одной целочисленной точки, абсциссы которых отличаются менее чем на b , прямая l_c ни при каком c иметь не может, то все $b - 1$ точек лежат по одной на каждой прямой. В частности, есть целочисленная точка и на прямой l_1 .

Упражнения

5. Любое подмножество множества целых чисел, содержащее вместе с любыми своими элементами a и b их разность $a - b$, является множеством всех кратных некоторого целого числа. Докажите это.

6. В $(a + b)$ -этажном доме лифт при нажатии кнопки поднимается на a этажей вверх или опускается на b этажей вниз. (Когда сверху меньше a этажей, лифт вверх не идет, аналогично – вниз.) Лифт стартовал с первого этажа. Сколько раз надо нажать на кнопку, чтобы лифт вернулся на первый этаж?

Центральная симметрия

Рассмотрим взаимно простые натуральные числа a и b . Буквой M обозначим множество целых чисел, представимых в виде $ax + by$, где x и y – целые неотрицательные числа.

Для $a = 3$ и $b = 7$ жирными точками на рисунке 4 на числовой прямой изображены числа, принадлежащие множеству M , а проколотыми – не принадлежащие. При симметрии относительно числа 5,5 жирные точки переходят в проколотые, а проколотые – в жирные! То же явление видим на рисунке 5 для $a = 4$ и $b = 9$ (центр симметрии – 11,5) и на рисунке 6 для $a = 5$, $b = 12$ (центр симметрии – 21,5).

Теорема 3. Если $\text{НОД}(a; b) = 1$, то представимые целые точки симметричны непредставимым целым точкам относи-

тельно точки $c = \frac{ab - a - b}{2}$.

Доказательство. Предположим сначала, что некоторая точка $m = ax_1 + by_1$, где x_1 и y_1 – неотрицательные целые числа, симметрична относительно точки c точке $n = ax_2 + by_2$, где x_2 и y_2 – тоже целые неотрицательные числа. Тогда $c = \frac{m + n}{2}$, т.е.

$$ab - a - b = a(x_1 + x_2) + b(y_1 + y_2).$$

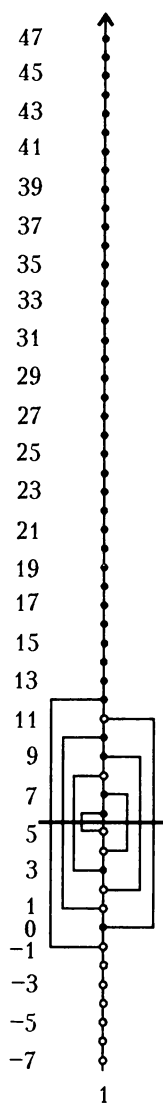


Рис. 4

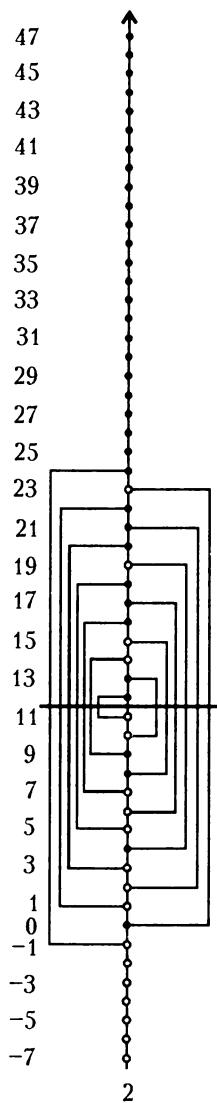


Рис. 5

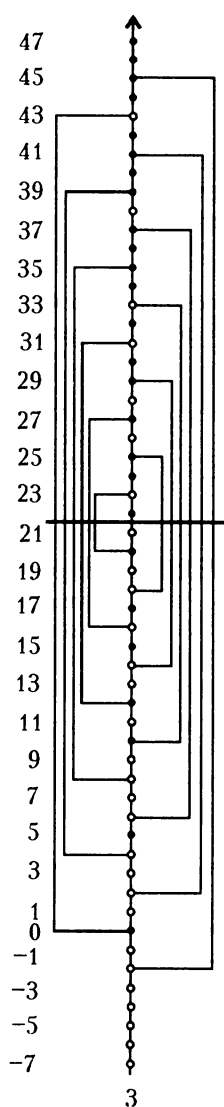


Рис. 6

Обозначив $x = x_1 + x_2$ и $y = y_1 + y_2$, получаем

$$ab = a(x+1) + b(y+1).$$

Поскольку числа ab и $a(x+1)$ делятся на a , то и число $b(y+1)$ делится на a . Значит, $y+1$ делится на a и поэтому $y+1 \geq a$, откуда получаем противоречие:

$$ab = a(x+1) + b(y+1) > b(y+1) \geq ab.$$

Теперь предположим, что относительно точки c симметричны две непредставимые точки m и n . Как мы только что видели, это означает, что

$$m + n = ab - a - b.$$

Поскольку числа a и b взаимно просты, то всякое целое число представимо в виде $ax + by$. Поскольку для любого целого t имеем

$$ax + by = a(x + bt) + b(y - bt),$$

то можно считать, что $0 \leq x < b$. Таким образом,

$$\begin{cases} m = ax_1 + by_1, \\ n = ax_2 + by_2, \end{cases}$$

где $0 \leq x_1, x_2 < b$, а числа y_1 и y_2 отрицательные. Складывая эти равенства, получаем

$$ab - a - b = a(x_1 + x_2) + b(y_1 + y_2),$$

т.е.

$$ab = a(x_1 + x_2 + 1) + b(y_1 + y_2 + 1).$$

Из последнего равенства следует делимость числа $x_1 + x_2 + 1$ на b . Поскольку x_1 и x_2 меньше числа b , то сумма $x_1 + x_2 + 1$ меньше $2b$. Следовательно, $x_1 + x_2 + 1 = b$. Значит,

$$ab = ab + b(y_1 + y_2 + 1),$$

что противоречит неравенствам $y_1 \leq -1$ и $y_2 \leq -1$.

Впрочем, теорему 3 можно гораздо проще доказать геометрически. Рассмотрим полосу, выделенную на плоскости неравенствами $0 \leq x < b$. Для любого целого числа c ровно одна точка прямой, заданной уравнением $ax + by = c$, принадлежит рассматриваемой полосе. Если ордината этой точки положительна, то число c представимо в виде $c = ax + by$ с неотрицательными числами x и y , а если ордината отрицательна, то не представимо.

Осталось заметить, что рассматриваемая полоса симметрична относительно точки $\left(\frac{b-1}{2}; -\frac{1}{2}\right)$. При этом $a \cdot \frac{b-1}{2} + b \cdot \left(-\frac{1}{2}\right) = \frac{ab - a - b}{2}$, что и доказывает симметрию множества M относительно точки c .

Упражнения

7. Лист бумаги можно разрезать на 6 или 12 частей. Каждый новый кусок можно разрезать на 6 или 12 частей или оставить целым, и так далее. а) Можно ли таким образом разрезать лист на 40 частей?

б) Докажите, что таким образом можно получить любое число частей, большее 40.

8. Для натуральных взаимно простых чисел a и b найдите наибольшее целое число, не представимое в виде $ax + by$ с неотрицательными x и y .

Китайская теорема об остатках

Какое число при делении на 3 дает остаток 2, при делении на 5 – остаток 3, а при делении на 7 – остаток 2? Эта задача о решении системы сравнений

$$\begin{cases} x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 2 \pmod{7} \end{cases}$$

была известна уже в древнем Китае. Сунь-цзы (между II и VI вв.) и более полно Цинь Цзю-шао (XIII в.) дали изложенное на примерах описание алгоритма решения таких задач. В точности эта задача есть и в «Книге об абак» итальянского математика Леонардо Пизанского (Фибоначчи) (1202 г.). Ответ получить несложно: $x \equiv 23 \pmod{105}$. (Проверьте!)

Но нас интересует не эта древняя задача, а общий случай. По определению, числа, дающие некоторый остаток r при делении на натуральное число m , имеют вид $mq + r$, где q – целое. Последовательность

$$r, r + m, r + 2m, r + 3m, \dots$$

называют арифметической прогрессией с разностью m .

Можно указать арифметические прогрессии из натуральных чисел, пересечение которых пусто. Например, поскольку ни одно число не является одновременно четным и нечетным, пусто пересечение прогрессии 2, 4, 6, ... с прогрессией 1, 3, 5, ...

Оказывается, если разности m и n двух арифметических прогрессий, члены которых – натуральные числа, являются взаимно простыми числами, то пересечение прогрессий – арифметическая прогрессия (и разность прогрессии-пересечения равна mn).

Китайская теорема об остатках. Если a и b – целые числа, m и n – взаимно простые натуральные числа, то пересечение

арифметической прогрессии

$$a, a + m, a + 2m, a + 3m, \dots$$

с арифметической прогрессией

$$b, b + n, b + 2n, b + 3n, \dots$$

является арифметической прогрессией с разностью mn .

Здесь натуральные числа упомянуты по той только причине, что арифметическая прогрессия «направлена в одну сторону». Если вместо прогрессий рассматривать бесконечные в обе стороны последовательности вида

$$\dots, a - 2m, a - m, a, a + m, a + 2m, a + 3m, \dots,$$

в которых соседи отличаются на m , то пересечение такой последовательности (а такие последовательности настолько важны, что получили название *классы вычетов по модулю m*) с последовательностью

$$\dots, b - 2n, b - n, b, b + n, b + 2n, b + 3n, \dots$$

будет (при условии $\text{НОД}(m; n) = 1$) последовательностью того же вида, но с разностью mn (т.е. пересечение класса вычетов по модулю m с классом вычетов по модулю n — класс вычетов по модулю mn).

Другими словами, если знать остаток a от деления целого числа x на m и остаток b от деления числа x на n , то можно, причем единственным образом, найти остаток от деления x на mn . Доказательство китайской теоремы об остатках вы легко проведете самостоятельно.

Упражнение 9 (только для тех, кто любит программировать).

Множество всех целых чисел представило в виде объединения арифметических прогрессий с попарно различными разностями: например, $0 \bmod 2, 0 \bmod 3, 1 \bmod 4, 1 \bmod 6, 11 \bmod 12$.

а) Постройте набор прогрессий, не использующий прогрессию с разностью 2.

б) Постройте набор арифметических прогрессий, разности которых не равны ни 2, ни 3.

Замечание. Придумавший эту задачу П.Эрдёш спросил, для любого ли натурального числа можно придумать такую систему, в которой все модули (разности прогрессий) больше этого числа. Ответ на этот вопрос неизвестен.

Если произведение двух натуральных чисел кратно числу 3, то хотя бы один из множителей делится на 3 без остатка. Этот факт настолько привычен, что многие даже не задумываются о его доказательстве. Между тем – если, конечно, рассматривать делимость не только на 3, но и на любое простое число, – это одно из важнейших свойств натуральных чисел.

Другими словами его можно сформулировать следующим образом. Множители любого натурального числа, представленного в виде произведения простых чисел, можно располагать в каком угодно порядке, и на этом свобода заканчивается: разложение единственно с точностью до порядка множители.

Рассмотрим множество натуральных чисел, оканчивающихся цифрой 1, и будем интересоваться лишь разложениями на множители, тоже оканчивающиеся на 1. Числа 11, 21, 31, 41, ..., ..., 111 разложить не удастся, а $121 = 11 \cdot 11$. Очевидно,

$$(3 \cdot 7)(13 \cdot 17) = (3 \cdot 17)(13 \cdot 7),$$

т.е.

$$21 \cdot 221 = 51 \cdot 91.$$

Числа 21, 221, 51 и 91 не представимы в виде произведения отличных от 1 и оканчивающихся на 1 натуральных чисел. Таким образом, для доказательства единственности разложения на простые множители мы обязаны не только умножать и делить, но и хоть как-то использовать свойства операций сложения или вычитания.

Основная теорема арифметики. *Любое натуральное число либо равно 1, либо простое (т.е. имеет ровно два натуральных делителя – 1 и само себя), либо единственным с точностью до порядка множителей способом разложимо в произведение простых чисел.*

Мы рассмотрим три доказательства. Первое использует идею из «Начал» Евклида. Второе изложено в «Арифметических исследованиях» К.Ф.Гаусса, изданных в 1801 году. Третье на рубеже XIX и XX веков придумал Э. Цермело (1871–1953).

Строго говоря, в «Началах» основная теорема арифметики нигде явно не сформулирована. Но все необходимое для доказательства там есть. «Все необходимое» – это алгоритм Евклида нахождения наибольшего общего делителя двух чисел и (легко получаемое при изучении работы этого алгоритма) утверждение: для любых взаимно простых целых чисел m и n существуют такие целые x и y , что $mx - ny = 1$.

Основная лемма. Если произведение двух натуральных чисел a и b делится на простое число p , то хотя бы одно из чисел a и b делится на p .

Доказательство основной леммы. Пусть a не делится на p . Тогда числа a и p взаимно просты, поэтому для некоторых целых чисел x и y выполнено равенство

$$ax - py = 1.$$

Следовательно,

$$b = abx - pby = p \left(\frac{ab}{p} \cdot x - by \right).$$

Поскольку число $\frac{ab}{p}$ целое, то b делится на p . Основная лемма доказана.

Докажем основную теорему арифметики. Возможность разложения очевидна: берем любое натуральное число и, если оно разложимо, разлагаем на два множителя. Если получили неразложимые сомножители – хорошо. Если хотя бы один из полученных сомножителей можно разложить – разлагаем его! И так действуем до тех пор, пока можно. Бесконечно долго этот процесс не продлится: на каждом шаге числа уменьшаются, а бесконечно долго уменьшать натуральное число, оставаясь во множестве натуральных чисел, невозможно.

Нетривиальную часть основной теоремы арифметики – однозначность разложения – получаем из основной леммы. А именно, пусть число

$$N = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$$

разложено на неразложимые и отличные от 1 множители двумя способами. Тогда произведение $q_1 q_2 \dots q_s$ кратно числу p_1 . В силу основной леммы хотя бы один из множителей q_1, q_2, \dots, q_s кратен p_1 . (Подумайте, почему можно пользоваться утверждением для s множителей, хотя лемму мы доказали только для двух!) Если некоторое неразложимое натуральное число q_k делится на p_1 , то $q_k = p_1$ и обе части равенства можно сократить на p_1 .

«Уничтожив» p_1 , точно так же поступим с p_2, \dots, p_r . Так и получится, что множители левой части разложения числа N могут отличаться от множителей правой части разве лишь порядком, в котором они записаны.

Гаусс доказывает существование разложения на простые множители точно так же, как Евклид, а вот основную лемму — несколько иначе. Пусть произведение некоторых двух натуральных чисел a и b , не делящихся на простое число p , делится на p . Зафиксируем числа a и p , а из всех возможных натуральных чисел b , для которых ab делится на p , выберем *наименьшее*. Очевидно, $b < p$ и число p , будучи простым, не делится на b . Поэтому число p расположено между некоторыми кратными числа b , т.е.

$$mb < p < (m+1)b$$

для некоторого натурального m . Обозначим $c = p - mb$. Очевидно, $0 < c < b$ (заметьте: $c \neq 0$ вследствие простоты числа p). Поскольку $ac = ap - abm$ делится на p , мы получили противоречие: на роль (наименьшего!) числа b претендует число $c < b$.

Цермело доказал единственность разложения следующим образом. Предположим, что существует натуральное число N , которое можно существенно разными способами представить в виде произведения простых чисел:

$$N = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s.$$

Пусть N — *наименьшее* из таких чисел. Тогда ни одно из чисел p_1, \dots, p_r не равно ни одному из чисел q_1, q_2, \dots, q_s (в противном случае мы сократили бы обе части равенства на общий множитель, получив меньшее число).

Обозначим $P = p_2 \dots p_r$ и $Q = q_2 \dots q_s$. Тогда

$$N = p_1 P = q_1 Q.$$

Не ограничивая общности, можно считать, что $p_1 < q_1$. При этом $P > Q$ и, значит, $p_1 Q < N$. Рассмотрим число

$$M = N - p_1 Q.$$

Поскольку $M < N$, число M разлагается на простые множители единственным образом. Но

$$p_1 (P - Q) = M = (q_1 - p_1) q_2 \dots q_s.$$

Левая часть равенства содержит простой множитель p_1 . Поскольку ни одно из чисел q_2, \dots, q_s не равно p_1 , то разность $q_1 - p_1$ делится на p_1 ; следовательно, q_1 делится на p_1 , что противоречит простоте числа q_1 и тому, что $p_1 \neq q_1$.

РЯДЫ ФАРЕЯ

Выписав в порядке возрастания несократимые правильные дроби, знаменатели которых не превосходят некоторого заданного числа n , мы получаем n -й ряд Фарея. В 1816 году француз Огюстен Луи Коши доказал две подмеченные Фареєм интересные закономерности.

• Если $\frac{a}{b} < \frac{c}{d}$ – две последовательные дроби ряда Фарея, то

$$bc - ad = 1.$$

• Если $\frac{a}{b} < \frac{c}{d} < \frac{e}{f}$ – три последовательные дроби ряда

Фарея, то средняя из них – медианта своих сосеждок:

$$\frac{c}{d} = \frac{a+e}{b+f}.$$

Дроби, равноотстоящие от краев ряда Фарея, имеют одинаковые знаменатели. Например (рис.1), в 5-м ряде симметрично

$\frac{0}{1}$																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																														
---------------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Рис.1

расположены относительно $1/2$ следующие пары дробей: $0/1$ и $1/1$, $1/5$ и $4/5$, $1/4$ и $3/4$, $1/3$ и $2/3$, $2/5$ и $3/5$. Более того, симметрично расположенные дроби дополняют одна другую до единицы (т.е. их сумма равна числу 1). Причина очевидна: неравенства $x < y$ и $1 - x > 1 - y$ равносильны.

6-й ряд Фарея отличается от 5-го тем, что добавляются две дроби: $1/6$ и $5/6$. Все другие правильные дроби со знаменателем 6 сократимы: $2/6 = 1/3$, $3/6 = 1/2$ и $4/6 = 2/3$. А вот в 7-м ряду появляются сразу 6 новых дробей. Каждая из них –

медианта дробей, между которыми она заключена: $\frac{1}{7} = \frac{0+1}{1+6}$, $\frac{2}{7} = \frac{1+1}{4+3}$, $\frac{3}{7} = \frac{2+1}{5+2}$, $\frac{4}{7} = \frac{1+3}{2+5}$, $\frac{5}{7} = \frac{2+3}{3+4}$, $\frac{6}{7} = \frac{5+1}{6+1}$.

Второй закон Фарея, как ни странно, следует из первого. А именно, из равенств

$$bc - ad = 1 = de - cf$$

следует равенство $c(b+f) = d(a+e)$, т.е. $\frac{c}{d} = \frac{a+e}{b+f}$.

Прежде чем заняться доказательством первого закона Фарея,

напомню, что *медианта* дробей $\frac{a}{b}$ и $\frac{c}{d}$ – это дробь $\frac{a+c}{b+d}$,

числитель которой равен сумме числителей, а знаменатель – сумме знаменателей. Если числа a , b , c и d положительные и

$\frac{a}{b} < \frac{c}{d}$ медианта $\frac{a+c}{b+d}$ расположена между дробями a/b и c/d .

Это легко доказать алгебраически.

Но есть и красивое геометрическое доказательство (рис. 2). Рассмотрим точки $(b; a)$ и $(d; c)$ и соединим их с началом координат. Тогда a/b и c/d – угловые коэффициенты полученных прямых. Диагональ параллелограмма лежит между его сторонами – это и есть нужное нам утверждение!

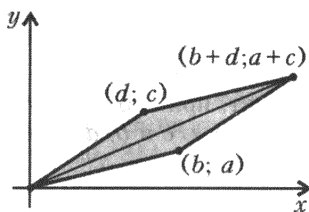


Рис. 2

Теперь **докажем первый закон Фарея** при помощи индукции. **База:** первый ряд Фарея состоит всего лишь из двух дробей $0/1$ и $1/1$, при этом $1 \cdot 1 - 0 \cdot 1 = 1$.

Переход. Предположим, что для некоторого натурального n , где $n > 1$, закон верен для $(n - 1)$ -го ряда Фарея. Чтобы

получить из $(n - 1)$ -го ряда n -й, мы должны добавить дроби вида m/n , где $1 \leq m \leq n$ и $\text{НОД}(m, n) = 1$. Рассмотрим одну из таких дробей m/n и обозначим через a/b и c/d ближайшие к ней слева и справа дроби $(n - 1)$ -го ряда:

$$\frac{a}{b} < \frac{m}{n} < \frac{c}{d}.$$

Теперь – внимание:

$$\begin{aligned} \frac{1}{bd} &= \frac{bc - ad}{bd} = \frac{c}{d} - \frac{a}{b} = \frac{c}{d} - \frac{m}{n} + \frac{m}{n} - \frac{a}{b} = \\ &= \frac{cn - dm}{dn} + \frac{bm - an}{bn} \geq \frac{1}{dn} + \frac{1}{bn} = \frac{b + d}{bdn}, (*) \end{aligned}$$

следовательно, $b + d \leq n$. Если бы это неравенство было строгим, то дробь $\frac{a+c}{b+d}$ – медианта дробей a/b и c/d – лежала бы между ними и принадлежала бы $(n - 1)$ -му ряду Фарея. Но никаких дробей между a/b и c/d в $(n - 1)$ -м ряду Фарея нет. Следовательно, $b + d = n$, а неравенство в формуле $(*)$ – на самом деле равенство. Значит,

$$cn - dm = 1 \text{ и } bm - an = 1.$$

Казалось бы, первый закон Фарея доказан: последние две формулы – это как раз нужные формулы для n -го ряда Фарея. Но... почему мы уверены, что в n -м ряду между дробями a/b и c/d расположена лишь одна дробь со знаменателем n ? Ответить на это возражение можно, например, так: приравняв левые части последних двух равенств, получаем

$$cn - dm = bm - an,$$

откуда $m(b + d) = n(a + c)$. Поскольку $n = b + d$, то $m = a + c$. Значит, при переходе от $(n - 1)$ -го к n -му ряду Фарея между дробями a/c и b/d вставляется одна дробь

$$\frac{m}{n} = \frac{a + c}{b + d}.$$

Доказательство завершено.

Упражнение 1. Натуральные числа q и p взаимно просты. Отрезок $[0; 1]$ разбит на $p + q$ одинаковых отрезков. Докажите, что в каждом из этих отрезков, кроме двух крайних, лежит ровно одно из $p + q - 2$ чисел

$$\frac{1}{p}, \frac{2}{p}, \dots, \frac{p-1}{p}, \frac{1}{q}, \frac{2}{q}, \dots, \frac{q-1}{q}.$$

Какова длина периода десятичного представления дроби $1/7^{77}$? А длина периода суммы двух бесконечных десятичных периодических дробей, длина периода одной из которых равна 6, а другой – 12? В этой статье рассказано о связи между обыкновенными дробями и периодическими десятичными дробями насколько подробно, что вы легко самостоятельно ответите на эти и другие вопросы.

Обыкновенные дроби

Обыкновенная дробь – это число, составленное из целого количества долей единицы. Дробь записывают в виде $\frac{m}{n}$ или m/n , где числитель m – целое число, а знаменатель n – натуральное число. Для получения дроби m/n надо разделить единицу на n равных частей и взять m таких частей. Величина дроби не изменится, если ее числитель и знаменатель умножить на одно и то же натуральное число. Благодаря этому любые две дроби a/b и c/d можно привести к общему знаменателю bd , заменив их на $\frac{ad}{bd}$ и $\frac{bc}{bd}$ соответственно.

Если числитель и знаменатель дроби имеют больший единицы общий делитель, то дробь можно сократить – разделить на него числитель и знаменатель. Вследствие этого всякую дробь можно представить в несократимом виде – в виде дроби, числитель и знаменатель которой взаимно просты. (Числа m и n *взаимно простые*, если единственным их общим делителем является число 1, т.е. если число m не делится ни на один из простых делителей числа n .) Например, $120/344$ – сократимая дробь $\left(\frac{120}{344} = \frac{15 \cdot 8}{43 \cdot 8} = \frac{15}{43}\right)$, а $15/43$ – равная ей несократимая дробь.

Дробь m/n называют *правильной*, если $0 \leq m < n$. Всякую дробь можно единственным образом представить в виде суммы целого числа $[m/n]$ (целой части дроби m/n) и правильной дроби $\{m/n\}$ (дробной части). Например,

$$\frac{91}{17} = \frac{5 \cdot 17 + 6}{17} = 5 + \frac{6}{17}.$$

Сумму и разность дробей с одинаковыми знаменателями определяют по правилам:

$$\frac{a}{n} \pm \frac{b}{n} = \frac{a \pm b}{n}.$$

Чтобы сложить или вычесть дроби a/b и c/d с разными знаменателями, их предварительно приводят к общему знаменателю. В качестве него можно взять наименьшее общее кратное $\text{НОК}[b; d]$ чисел b и d или произведение bd .

От обыкновенной дроби – к десятичной

Нидерландский ученый и инженер Симон Стевин (1548–1620) предложил использовать дроби, знаменатели которых – степени числа 10. Складывать, вычитать и (особенно!) сравнивать их легче, чем обыкновенные дроби. Десятичные дроби обычно пишут без знаменателя, при помощи так называемой десятичной запятой (иногда – не запятой, а точки);

например, $\frac{5481475}{10000} = 548,1475$ и $\frac{23}{1000} = 0,023$.

Как записать обыкновенную дробь m/n в десятичном виде? Если n – степень двойки, степень пятерки или произведение степеней двойки и пятерки, то ответ – конечная десятичная дробь. Например,

$$\frac{13}{64} = \frac{13 \cdot 15625}{64 \cdot 15625} = \frac{203125}{1000000} = 0,203125;$$

$$\frac{3}{25} = \frac{3 \cdot 4}{25 \cdot 4} = 0,12;$$

$$\frac{3}{40} = \frac{3 \cdot 25}{40 \cdot 25} = \frac{75}{1000} = 0,075.$$

Хотя число 35 не является произведением степеней двойки и пятерки, дробь $7/35$ представима в виде конечной десятичной дроби:

$$\frac{7}{35} = \frac{1}{5} = 0,2.$$

Но если дробь m/n несократима и при этом хотя бы один из простых делителей числа n отличен от 2 и 5, то m/n нельзя представить в виде конечной десятичной дроби. В самом деле, если $m/n = a/10^b$, то $10^b m = an$; рассмотрев любой отличный от 2 и 5 простой делитель p числа n и применив основную теорему арифметики, приходим к противоречию: an кратно p , а равное ему число $10^b m$ не кратно.

$$\begin{array}{r} 3 \overline{) 7} \\ \underline{0} \\ 30 \\ \underline{28} \\ 20 \\ \underline{14} \\ 60 \\ \underline{56} \\ 40 \\ \underline{35} \\ 50 \\ \underline{49} \\ 10 \\ \underline{7} \\ 3 \end{array}$$

$$10 = 1 \cdot 7 + 3.$$

Puc. 1

$$\frac{3}{7} = 0,428571428571428571\dots$$

Если повторяющаяся группа цифр (период) расположена непосредственно после запятой, то такую десятичную дробь называют *чисто периодической*; в противном случае говорят, что дробь имеет *предпериод* и называют ее *смешанной периодической*.

Доказательство. Чтобы получить первую цифру после запятой, мы приписываем к t нуль (т.е. умножаем t на 10) и делим (с остатком) полученное число на n . Вообще весь процесс деления уголком – повторяемое вновь и вновь умножение очередного остатка на 10 и деление (с остатком) на n .

Если на каком-то шаге получится нулевой остаток, то дробь – конечная. Конечную дробь, приписав к ней справа бесконечно много нулей, естественно считать периодической с периодом

длины 1. По условию, $1 \leq n - 1$, так что в этом случае утверждение теоремы выполнено.

Если же процесс деления никогда не закончится, то будут получаться только ненулевые остатки – числа от 1 до $n - 1$. Значит, не позже чем на n -м шаге остаток повторится. С этого момента процесс деления заикнется, что и требовалось доказать.

Упражнения

1. Убедитесь, что а) $1/3 = 0,(3)$, б) $1/6 = 0,1(6)$; в) $7/30 = 0,2(3)$, г) $7/11 = 0,(63)$

2. Найдите сотую цифру после запятой в десятичной записи числа $1/7$.

3. Разделите «уголком» число 1 на а) 9, б) 99, в) 9999999.
г) Докажите общее правило: $1/\underbrace{99\dots9}_n = 0,(\underbrace{0\dots01}_{n-1})$.

4. Проверьте равенства. а) $0,(6) + 0,(5) = 1,(2)$; б) $0,(845) + 0,(49) = 1,(340795)$; в) $2,70(584) + 6,917(49) = 9,623(340795)$

От периодической десятичной дроби – к обыкновенной

Пусть

$$x = 0,11111\dots$$

Тогда

$$10x = 1,1111\dots,$$

откуда $10x = 1 + x$, т.е. $x = 1/9$. Мы получили замечательный результат:

$$0,11111\dots = 1/9.$$

Это равенство не приближенное, а *точное*: бесконечная десятичная периодическая дробь $0,(1)$ является в точности тем же самым числом, что и обыкновенная дробь $1/9$. (Между прочим, равенство $0,999\dots = 1$ тоже абсолютно точное!)

Далее, пусть

$$y = 0,17331733173317331733\dots$$

Тогда

$$10000y = 1733,1733173317331733\dots,$$

откуда

$$10000y = 1733 + 0,1733173317331733\dots = 1733 + y.$$

Из уравнения

$$10000y = 1733 + y$$

находим $9999y = 1733$, т.е. $y = 1733/9999$.

Если провести вычисления не для частных примеров, как это сделали мы, а в общем виде, то можно установить следующее правило:

Чисто периодическая правильная дробь равна обыкновенной дроби, в числителе которой – период, а в знаменателе – число $10^r - 1 = \underbrace{9 \dots 9}_r$, где r – длина периода.

Упражнения

5. Обратите в десятичные дроби числа: а) $23/99$; б) $1234/999999$

6. Обратите в обыкновенные дроби числа: а) $0,(012)$; б) $3,1(3)$; в) $1,93(173)$.

7. Докажите, что сумма (произведение, разность) двух периодических десятичных дробей – периодическая дробь.

8. Цифры любой бесконечной десятичной непериодической дроби можно переставить так, что получится периодическая дробь. Докажите это.

Предпериод

Если делить «уголком» 3 на 14, то заикливание произойдет не сразу:

$$3/14 = 0,2(142857).$$

Период, заметьте, такой же, как у дроби $1/7$. Это легко объяснить:

$$\frac{3}{14} = \frac{30}{14} : 10 = \frac{15}{7} : 10 = \left(2 + \frac{1}{7}\right) : 10,$$

а делить на 10 очень легко: достаточно перенести запятую на одну позицию.

В общем случае выделим в знаменателе степени двойки и пятерки – запишем дробь в виде $m/(2^a 5^b k)$, где a, b – неотрицательные целые числа, k – натуральное число, не кратное ни 2, ни 5. Обозначим наибольшее из чисел a, b буквой c и выполним преобразование:

$$\frac{m}{2^a 5^b k} = \frac{m \cdot 2^c \cdot 5^c}{2^a 5^b k} : 10^c = \frac{m \cdot 2^{c-a} 5^{c-b}}{k} : 10^c.$$

Значит, для решения вопроса о длинах периодов десятичных дробей достаточно изучить дроби со знаменателями, не кратными ни 2, ни 5 – со знаменателями, взаимно простыми с числом 10.

Упражнения

9. Зная, что $1/13 = 0,(076923)$, запишите в виде обыкновенной дроби бесконечную периодическую дробь $0,(692307)$.

10. Зная, что $7/17 = 0,(4117647058823529)$, обратите в десятичные дроби числа: а) $12/85$; б) $3/68$.

11*. Если в периоде десятичного представления дроби m/n , где m и n — натуральные числа, есть последовательность цифр 167, то $n > 100$. Докажите это.

Числа вида 99...9

Взглянем еще раз на равенства $\frac{1}{7} = 0,(142857)$ и $\frac{1}{13} = 0,(076923)$. Заметьте:

$$142857 \cdot 7 = 999999$$

и

$$76923 \cdot 13 = 999999.$$

Это не случайность: в правиле преобразования чисто периодической дроби в обыкновенную фигурирует число $10^r - 1 = \underbrace{9 \dots 9}_r$.

Лемма 1. Для всякого натурального числа k , не кратного ни 2, ни 5, существует такое натуральное число r , что разность $10^r - 1$ кратна k .

Доказательство. Рассмотрим k чисел: 9, 99, 999, ..., $\underbrace{99 \dots 9}_k$.

Докажем, что хотя бы одно из них кратно k . Предположим противное: пусть ни одно из них не кратно k . Поскольку количество ненулевых остатков от деления на k равно $k - 1$, какие-то два из k рассматриваемых чисел дают одинаковые остатки при делении на k . Разность этих чисел делится на k и представляет из себя несколько девяток, после которых написано несколько нулей:

$$\underbrace{99 \dots 9}_{r+s} - \underbrace{99 \dots 9}_s = \underbrace{99 \dots 9}_r \underbrace{00 \dots 0}_s.$$

Поскольку k взаимно просто с 10, из делимости числа $\underbrace{99 \dots 9}_r \underbrace{00 \dots 0}_s$ на k следует, что число $\underbrace{99 \dots 9}_r$ делится на k .

Это доказательство можно изложить и следующим образом. Рассмотрим k чисел: $1, 10, 10^2, \dots, 10^{k-1}$. Ни одно из них не кратно k . Поскольку количество ненулевых остатков от деления на k равно $k - 1$, какие-то два из k рассматриваемых чисел дают одинаковые остатки при

делении на k . Разность этих чисел $10^{r+s} - 10^s$, где $0 \leq s < r+s < k$, делится на k .

Из делимости числа $10^{r+s} - 10^s = 10^s(10^r - 1)$ на k и из взаимной простоты чисел 10 и k следует, что $10^r - 1$ кратно k , т.е. $10^r - 1 = kt$, где t – натуральное число. (Например, для $k = 7$ можно взять $r = 6$; при этом $t = (10^6 - 1)/7 = 142857$.)

Упражнения

12 (M206). Дана бесконечная последовательность цифр. Докажите, что для любого натурального числа n , взаимно простого с числом 10 , можно указать такую группу стоящих подряд цифр последовательности, что записываемое этими цифрами число делится на n .

13. Сколько чисел, кратных 13 , имеется среди первых ста чисел последовательности $1, 11, 111, 1111, \dots$?

14. Если число вида $11\dots 11$ кратно 7 , то оно кратно и 11 , и 13 , и 15873 . Докажите это.

15. Первую цифру k -значного числа, кратного 13 , стерли и записали позади последней цифры этого числа. При каких k полученное число кратно 13 ? (Например, из чисел 503906 и 7969 , кратных 13 , таким образом получаем числа 39065 и 9697 , первое из которых кратно 13 , а второе – нет.)

16. Для каких пар натуральных чисел $(m; n)$, где $n > 1$, число $\underbrace{100\dots 01}_m$ кратно числу $\underbrace{11\dots 1}_n$?

17. а) Если p – простое число, а наименьший период десятичного разложения дроби $1/p$ состоит из $2n$ цифр, то сумма двух n -значных чисел (могущих начинаться и с нуля), образованных первыми n и последними n цифрами периода, равна $10^n - 1$. Докажите это. (Например, $1/13 = 0,(076923)$, при этом $76 + 923 = 999$. Простота знаменателя существенна: $1/21 = 0,(047619)$, но $47 + 619 \neq 999$.)

б) Длина наименьшего периода десятичного представления дроби $1/p$, где p – простое число, четна в точности тогда, когда p является делителем некоторого числа вида $10^n + 1$. Докажите это.

18. а) Найдите длину наименьшего периода десятичного представления дроби $1/31$. **б)** Существует ли число вида $100\dots 01$, кратное 31 ?

19 (M981). Число $11\dots 1$ (1986 единиц) имеет по крайней мере а) 8 ; б) 128 ; в) 1024 различных делителей. Докажите это.

Длина периода

Теорема 2. Если m, k – взаимно простые натуральные числа, причем k взаимно просто с 10 и $m < k$, то десятичное представление дроби m/k является чисто периодической дробью. Длина ее наименьшего периода – это такое наименьшее натуральное число r , что $10^r - 1$ кратно k .

Доказательство. По лемме 1, $10^r - 1 = kt$ для некоторых натуральных чисел r и t . Следовательно,

$$\frac{m}{k} = \frac{mt}{kt} = \frac{mt}{10^r - 1}.$$

Воспользовавшись равенством $1 / (10^r - 1) = 0, \underbrace{(0 \dots 01)}_{r-1}$, получаем:

$$\frac{m}{k} = mt \cdot 0, \underbrace{(0 \dots 01)}_{r-1}.$$

Поскольку $m < k$, то $mt < kt < 10^r$, так что произведение числа mt на число $0, \underbrace{(0 \dots 01)}_{r-1}$ — это периодическая дробь, длина периода которой равна r , а период — десятичная запись числа mt , возможно дополненная слева необходимым количеством нулей.

Осталось понять, почему *наименьшему* возможному числу r соответствует *наименьший* возможный период. Это очевидно из правила перевода периодической десятичной дроби в обыкновенную.

Следствие теоремы 2. Длиной наименьшего периода десятичного представления несократимой дроби m/n , где $n = 2^a 5^b k$, причем $a, b \geq 0$ и $\text{НОД}(k; 10) = 1$, является такое наименьшее натуральное число r , что $10^r - 1$ кратно k .

Следствие следствия теоремы 2. Длина наименьшего периода десятичного представления несократимой дроби m/n зависит только от знаменателя n , а не от числителя m .

Функция $L(n)$

Обозначим через $L(n)$ длину наименьшего периода десятичного представления дроби $1/n$. Функция L определена на всем множестве натуральных чисел, но в силу теоремы 2 и следствия из нее интерес представляют только числа, взаимно простые с числом 10.

Таблица 1

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$L(n)$	1	1	1	1	1	1	6	1	1	1	2	1	6	6	1	1	6

Теорема 3. Если m, n — взаимно простые натуральные числа, то $L(mn) = \text{НОК}[L(m); L(n)]$.

Идея доказательства. Если $10^r - 1$ кратно каждому из двух взаимно простых натуральных чисел m и n , то $10^r - 1$ кратно и произведению mn .

Упражнения

20. Найдите длину наименьшего периода дроби: а) $19/42$;
б) $2000/(3 \cdot 7 \cdot 11 \cdot 13 \cdot 13)$

21 (М1399). Какой может быть длина периода суммы двух бесконечных десятичных периодических дробей, длины периодов которых равны: а) 6 и 12; б) 12 и 20?

в) Для любых двух натуральных чисел r и s через $f(r, s)$ обозначим произведение таких степеней p^a простых чисел, для которых ровно одно из чисел r, s кратно p^a и не кратно при этом степени p^{a+1} , а другое из чисел r, s не кратно числу p^a . (Например, $f(2^3 \cdot 3 \cdot 11^6, 2^4 \cdot 3 \cdot 11^2 \cdot 23) = 2^4 \cdot 11^6 \cdot 23$.) Докажите, что числу $f(r, s)$ кратна длина t наименьшего периода суммы любых двух десятичных дробей, длины наименьших периодов которых равны r и s .

г) Пусть r, s, t – натуральные числа, причем t кратно числу $f(r, s)$ и является делителем числа $\text{НОК}[r; s]$. Докажите существование двух десятичных периодических дробей, длины наименьших периодов которых равны r и s соответственно, а длина наименьшего периода суммы этих дробей равна t .

Наблюдения Гаусса

Великий немецкий математик Карл Фридрих Гаусс, будучи гимназистом, обращал дроби вида $1/p$, где p – простое число, отличное от 2 и 5, в бесконечные десятичные дроби: в каждом случае он с поразительным терпением ожидал, когда знаки начнут повторяться. Ему хотелось понять, как зависит длина периода такой дроби от p .

Выписывание полного периода, скажем, для $p = 47$ – утомительное занятие (46 знаков!). Однако Гаусс не терял надежды и продолжал вычисления: он выписал периоды для всех простых чисел $p < 1000$. Главная закономерность, которую он обнаружил, состоит в том, что длина $L(p)$ наименьшего периода такой дроби является делителем числа $p - 1$, иногда совпадая с ним. А именно, $L(p) = p - 1$ для $p = 7, 17, 23, 47, 59, 61, 97, 109, 113, 131, 149, 167, 179, 181, 193$ и некоторых других чисел. (Конечно или бесконечно множество чисел, для которых $L(p) = p - 1$, по сей день неизвестно. Это частный случай гипотезы Артино, о которой рассказано в статье «Малая теорема Ферма».)

Таблица 2

p	3	7	11	13	17	19	23	29	31	37	41	43	47
$L(p)$	1	6	2	6	16	18	22	28	15	3	5	21	46

Чтобы понять причину такого явления, рассмотрим следующие разложения:

$$1/7 = 0,(142857),$$

$$2/7 = 0,(285714),$$

$$3/7 = 0,(428571),$$

$$4/7 = 0,(571428),$$

$$5/7 = 0,(714285),$$

$$6/7 = 0,(857142).$$

Периоды этих шести дробей начинаются сразу после запятой и получаются друг из друга циклическим сдвигом.

Возьмем вместо 7 число 41. Очевидно, $1/41 = 0,(02439)$.

«Прокрутим» период:

$$0,(24390) = 10/41,$$

$$0,(43902) = 10 \cdot 0,(24390) - 2 = \frac{100}{41} - 2 = 18/41,$$

$$0,(39024) = 10 \cdot 0,(43902) - 4 = \frac{180}{41} - 4 = 16/41,$$

$$0,(90243) = 10 \cdot 0,(39024) - 3 = \frac{160}{41} - 3 = 37/41.$$

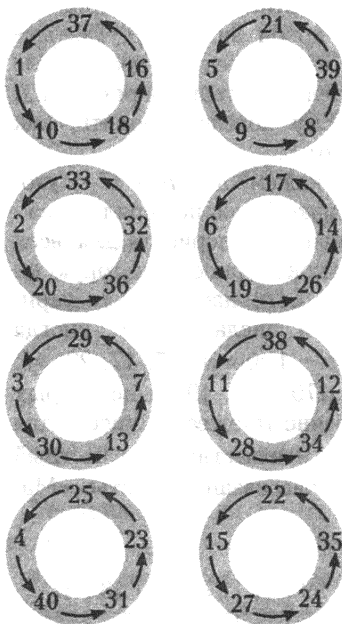


Рис. 2

Получили цикл из пяти чисел: 1, 10, 18, 16, 37. Каждое число этого цикла – остаток от деления удвоенного предыдущего на 41.

Начав с $2/41 = 0,(04878)$, получаем другой цикл: $0,(48780) = 20/41$, $0,(87804) = 36/41$, $0,(78048) = 32/41$, $0,(80487) = 33/41$. Всего для $p = 41$ получаем 8 циклов, по 5 дробей в каждом (рис.2).

В общем случае, если натуральное число n взаимно просто с 10 и отлично от 1, то все правильные несократимые дроби со знаменателем n разбиваются на циклы по $L(n)$ дробей в каждом цикле. Значит, количество таких дробей кратно числу $L(n)$. В частности, если p – простое число, то все дроби вида

m/p , где $1 \leq m < p$, – несократимые, откуда и следует обнаруженная юным Гауссом закономерность.

Упражнения

22. а) Решите ребус ПЛОМБА 5 = АПЛОМБ. (Здесь в записях шестизначных чисел ПЛОМБА и АПЛОМБ разные буквы обозначают разные цифры.)

б) Найдите шестизначное число, уменьшающееся в 5 раз при переносе первой цифры в конец числа.

в) Решите ребус НИКЕЛЬ 6 = ЕЛЬНИК.

г) Существует ли шестизначное число, которое при умножении на 2, 3, 4, 5 и 6 дает числа, записанные теми же цифрами, что и само число, но в другом порядке?

д) Найдите все шестизначные числа, которые увеличиваются в целое число раз при переносе последней цифры из конца в начало.

23. Пятизначное число делится на 41. Докажите, что если его цифры циклически переставить, то полученное число тоже будет делиться на 41.

24. Число оканчивается на 2. Если эту цифру перенести в начало числа, оно удвоится. Найдите наименьшее такое число.

25 (M1252). Пусть a и n – натуральные числа, $a > 1$. Докажите, что количество правильных несократимых дробей со знаменателем $a^n - 1$ кратно n .

Теорема Эйлера

Количество правильных несократимых дробей со знаменателем n обозначают через $\varphi(n)$. Для любого простого числа p , очевидно, $\varphi(p) = p - 1$.

Таблица 3

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$\varphi(n)$	1	1	2	3	4	2	6	4	6	4	10	4	12	6	8	8	16

Поскольку $\varphi(n)$ правильных несократимых дробей можно разбить на циклы по $L(n)$ дробей в каждом цикле, то $\varphi(n)$ кратно числу $L(n)$. Если натуральное число n взаимно просто с числом 10, то $10^{\varphi(n)} - 1$ кратно n .

Если бы мы рассматривали не десятичную систему счисления, а систему счисления с основанием a , где a – отличное от единицы натуральное число, то аналогичным образом получили бы утверждение, которое называют теоремой Эйлера: *если n – натуральное число, взаимно простое с целым числом a , где $a > 1$, то $a^{\varphi(n)} - 1$ кратно n* . Честно говоря, условие $a > 1$

излишне: если нас интересуют остатки от деления на n , то из любого целого числа a , прибавив к нему n необходимое количество раз, можно получить число, большее единицы.

Функция $L(p^m)$

Число 111 делится на 3. Число $111111111 = 111 \cdot 1001001$ делится на 9 как произведение двух чисел, каждое из которых делится на 3. Записываемое 27 единицами число

$$111111111111111111111111 =$$

$$= 11111111 \cdot 1000\,000\,001\,000\,000\,001$$

делится на 27 как произведение числа, кратного 9, и числа, кратного 3. И вообще, равенство

$$\underbrace{111\dots 11}_{3^n} \underbrace{111\dots 11}_{3^n} \underbrace{111\dots 11}_{3^n} = \underbrace{111\dots 11}_{3^n} \cdot 1 \underbrace{00\dots 00}_{3^n-1} 1 \underbrace{00\dots 00}_{3^n-1}$$

показывает, что если число, записываемое 3^n единицами, кратно 3^n , то число, записываемое 3^{n+1} единицами, кратно 3^{n+1} .

Таким образом по индукции можно доказать, что число $\frac{11\dots 11}{3^n}$ кратно числу 3^n , т.е. число $\frac{99\dots 99}{3^n}$ кратно числу 3^{n+2} , откуда $L(3^{n+2}) \leq 3^n$. А если мы еще заметим, что использованные нами числа $\frac{100\dots 00}{3^{n-1}} \frac{100\dots 00}{3^{n-1}}$ делятся только на 3, но не на 9, то получим точный результат: $L(3^{n+2}) = 3^n$.

Давайте примерно тем же способом изучим свойства величин $L(p^m)$, где p – простое число, отличное от 2 и 5, m – натуральное число.

Теорема 4. Если p – простое число, отличное от 2 и 5, причем p^k – наивысшая степень простого числа p , которой кратно число $10^{L(p)} - 1$, то $L(p^{k+m}) = p^m L(p)$ для любого неотрицательного целого числа m . (Например, $L(3^{m+2}) = 3^m$, $L(7^{m+1}) = 6 \cdot 7^m$ и $L(11^{m+1}) = 2 \cdot 11^m$.)

Лемма 2. Если $a = 1 + pb$, где p – простое число, $p > 2$, b – целое число, то сумма $a^{p-1} + a^{p-2} + \dots + a + 1$ кратна p , но не кратна p^2 .

Доказательство леммы 2. Легко понять (рассуждая по индукции или применив бином Ньютона), что при делении на r^2

числа a, a^2, \dots, a^{p-2} и a^{p-1} дают такие же остатки, как $1 + pb$, $1 + 2pb$, ..., $1 + (p-2)pb$ и $1 + (p-1)pb$. Следовательно,

$$1 + a + a^2 + \dots + a^{p-2} + a^{p-1} \equiv$$

$$\begin{aligned} &\equiv 1 + (1 + pb) + (1 + 2pb) + \dots + (1 + (p-2)pb) + (1 + (p-1)pb) = \\ &= p + pb \frac{p(p-1)}{2} \equiv p \pmod{p^2}. \end{aligned}$$

Лемма доказана.

Докажем теорему 4 по индукции. **База** ($m = 0$) очевидна. **Индукционный переход** выполним при помощи леммы 2. Обозначим $r = L(p^{k+m}) = p^m L(p)$ и рассмотрим разложение на множители:

$$10^{qr} - 1 = (10^r - 1) \left((10^r)^{q-1} + (10^r)^{q-2} + \dots + 10^r + 1 \right),$$

где q — натуральное число. Первый множитель правой части этого равенства кратен p^{k+m} и не кратен p^{k+m+1} . Каждое слагаемое второго множителя дает остаток 1 при делении на p . Поэтому если q не кратно p , то второй множитель не кратен p . Если же $q = p$, то второй множитель, в силу леммы 2, кратен p , но не кратен p^2 . Таким образом, в разложение числа $10^{qr} - 1$ на простые множители число p входит в $(k + m + 1)$ -й степени. Это и требовалось доказать.

Упражнения

26. Какое наименьшее количество единиц подряд надо написать, чтобы получилось число, кратное: а) 999999999; б) 9^9 ; в) 11^{11} , г) $3^k 7^l$, где k, l — натуральные числа?

27. На какую наибольшую степень двойки делится число $5^{2000} - 1$?

28. Если p — простое число, $p \neq 2$, то сумма $1 + a + a^2 + \dots + a^{p-1}$ не кратна p^2 ни для какого целого числа a . Докажите это.

29* (M1280). В периоде бесконечной десятичной дроби $1/3^{100}$ имеется любая последовательность из 46 цифр. Докажите это.

30 (M792). а) Ни при каком нечетном $p > 3$ и натуральном $m > 1$ ни одно из чисел $p^m + 1$ и $p^m - 1$ не может быть степенью двойки. Докажите это.

б) Найдите все натуральные n , при которых оба числа $1/n$ и $1/(n+1)$ выражаются конечными десятичными дробями.

Решите в натуральных числах уравнения в) $3^x + 1 = 2^y$; г) $3^x - 1 = 2^y$.

31. (Только для тех, кто любит программировать.) а) Найдите такое простое число $p > 5$, что длины периодов разложений в десятичные дроби чисел $1/p$ и $1/p^2$ совпадают и равны $p-1$. б) Найдите еще одно такое простое число.

*Жил на свете великий Ферма,
Математиков сведший с ума.
Эти жертвы науки –
Каждый день по три штуки –
В сумасшедшие едут дома.*

А.Котова

Часть I. Примеры и три доказательства

Теорема, открытая советником парламента Тулузы (Франция) Пьером Ферма (1601–1665) в 1640 году, формулируется очень коротко: *если p – простое число, a – целое число, то $a^p - a$ кратно p* . Сразу и не видно, почему такое скромное с виду утверждение столь важно. Тем не менее, оно заслуживает величайшего внимания.

Эта статья насыщена задачами и упражнениями. Вряд ли возможно при первом чтении решить их все. Но мы уверены: многие из них настолько заинтригуют вас, что рано или поздно будут решены – самостоятельно или с помощью раздела «Ответы, указания, решения».

Частные случаи

Если из книги вытекает какой-нибудь поучительный вывод, он должен получаться помимо воли автора, в силу самих изображенных фактов.

Ги де Мопассан

Из любых двух последовательных целых чисел a и $a + 1$ одно четное, а другое нечетное. Поэтому произведение $a(a + 1) = a^2 + a$ четно при любом целом a .

Делимость числа $a^2 + a$ на 2 можно доказать и по-другому, разобрав два случая:

– если a четно, то a^2 тоже четно, а сумма двух четных чисел a и a^2 четна;

– если a нечетно, то a^2 тоже нечетно, а сумма двух нечетных чисел a и a^2 четна.

Вот так доказывают замечательное свойство многочлена $a^2 + a$. Впрочем, при $p = 2$ в малой теореме Ферма фигурирует другой многочлен: $a^2 - a = (a - 1)a$. Все его значения в целых точках – четные числа (докажите!).

Теперь рассмотрим многочлен $a^3 - a$. Его легко разложить на множители:

$$a^3 - a = a(a^2 - 1) = a(a - 1)(a + 1).$$

Получили произведение трех последовательных целых чисел: $a - 1$, a и $a + 1$. Как мы уже знаем, это произведение четно. Поскольку из любых трех последовательных чисел одно кратно 3, их произведение $(a - 1)a(a + 1) = a^3 - a$ кратно 3 (и, значит, даже кратно 6).

Упражнение 1. При любом целом a сумма $a^3 + 5a$ кратна 6. Докажите это.

Многочлен $a^4 - a$ при $a = 2$ и $a = 3$ принимает значения $2^4 - 2 = 14$ и $3^4 - 3 = 78$. Конечно, эти значения четны, но никакого общего делителя кроме 2 (и 1) у них нет. Не повезло! Впрочем, число 4 составное, а малая теорема Ферма говорит только о многочленах вида $a^p - a$, где p – простое число.

Пусть $p = 5$. Вычислим несколько значений многочлена $a^5 - a$. При $a = \pm 1$ и при $a = 0$ получаем ноль. Смотрим дальше: $2^5 - 2 = 30$, $3^5 - 3 = 240$, $4^5 - 4 = 1020$, $5^5 - 5 = 3120$, $6^5 - 6 = 7770, \dots$ Все эти значения кратны числу 30.

Поскольку $30 = 2 \cdot 3 \cdot 5$, доказательство делимости на 30 распадается на три части: во-первых, надо доказать, что $a^5 - a$ кратно 2; во-вторых, $a^5 - a$ кратно 3; в-третьих, $a^5 - a$ кратно 5.

Первая часть очевидна: числа a^5 и a либо оба четны, либо оба нечетны. Не вызывает затруднений и вторая часть:

$$a^5 - a = a(a^4 - 1) = a(a^2 - 1)(a^2 + 1) = (a - 1)a(a + 1)(a^2 + 1),$$

произведение трех последовательных чисел всегда кратно 3.

Чуть сложнее третья часть. Нет, конечно, из пяти последовательных целых чисел обязательно одно кратно 5, так что произведение $(a - 2)(a - 1)a(a + 1)(a + 2)$ кратно 5. Но $a^2 + 1 \neq (a - 2)(a + 2)$.

Как же быть? Самый бесхитростный способ – перебрать все подряд остатки от деления на 5: любое целое число при делении на 5 дает в остатке 0, 1, 2, 3 или 4. Если остаток равен 0, то кратен 5 второй множитель произведения $(a - 1)a(a + 1)(a^2 + 1)$. Если

остаток равен 1 или 4, то кратен 5 первый или третий множитель. Если же остаток равен 2 или 3, то в дело вступает четвертый множитель. (Для тех, кто еще не привык работать с остатками, объясним: если $a = 5b + 2$, т. е. если a дает остаток 2 при делении на 5, то $a^2 + 1 = (5b + 2)^2 + 1 = 5(5b^2 + 4b + 1)$. Аналогично можно рассмотреть случай $a = 5b + 3$.)

Есть и другой способ:

$$a^2 + 1 = (a - 2)(a + 2) + 5,$$

значит, если нас интересуют только остатки от деления на 5, то $a^2 + 1$ можно-таки заменить на $(a - 2)(a + 2)$. Формулой это записывают так:

$$a^2 + 1 \equiv (a - 2)(a + 2) \pmod{5}.$$

Предложенное в 1801 году К. Ф. Гауссом обозначение « \equiv » еще не раз будет использовано нами. По определению, a сравнимо с b по модулю n , если $a - b$ кратно n , т. е. если $a - b = kn$, где k — целое число.

Обозначение

$$a \equiv b \pmod{n}$$

оказалось удачным потому, что свойства сравнений похожи на свойства обычных равенств. Сравнения можно складывать: если $a \equiv b \pmod{n}$ и $c \equiv d \pmod{n}$, то $a + c \equiv b + d \pmod{n}$. В самом деле, по определению, $a = b + kn$ и $c = d + ln$, где k, l — целые числа. Значит,

$$a + c = (b + kn) + (d + ln) = b + d + (k + l)n,$$

что и требовалось.

Аналогично, формулы

$$a - c = (b + kn) - (d + ln) = b - d + (k - l)n,$$

$$ac = (b + kn)(d + ln) = bd + knd + bln + kln^2 =$$

$$= bd + (kd + bl + kln)n$$

позволяют утверждать, что сравнения можно вычитать и умножать. Если можно умножать, то можно и возводить в степень: если $a \equiv b \pmod{n}$, то для любого натурального числа m верно сравнение $a^m \equiv b^m \pmod{n}$.

Сокращать сравнения надо с осторожностью:

$$6 \equiv 36 \pmod{10},$$

но

$$1 \not\equiv 6 \pmod{10}.$$

Упражнения

2. Решите сравнение $3x \equiv 11 \pmod{101}$.

3. Какие целые числа x удовлетворяют сравнению $14x \equiv 0 \pmod{12}$?

4. Пусть $k \neq 0$. Докажите, что а) если $ka \equiv kb \pmod{kn}$, то $a \equiv b \pmod{n}$;

б) если $ka \equiv kb \pmod{n}$ и числа k, n взаимно просты, то $a \equiv b \pmod{n}$.

Продолжим изучение многочленов вида $a^p - a$: докажем, что при любом целом a число $a^7 - a$ кратно 7. Как всегда, можно рассмотреть все 7 остатков от деления на 7: $0^7 - 0 = 0$, $1^7 - 1 = 0$, $2^7 - 2 = 126 = 7 \cdot 18, \dots$, $6^7 - 6 = 279930 = 7 \cdot 39990$. (Можно и чуточку сэкономить: поскольку любое целое число представимо в виде $a = 7b, 7b \pm 1, 7b \pm 2$ или $7b \pm 3$, очевидно, при проверке малой теоремы Ферма для $p = 7$ можно ограничиться рассмотрением случаев $a = 0, 1, 2$ и 3.)

Но бездумная проверка не может научить нас ничему интересному. Лучше рассмотрим разложение на множители:

$$\begin{aligned} a^7 - a &= a(a^6 - 1) = \\ &= a(a^3 - 1)(a^3 + 1) = a(a - 1)(a^2 + a + 1)(a + 1)(a^2 - a + 1). \end{aligned}$$

Поскольку

$$a^2 + a + 1 = (a^2 + a - 6) + 7 \equiv a^2 + a - 6 = (a - 2)(a + 3) \pmod{7}$$

и

$$a^2 - a + 1 \equiv a^2 - a - 6 = (a + 2)(a - 3) \pmod{7},$$

имеем:

$$a^7 - a \equiv a(a - 1)(a - 2)(a + 3)(a + 1)(a + 2)(a - 3) \pmod{7}.$$

Произведение семи последовательных целых чисел кратно 7.

Упражнение 5. Докажите, что а) наибольший общий делитель чисел вида $a^7 - a$ равен 42; б) наибольший общий делитель чисел вида $a^9 - a$ равен 30. (Заметьте: 30 не кратно 9. Это находится в согласии с тем, что число 9 не простое, а составное.)

Теперь рассмотрим число $p = 11$. Очевидно,

$$\begin{aligned} a^{11} - a &= a(a^{10} - 1) = a(a^5 - 1)(a^5 + 1) = \\ &= a(a - 1)(a^4 + a^3 + a^2 + a + 1)(a + 1)(a^4 - a^3 + a^2 - a + 1). \end{aligned}$$

Тут не так-то просто догадаться, как быть дальше. Но полный перебор всех 11 остатков все еще возможен. И когда мы его

выполним, окажется, что значения многочлена $a^4 + a^3 + a^2 + a + 1$ кратны 11 при $a \equiv 3, 4, 5$ или $9 \pmod{11}$, а значения многочлена $a^4 - a^3 + a^2 - a + 1$ кратны 11 при $a \equiv 2, 6, 7$ или 8 .

Между прочим, если мы раскроем скобки в произведении $(a - 3)(a - 4)(a - 5)(a - 9)$, получим

$$\begin{aligned} (a^2 - 7a + 12)(a^2 - 14a + 45) &\equiv (a^2 + 4a + 1)(a^2 - 3a + 1) = \\ &= a^4 + a^3 - 10a^2 + a + 1 \equiv a^4 + a^3 + a^2 + a + 1 \pmod{11}. \end{aligned}$$

Аналогично можно проверить, что $(a - 2)(a - 6)(a - 7)(a - 8) \equiv a^4 - a^3 + a^2 - a + 1 \pmod{11}$.

Что дальше? При $p = 13$, если действовать нашим способом, придется возводить в двенадцатую степень числа от 1 до 12 или раскрывать скобки в произведении тринадцати множителей: $a - 6, a - 5, \dots, a + 5, a + 6$. Заниматься этим не хочется, даже если ограничиться возведением в степень чисел 1, 2, 3, 4, 5, 6 или перемножать «всего лишь» шесть скобок: $(a^2 - 1)(a^2 - 4)(a^2 - 9)(a^2 - 16)(a^2 - 25)(a^2 - 36)$.

Чем больше p , тем больше вариантов надо перебирать. Поэтому мы прекратим разбор частных случаев и перейдем к доказательству малой теоремы Ферма, которое охватывает сразу все простые числа p .

Упражнения

6. Докажите следующие утверждения. а) Произведение любых четырех последовательных целых чисел кратно 24. б) Произведение любых пяти последовательных целых чисел кратно 120. в) $a^5 - 5a^3 + 4a$ при всяком целом a кратно 120.

7. Для любого натурального a число a^5 оканчивается на ту же цифру, что и a . Докажите это.

8. Докажите, что $m^5n - mn^5$ кратно 30 при любых целых m и n .

9. Если число k не кратно ни 2, ни 3, ни 5, то $k^4 - 1$ кратно 240. Докажите это.

10. Докажите, что $2222^{5555} + 5555^{2222}$ кратно 7.

11. Докажите, что число $11^{10} - 1$ оканчивается на два нуля (т.е. кратно 100).

12. а) Найдите все целые числа a , для которых $a^{10} + 1$ оканчивается цифрой ноль. б) Докажите, что ни при каком целом a число $a^{100} + 1$ не оканчивается цифрой ноль.

13. Пусть n — четное число. Найдите наибольший общий делитель чисел вида $a^n - a$, где a — целое число.

14. Пусть n — натуральное число, $n > 1$. Докажите, что наибольший общий делитель чисел вида $a^n - a$, где a пробегает множество всех

целых чисел, совпадает с наибольшим общим делителем чисел вида $a^n - a$, где $a = 1, 2, 3, \dots, 2^n$. (Заметьте: из этого следует, что наибольший общий делитель чисел вида $a^n - a$, где a – целое, совпадает с наибольшим общим делителем чисел такого вида, где a – натуральное.)

Общий случай

И каждого в свою уложат яму.

Эжен Гильвик

Выпишем в строчку числа $1, 2, 3, \dots, p - 1$, домножим каждое из них на k , где k не кратно p , и рассмотрим остатки от деления на p . Например, при $p = 19$ и $k = 4$ получим таблицу 1. В нижней строке таблицы – те же самые числа, что и в верхней, только они расположены в другом порядке! Оказывается, это общий закон: не только при $p = 19$ и $k = 4$, но *при любом простом p и не кратном p целом числе k всегда получатся те же самые числа $1, 2, 3, \dots, p - 1$, возможно, записанные в некотором другом порядке.*

Таблица 1

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$4a$	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60	64	68	72
$4a$ mod 19	4	8	12	16	1	5	9	13	17	2	6	10	14	18	3	7	11	15

Почему? Ну, во-первых, в нижней строке не может появиться 0, ибо произведение не кратных простому числу p чисел a и k не может быть кратно p . Во-вторых, все числа нижней строки разные (это легко доказать «от противного»: если бы числа ak и bk давали при делении на p одинаковые остатки, то разность $ak - bk = (a - b)k$ была бы кратна p , что невозможно, поскольку $a - b$ не кратно p). Этих двух замечаний достаточно: ненулевых остатков от деления на p существует $p - 1$ штук, все они вынуждены по одному разу появиться в нижней строке таблицы.

Упражнения

15. Существует ли такое натуральное n , что число $1999n$ оканчивается на цифры 987654321?

16. Если целое число k взаимно просто с натуральным числом n , то существует такое натуральное число x , что $kx - 1$ кратно n . Докажите это.

17. Если целые числа a и b взаимно просты, то любое целое число c представимо в виде $c = ax + by$, где x, y – целые числа. Докажите это.

Как вы помните, малая теорема Ферма утверждает, что при любом целом k и простом p число $k^p - k = k(k^{p-1} - 1)$ кратно p . Значит, для чисел k , не кратных p , теорему можно формулировать следующим образом:

Теорема 1. Если целое число k не кратно простому числу p , то k^{p-1} дает остаток 1 при делении на p .

Доказательство. Поскольку остатки от деления на p чисел $k, 2k, 3k, \dots, (p-1)k$ — это (с точностью до перестановки) числа $1, 2, 3, \dots, p-1$, то

$$k \cdot 2k \cdot 3k \cdot \dots \cdot (p-1)k \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \pmod{p},$$

откуда

$$k^{p-1} (p-1)! \equiv (p-1)! \pmod{p}.$$

Сократив на $(p-1)!$, получим желаемое:

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

А тот, кто не решил упражнение 4,6) и не знает, почему сравнения можно сокращать (на число, взаимно простое с модулем), пусть рассуждает следующим образом: поскольку произведение $(k^{p-1} - 1) \cdot (p-1)!$ кратно p , а число $(p-1)!$ не кратно p , то в силу основной теоремы арифметики число $k^{p-1} - 1$ кратно простому числу p .

Упражнения

18. Найдите остаток от деления числа 3^{2000} на 43

19. Если целое число a не кратно 17, то $a^8 - 1$ или $a^8 + 1$ кратно

17 Докажите это

20. Докажите, что $m^{61}n - mn^{61}$ кратно 56786730 при любых целых m и n .

21. Найдите все такие простые числа p , что $5^{p^2} + 1$ кратно p .

22. Пусть p — простое число, $p \neq 2$. Докажите, что число $7^p - 5^p - 2$ кратно $6p$

23. Если p — простое число, то сумма $1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1}$ при делении на p дает остаток $p-1$. Докажите это.

24. Шестизначное число кратно 7. Его первую цифру стерли и затем записали ее позади последней цифры числа. Докажите, что полученное число тоже кратно 7. (Например, из кратных 7 чисел 632387 и 200004 таким образом получаем числа 323876 и 42, которые тоже кратны 7.)

25. Пусть p — простое число, отличное от 2, 3 и 5. Докажите, что число, записанное $p-1$ единицей, кратно p . (Например, 111111 кратно 7.)

26*. Докажите, что для любого простого p число 11 1122...22...99...99, состоящее из $9p$ цифр (сначала p единиц, потом p двоек, p троек, ..., наконец, p девяток), при делении на p дает такой же остаток, как и число 123456789

Бином Ньютона

Малую теорему Ферма легко доказать по индукции, если использовать формулу бинома Ньютона. Мы сделаем это для натуральных чисел a , оставив случай отрицательных чисел читателю.

Пусть сначала $p = 3$. **База индукции:** $1^3 - 1 = 0$ кратно 3. **Переход:** если для некоторого числа a уже доказали, что $a^3 - a$ кратно 3, то

$$\begin{aligned}(a+1)^3 - (a+1) &= \\ &= a^3 + 3a^2 + 3a + 1 - (a+1) \equiv a^3 + 1 - a - 1 = a^3 - a \equiv 0 \pmod{3}.\end{aligned}$$

Аналогично для $p = 5$: база очевидна ($1^5 - 1 \equiv 0 \pmod{5}$), а для перехода используем формулу

$$(a+1)^5 = a^5 + 5a^4 + 10a^3 + 10a^2 + 5a + 1.$$

Видите, коэффициенты при a^4 , a^3 , a^2 и a кратны 5. Поэтому

$$(a+1)^5 \equiv a^5 + 1 \pmod{5},$$

откуда и следует возможность индукционного перехода:

$$(a+1)^5 - (a+1) \equiv a^5 + 1 - a - 1 = a^5 - a \pmod{5}.$$

Займемся общим случаем. Формула бинома имеет вид

$$\begin{aligned}(a+1)^p &= a^p + pa^{p-1} + \frac{p(p-1)}{2}a^{p-2} + \\ &+ \frac{p(p-1)(p-2)}{3!}a^{p-3} + \dots + \frac{p(p-1)}{2}a^2 + pa + 1.\end{aligned}$$

Биномиальные коэффициенты $C_p^1 = p$, $C_p^2 = p(p-1)/2$, ..., $C_p^2 = p(p-1) \dots (p-k+1)/(k!)$, ..., $C_p^{p-1} = p$ кратны простому числу p . Поэтому $(a+1)^p \equiv a^p + 1 \pmod{p}$, что и требовалось: $(a+1)^p - (a+1) \equiv a^p + 1 - a - 1 = a^p - a \pmod{p}$.

Упражнение 27. Если n составное, то хотя бы один из биномиальных коэффициентов $C_n^1, C_n^2, \dots, C_n^{n-1}$ не кратен n . Докажите это.

Комбинаторное доказательство

На рисунке 1 изображены все 32 способа раскраски в два цвета круга, который разделен на 5 равных секторов.

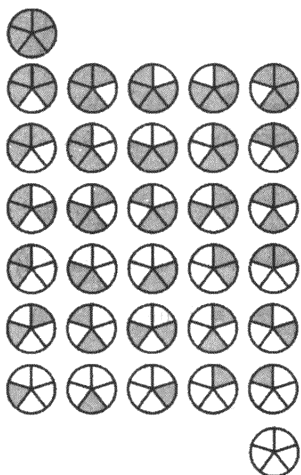


Рис. 1

Среди них выделяются два способа — когда весь круг одного цвета и когда он весь другого. А остальные разбиты на 6 групп по 5 раскрасок, получающихся одна из другой поворотом.

Спросим себя, сколькими способами можно раскрасить a разными красками круг, разбитый на p одинаковых секторов, где p — простое число? (Каждый сектор окрашивается одной краской; не обязательно использовать все краски; две раскраски, совпадающие при повороте круга, считаются одинаковыми.)

Очевидно, можно все секторы покрасить одной краской. Таких способов столько же, сколько красок, т.е. a способов.

А вот из любой другой раскраски поворотами можно получить p разных раскрасок (считая и саму эту раскраску: она получается поворотом на 0°). Значит, ответ таков:

$$a + \frac{a^p - a}{p}.$$

Поскольку количество способов не бывает дробным, число $a^p - a$ обязано нацело делиться на p .

Упражнение 28. Сколькими способами можно раскрасить a разными красками круг, разбитый: а) на p^2 секторов, где p — простое число; б) на pq секторов, где p, q — простые числа, $p \neq q$? (Каждый сектор окрашиваем одной краской; не обязательно использовать все краски; две раскраски, совпадающие при повороте круга, считаем одинаковыми.)

Часть II. Функция Эйлера

Таблицы умножения

Назло ей я все-таки перемножил землекопов. Правда, ничего хорошего про них не узнал, но зато теперь можно было переходить к следующему вопросу.

Л.Гераскина

Рассмотрим все $n - 1$ разных ненулевых остатков от деления на n . Составим таблицу умножения, написав на пересечении a -го столбца и b -й строки остаток от деления на n произведения ab . Например, при $n = 5$ получим таблицу 2, а при $n = 11$ — таблицу 3.

Таблица 2

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Таблица 3

×	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

Поскольку в обоих примерах число n простое, в каждой строке, как и в каждом столбце, возникает некоторая перестановка чисел $1, 2, \dots, n - 1$. Если же рассмотреть составное число, то в таблице обязательно встретится нуль. Например, при $n = 4$ имеем $2 \cdot 2 = 0$ (табл.4); не лучше ситуация и при $n = 12$ (табл.5): опять в некоторых строках есть нули! И вообще, при

Таблица 4

×	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Таблица 5

×	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11
2	2	4	6	8	10	0	2	4	6	8	10
3	3	6	9	0	3	6	9	0	3	6	9
4	4	8	0	4	8	0	4	8	0	4	8
5	5	10	3	8	1	6	11	4	9	2	7
6	6	0	6	0	6	0	6	0	6	0	6
7	7	2	9	4	11	6	1	8	3	10	5
8	8	4	0	8	4	0	8	4	0	8	4
9	9	6	3	0	9	6	3	0	9	6	3
10	10	8	6	4	2	0	10	8	6	4	2
11	11	10	9	8	7	6	5	4	3	2	1

любом составном числе $n = ab$, где $1 < a, b < n$, на пересечении a -й строки и b -го столбца стоит остаток от деления ab на n , т.е. 0.

Итак, если n составное, то имеются *делители нуля* – ненулевые остатки a и b , произведение ab которых кратно n , иными словами, равно нулю по модулю n . Но даже при составном n в некоторых строках таблицы умножения нет нулей. В таблице 4 таковы первая и третья строки, а в таблице 5 – первая, пятая, седьмая и одиннадцатая. Подумав немного, можно понять, что нули присутствуют в тех и только тех строках, номера которых имеют с числом n общий делитель, отличный от 1 (докажите это!). Давайте же вычеркнем из таблицы все такие строки и столбцы. (Если n – простое число, то вычеркивать ничего не придется.) При $n = 4$ получим таблицу из двух строк и столбцов (табл.6), а при $n = 12$ останется таблица размером 4×4 (табл.7).

Таблица 6

×	1	3
1	1	3
3	3	1

Таблица 7

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Упражнение 29. Заметьте, что каждая из таблиц 2–7 симметрична относительно обеих своих диагоналей. Докажите, что это так для любого n .

Теорема Эйлера

Чтобы обобщить малую теорему Ферма на случай составного числа n , оставим в таблице умножения только те строки и столбцы, в которых нет нулей, т.е. рассмотрим взаимно простые с n остатки от деления на n . В новой таблице строки (и столбцы) отличаются друг от друга лишь порядком, в котором расположены числа. Другими словами, если мы для натурального числа n выпишем все остатки a_1, a_2, \dots, a_r , взаимно простые с n , и домножим каждый из них на взаимно простое с n число k , то получим числа ka_1, ka_2, \dots, ka_r , которые тоже взаимно просты с n и дают разные остатки при делении на n (докажите!).

Итак, строка остатков от деления на n чисел ka_1, ka_2, \dots, ka_r может отличаться от строки a_1, a_2, \dots, a_r только порядком расположения чисел. Поэтому точно так же, как для простого p , для составного n имеем:

$$ka_1ka_2 \dots ka_r \equiv a_1a_2 \dots a_r \pmod{n},$$

откуда

$$(k^r - 1)a_1a_2 \dots a_r \equiv 0 \pmod{n}.$$

Значит, произведение $(k^r - 1)a_1a_2 \dots a_r$ кратно n . Поскольку числа a_1, a_2, \dots, a_r взаимно просты с n , то $k^r - 1$ кратно n . Если n – простое число, то $r = n - 1$ и получаем в точности утверждение малой теоремы Ферма. В общем же случае приходим к теореме Эйлера:

Теорема 2. Если k – целое число, взаимно простое с натуральным числом n , то $k^r - 1$ кратно n , где r – количество взаимно простых с n натуральных чисел, не превосходящих n .

Упражнения

30. Докажите, что если число k не кратно 3, то

а) k^3 при делении на 9 дает остаток 1 или 8;

б) k^{81} при делении на 243 дает остаток 1 или 242.

31. а) Если $a^3 + b^3 + c^3$ кратно 9, то хотя бы одно из целых чисел a, b, c кратно 3. Докажите это.

б) Сумма квадратов трех целых чисел кратна 7 в том и только том случае, когда сумма четвертых степеней этих чисел кратна 7. Докажите.

32. Докажите, что число $7^{7^{7^{7^7}}} - 7^{7^7}$ кратно 10.

33. Каковы три последние цифры числа 7^{9999} ?

34. Если целое число a взаимно просто с натуральным числом $n > 1$, то сравнение $ax \equiv b \pmod{n}$ равносильно сравнению $x \equiv a^{\varphi(n)-1}b \pmod{n}$. Докажите это.

35. Если n – нечетное натуральное число, то $2^{n-1} - 1$ кратно n . Докажите это.

36*. Найдите все натуральные $n > 1$, для которых сумма $1^n + 2^n + \dots + (n-1)^n$ кратна n .

37*. Для каждого натурального числа s существует кратное ему натуральное число n , сумма цифр которого равна s . Докажите это.

Формула включений-исключений

В 1763 году Леонард Эйлер (1707–1783) ввел обозначение $\varphi(n)$ (читают: фи от эн) для количества остатков, взаимно простых с n . Например, $\varphi(1) = 1$, $\varphi(4) = 2$, $\varphi(12) = 4$.

Если число p простое, то $\varphi(p) = p - 1$. Легко вычислить и $\varphi(p^m)$, где m – натуральное число. В самом деле, выпишем все p^m возможных остатков: $0, 1, 2, \dots, p^m - 1$. Из них кратны p в точности остатки $0, p, 2p, \dots, p^m - p$. Значит,

$$\varphi(p^m) = p^m - p^{m-1} = p^m \left(1 - \frac{1}{p}\right).$$

Давайте вычислим $\varphi(1000)$ – количество чисел первой тысячи, которые не кратны ни 2, ни 5. Для этого из 1000 вычтем сначала 500 – именно столько в первой тысяче четных чисел. Не забудем вычесть и $1000 : 5 = 200$ – столько в первой тысяче чисел, кратных 5. А еще мы должны учесть, что числа, оканчивающиеся цифрой 0, кратны и 2, и 5. Таких чисел 100 штук; каждое из них мы учитывали оба раза, а надо было – только один раз! Поэтому правильный ответ дает формула

$$\varphi(1000) = 1000 - 500 - 200 + 100 = 400.$$

В принципе, так можно вычислить $\varphi(n)$ для любого натурального числа n . Например, чтобы вычислить $\varphi(300)$, мы можем выписать все числа от 1 до 300 и вычеркнуть 150 четных чисел, а также 100 чисел, кратных 3, и 60 чисел, кратных 5. Затем мы должны вспомнить, что некоторые числа вычеркнуты дважды (а иные даже трижды), и «восстановить справедливость», т.е. к числу $300 - 150 - 100 - 60$ прибавить 50 (количество чисел, кратных $2 \cdot 3 = 6$), а также $300 : (2 \cdot 5) = 30$ и $300 : (3 \cdot 5) = 20$. Но и этого недостаточно: каждое из

десяти чисел, кратных $2 \cdot 3 \cdot 5 = 30$, было сначала трижды выброшено (как кратное 2, 3, 5), а затем трижды возвращено (как кратное 6, 10, 15). Но выбросить эти 10 чисел все-таки надо! Поэтому

$$\varphi(300) = 300 - 150 - 100 - 60 + 50 + 30 + 20 - 10 = 80.$$

Упражнения

38. Найдите $\varphi(2^a 5^b)$, где a, b – натуральные числа.

39. Пусть p, q – различные простые числа. Найдите а) $\varphi(pq)$, б) $\varphi(p^a q^b)$, где a, b – натуральные числа.

40. Решите уравнения: а) $\varphi(7^x) = 294$; б) $\varphi(3^x 5^y) = 360$.

Ничего сложного, как видите, нет. Для числа $n = p_1^{a_1} p_2^{a_2} \cdot \dots \cdot p_s^{a_s}$, где p_1, p_2, \dots, p_s – различные простые числа, a_1, a_2, \dots, a_s – натуральные числа, получаем при помощи формулы включений-исключений

$$\begin{aligned} \varphi(n) &= n - \frac{n}{p_1} - \frac{n}{p_2} - \dots - \frac{n}{p_s} + \frac{n}{p_1 p_2} + \dots + (-1)^s \frac{n}{p_1 p_2 \dots p_s} = \\ &= n \left(1 - \frac{1}{p_1} \right) \left(1 - \frac{1}{p_2} \right) \dots \left(1 - \frac{1}{p_s} \right). \end{aligned}$$

Мультипликативность функции Эйлера

Можно вывести формулу для функции Эйлера без использования включений-исключений.

Теорема 3. *Функция Эйлера мультипликативна, т.е. $\varphi(mn) = \varphi(m)\varphi(n)$ для любых взаимно простых натуральных чисел m и n .*

Следствие. *Если $n = p_1^{a_1} p_2^{a_2} \cdot \dots \cdot p_s^{a_s}$, где p_1, p_2, \dots, p_s – различные простые числа, a_1, a_2, \dots, a_s – натуральные числа, то*

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{a_1}) \varphi(p_2^{a_2}) \cdot \dots \cdot \varphi(p_s^{a_s}) = \\ &= (p_1^{a_1} - p_1^{a_1-1}) (p_2^{a_2} - p_2^{a_2-1}) \cdot \dots \cdot (p_s^{a_s} - p_s^{a_s-1}). \end{aligned}$$

Доказательство теоремы 3. Рассмотрим числа вида $mx + ny$, где $0 \leq x < n$ и $0 \leq y < m$. Запишем их в виде таблицы размером $n \times m$. Например, при $n = 5$ и $m = 8$ получаем таблицу 8.

Таблица 8

$y \backslash x$	0	1	2	3	4	5	6	7
0	0	5	10	15	20	25	30	35
1	8	13	18	23	28	33	38	43
2	16	21	26	31	36	41	46	51
3	24	29	34	39	44	49	54	59
4	32	37	42	47	52	57	62	67

Остатки от деления на mn всех чисел этой таблицы разные. В самом деле, если бы какие-то два остатка совпали, то было бы выполнено сравнение

$$mx_1 + ny_1 \equiv mx_2 + ny_2 \pmod{mn},$$

где $0 \leq x_1, x_2 < n$ и $0 \leq y_1, y_2 < m$. Переходя от сравнения по модулю mn к сравнению по модулю n , получаем:

$$mx_1 + ny_1 \equiv mx_2 + ny_2 \pmod{n},$$

откуда $mx_1 \equiv mx_2 \pmod{n}$. Вследствие взаимной простоты чисел m и n получаем

$$x_1 \equiv x_2 \pmod{n}.$$

Поскольку $0 \leq x_1, x_2 < n$, получаем: $x_1 = x_2$. Аналогично сравнение по модулю m приводит к равенству $y_1 = y_2$.

Итак, все mn чисел таблицы разные. Но возможных остатков от деления на mn ровно столько же, сколько чисел в таблице! Значит, для любого числа $d = 0, 1, \dots, mn - 1$ существует и единственна такая пара целых чисел x, y , что $0 \leq x < n$, $0 \leq y < m$ и $d \equiv mx + ny \pmod{mn}$.

В таблице 8 четные числа образуют четыре столбца, а числа, кратные 5, образуют одну строку. Это не случайно:

$$\text{НОД}(mx + ny; m) = \text{НОД}(ny; m) = \text{НОД}(y; m);$$

аналогично, $\text{НОД}(mx + ny; n) = \text{НОД}(x; n)$. По этой причине в рассматриваемой таблице числа, взаимно простые с m , расположены в $\varphi(m)$ строках (тех, где y взаимно просто с m), а числа, взаимно простые с n , образуют $\varphi(n)$ столбцов.

Теперь доказательство теоремы 3 не составляет труда: чтобы d было взаимно просто с mn , необходимо и достаточно, чтобы d было взаимно просто с числами m и n . Такие числа d лежат на пересечении $\varphi(m)$ строк с $\varphi(n)$ столбцами. Всего получаем «решетку» из $\varphi(m)\varphi(n)$ чисел, что и требовалось доказать.

Упражнения

41. Запишем числа от 0 до $mn - 1$ в таблицу из m строк и n столбцов (табл.9).

Таблица 9

0	1	2	...	$n - 1$
n	$n + 1$	$n + 2$...	$2n - 1$
$2n$	$2n + 1$	$2n + 2$...	$3n - 1$
...
...
$(m - 1)n$	$(m - 1)n + 1$	$(m - 1)n + 2$...	$mn - 1$

а) Составьте такую таблицу для $m = 3$ и $n = 4$. Зачеркните в ней сначала все четные числа, а затем — те из оставшихся чисел, которые кратны 3. Заметьте, что незачеркнутыми остались в точности числа, взаимно простые с 12, и что незачеркнутые числа не образуют решетки.

б) Докажите теорему 3 по следующему плану:

1) числа, взаимно простые с n , заполняют собой $\varphi(n)$ столбцов таблицы 9;

2) остатки от деления на m всех m чисел любого столбца таблицы 9 различны;

3) в каждом столбце присутствует ровно $\varphi(m)$ чисел, взаимно простых с m ;

4) число взаимно просто с mn тогда и только тогда, когда оно взаимно просто с n (такие числа лежат в $\varphi(n)$ столбцах) и взаимно просто с m (в каждом столбце таких чисел $\varphi(m)$).

42. Окружность разделили n точками на n равных частей. Сколько можно построить различных замкнутых ломаных из n равных звеньев с вершинами в этих точках? (Две ломаные, получающиеся одна из другой поворотом, считаем одинаковыми. На рисунке 2 изображены все четыре такие ломаные при $n = 20$, а на рисунке 3 — все четыре ломаные сразу.)

43. Для любых натуральных чисел m и n докажите равенства:

а) $\varphi(m)\varphi(n) = \varphi(\text{НОК}(m;n))\varphi(\text{НОД}(m;n))$;

б) $\varphi(mn) = \varphi(\text{НОК}(m;n)) \cdot \text{НОД}(m;n)$;

в) $\varphi(m)\varphi(n)\text{НОД}(m;n) = \varphi(mn)\varphi(\text{НОД}(m;n))$.

г) Пусть m и n — натуральные числа, причем $\text{НОД}(m;n) > 1$. Докажите неравенство $\varphi(mn) > \varphi(m)\varphi(n)$.

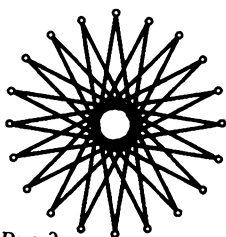
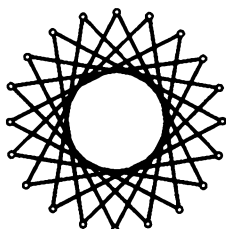
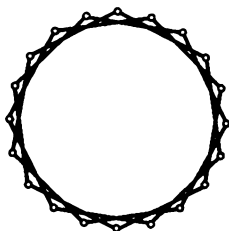
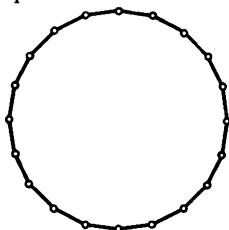


Рис. 2

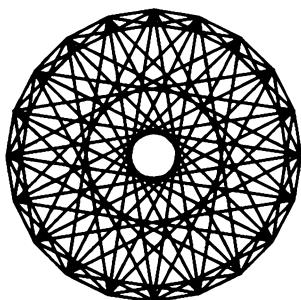


Рис. 3

44. Решите уравнения: а) $\varphi(x) = 18$; б) $\varphi(x) = 12$; в) $x - \varphi(x) = 12$; г*) $\varphi(x^2) = x^2 - x$; д) $\varphi(x) = x/2$; е) $\varphi(x) = x/3$; ж*) $\varphi(x) = x/n$, где n – натуральное число, $n > 3$; з) $\varphi(nx) = \varphi(x)$, где n – натуральное число, $n > 1$.

Сумма значений функции Эйлера

Рассмотрим 100 дробей: $1/100, 2/100, \dots, 100/100$. Если каждую из них привести к несократимому виду, то получим $\varphi(100) = 40$ дробей со знаменателем 100, $\varphi(50) = 20$ дробей со знаменателем 50, и так далее: для каждого делителя d числа 100 получим $\varphi(d)$ дробей со знаменателем d . (Почему? Потому что $\varphi(d)$ – это количество несократимых правильных дробей со знаменателем d .)

Мы получили равенство:

$$100 = \varphi(100) + \varphi(50) + \varphi(25) + \varphi(20) + \\ + \varphi(10) + \varphi(5) + \varphi(4) + \varphi(2) + \varphi(1).^1$$

Если бы мы рассмотрели не дроби со знаменателем 100, а дроби со знаменателем n , то точно так же доказали бы, что для любого натурального числа n сумма значений функции Эйлера $\varphi(d)$ по всем делителям d числа n равна n , т.е.

$$n = \sum_{d|n} \varphi(d).$$

Упражнения

45. Если d – делитель числа n , то существует ровно $\varphi(n/d)$ таких натуральных чисел k , что $k \leq n$ и $\text{НОД}(k; n) = d$. Докажите это.

46. Пусть $n > 1$. Найдите сумму всех несократимых правильных дробей, знаменатели которых равны n .

¹ Для Фомы неверующего: $40 + 20 + 20 + 8 + 4 + 4 + 2 + 1 + 1 = 100$.

Шифры с открытым ключом

*На вопрос, что он написал в шифровке,
Штирлиц ответил: «Не помню.
Теперь это знает только Центр».*

Вообразите, что вам нужно получить зашифрованное сообщение от друга, но вы с ним не договорились заранее, каким шифром будете пользоваться. Как быть? Существует ли такой метод шифрования, что этот метод можно сообщить всему миру (в том числе и вашему другу, и врагам), но это не даст врагам возможности расшифровать сообщение?

Это был бы замечательный шифр: в отличие от старых шифров, в которых главный секрет – ключ, знание которого позволяет и зашифровывать, и расшифровывать сообщения, новый шифр – «с открытым ключом»: каждый может зашифровывать, но только автор шифра может расшифровать получаемые сообщения.

Шифр RSA

...Так начались необычайные события, которые вовлекли в свой круговорот немало людей.

Е.Велтистов

Возможно, шифр с открытым ключом уже изобретен. В 1978 году три математика – Ривест, Р.Шамир и Л.Адлеман – зашифровали некоторую английскую фразу и пообещали награду в 100\$ первому, кто расшифрует сообщение

$y = 9686961375462206147714092225435588290575999112457431$
 $98746951209308162982251457083569314766228839896280133919$
 $90551829945157815154.$

Они подробно объяснили способ шифрования. Сначала фразу бесхитростно ($a = 01$, $b = 02$, $c = 03, \dots$, $z = 26$, пробел = 00) записали в виде последовательности цифр. Получилось некоторое 78-значное число x . Затем взяли 64-значное простое число p и 65-значное простое число q . Перемножили их (не вручную, разумеется, а на компьютере):

$pq = 114381625757888867669325779976146612010218296721242$
 $3625625618429357069352457338978305971235639587050589890751$
 $47599290026879543541.$

Теперь – главное:

$$y \equiv x^{9007} \pmod{pq}.$$

Понимаете? Они опубликовали и произведение pq , и число 9007, и сам метод шифрования (и, разумеется, число y). Было даже сказано, что из чисел p и q одно 64-значное, а другое 65-значное. В секрете остались только сами числа p и q . Требовалось найти x .

В 1994 году Д.Аткинс, М.Грэфф, А.Ленстра и П.Лейланд расшифровали эту фразу: «The magic words are squeamish ossifrage». (Приведем перевод двух последних слов этой, по всей видимости, бессмысленной фразы: squeamish – брезгливый, привередливый, обидчивый; ossifrage – скопа.)

Числа p и q оказались равны

$$p = 3490529510847650949147849619903898133417764638493387 \\ 843990820577,$$

$$q = 2769132993266709549961988190834461413177642967992942 \\ 539798288533.$$

В книге «Введение в криптографию» (М., МЦНМО, 1998 г.) сказано: «Этот замечательный результат (разложение на множители 129-значного числа) был достигнут благодаря использованию алгоритма разложения чисел на множители, называемого методом квадратичного решета. Выполнение вычислений потребовало колоссальных ресурсов. В работе, возглавлявшейся четырьмя авторами проекта и продолжавшейся после предварительной теоретической подготовки примерно 220 дней, на добровольных началах участвовало около 600 человек и примерно 1600 компьютеров, объединенных сетью Internet.»

Рассказ о методе квадратичного решета нам не по силам; можно лишь обсудить основную идею системы RSA (по первым буквам фамилий авторов: Rivest R. L., Shamir A., Adleman L.).

Во-первых, зная p и q , можно найти $\varphi(pq) = (p-1)(q-1)$. Во-вторых (и это главное!), если

$$ef = 1 + k\varphi(pq),$$

где e, f, k – натуральные числа, то для любого числа x , взаимно простого с pq , по теореме Эйлера имеем

$$x^{ef} = x \cdot (x^k)^{\varphi(pq)} \equiv x \cdot 1 = x \pmod{pq}.$$

Вы поняли, что такое e и f ? В нашем примере $e = 9007$

(единственное обязательное математическое требование к числу e – его взаимная простота с числом $(p-1)(q-1)$; впрочем, брать $e = 1$ или $e = (p-1)(q-1) - 1$ вряд ли разумно, если хотите сохранить секреты). А число f , как уже было сказано, – решение сравнения

$$ef \equiv 1 \pmod{\varphi(pq)}.$$

(В статье «Алгоритм Евклида» рассказано, как решать такие сравнения.)

Сравнения

$$y^f \equiv x^{ef} \equiv x \pmod{pq}$$

показывают, что для нахождения x достаточно найти остаток от деления y^f на pq . (Числа выбраны так, что $x < pq$. При этом x не кратно ни p , ни q . Не подумайте, что это всерьез нас ограничивает: если p и q – большие числа, то вероятность того, что x нацело разделится на p или q , пренебрежимо мала. Кроме того, можно предусмотреть в алгоритме, чтобы в случае чего сообщение x было автоматически как-то так чуть-чуть изменено, без изменения его смысла, что x и pq станут взаимно просты. Как быстро возводить в большую степень, рассказано чуть ниже.)

Почему многие надеются, что шифр RSA является шифром с открытым ключом? Да потому, что числа pq и e можно сделать общедоступными. Тогда зашифровать сообщение сможет любой, у кого есть компьютер (и какая-нибудь программа, позволяющая выполнять действия с многозначными числами). Расшифровать сообщение легко, если мы знаем число f . Но единственный известный ныне способ нахождения числа f требует нахождения чисел p и q , т.е. разложения произведения pq на множители. А эффективных алгоритмов решения этой задачи пока нет (удача 1994 года не в счет: если бы в числах p и q было не 64 и 65, а хотя бы по 300 цифр, то и ресурсов сети Internet не хватило бы!). Впрочем, нет сейчас и доказательств того, что никто никогда не научится быстро (математик сказал бы: «за время, полиномиальное от количества цифр») разлагать числа на простые множители.

Как возводить в большую степень?

Чтобы возвести число x в 9007-ю степень, по определению, достаточно выполнить 9006 умножений. Но можно обойтись и меньшим числом операций: вычислить x^2 , $(x^2)^2 = x^4$, $(x^4)^2 = x^8$, ..., $(x^{2048})^2 = x^{4096}$, наконец, $(x^{4096})^2 = x^{8192}$ и воспользоваться

формулой

$$x^{9007} = x \cdot x^2 \cdot x^4 \cdot x^8 \cdot x^{32} \cdot x^{256} \cdot x^{512} \cdot x^{8192},$$

которая основана на том, что в двоичной системе счисления 9007 имеет вид

$$9007_{10} = 10001100101111_2.$$

Понимаете? Мы разложили 9007 в сумму $1 + 2 + 4 + 8 + 32 + 256 + 512 + 8192$ и смогли сильно сэкономить: обошлись 13-ю возведениями в квадрат на первом этапе вычислений и 7-ю умножениями на втором этапе. Всего 20 умножений вместо 9006. Огромная экономия! (Для придирчивого читателя отметим, что выше следовало бы говорить не об умножениях, а об умножениях по модулю pq : дабы количество цифр не росло катастрофически, мы всякий раз должны не только перемножать, но и брать остаток от деления на pq . Но сейчас разговор не об этом.)

Преимущества изложенного метода возведения в степень тем нагляднее, чем больше показатель степени. Например, если показатель степени состоит не из четырех цифр, как 9007, а из нескольких десятков или сотен цифр, то наивный способ не то что утомителен, а неосуществим ни на каких, даже самых мощных компьютерах. А основанный на двоичной системе – работает и в такой ситуации!

Упражнение 47 (M1086). С числом разрешено производить две операции: «увеличить в 2 раза» и «увеличить на 1». За какое наименьшее число операций можно из числа 0 получить число а) 100; б) 9907; в) n , если в двоичной системе счисления n имеет вид $\overline{a_m a_{m-1} \dots a_1 a_0}$?

Что дальше?

*Что остается от сказки потом,
После того, как ее рассказали?*

В.Высоцкий

Подытожим. В первой части статьи мы доказали малую теорему Ферма. Во второй части доказали ее обобщение – теорему Эйлера, рассказали о функции Эйлера и о практическом применении теоремы Эйлера в криптографии. Правда, осталось тайной, откуда взялись числа p , q (точнее говоря, как можно конструировать большие – в несколько десятков или сотен цифр – простые числа).

В третьей части мы расскажем об основанных на малой теореме Ферма методах конструирования больших простых чисел. Расскажем и о числах Кармайкла, история которых началась в древнем Китае, а существование бесконечного множества которых доказано в 1994 году.

Но главное – расскажем о периодичности остатков, и это приведет нас к теореме о существовании первообразного корня по простому модулю и затем к теореме о строении мультипликативной группы вычетов по (не обязательно простому) модулю n . Чтобы вы лучше оценили силу результатов третьей части статьи, подумайте над следующими задачами. Не огорчайтесь даже в том случае, если ни одна из них не получится: это не упражнения, а довольно трудные задачи!

Задачи

1. Для каких простых чисел p существует такое целое число a , что сумма $a^4 + a^3 + a^2 + a + 1$ кратна p ?

2. Ни для какого натурального числа n число $2^n + 1$ не кратно $n + 1$. Докажите это.

3. Если $2^n + 1$ кратно n , то $n = 1$ или n кратно 3. Докажите это.

4. Существует ли такое составное число n (число Кармайкла), что для любого целого числа a разность $a^n - a$ кратна n ?

5. Для каких n числа $1, 2, \dots, n$ можно расставить вдоль окружности так, чтобы для любых подряд идущих чисел a, b, c разность $b^2 - ac$ была кратна $n + 1$? (На рисунке 4 изображен случай $n = 10$.)

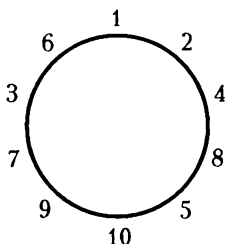


Рис. 4

Часть III. Длины периодов

*Мы заняты делом,
отвлечься не может;
мы числа в тетради
все множим и множим.*

А. Котова

Остатки от деления на 11

Какие остатки дают степени двойки при делении на 11? Чтобы ответить на этот вопрос, составим таблицу:

Таблица 10

n	1	2	3	4	5	6	7	8	9	10	11	12
2^n	2	4	8	16	32	64	128	256	512	1024	2048	4096
$2^n \bmod 11$	2	4	8	5	10	9	7	3	6	1	2	4

Дальше можно не продолжать: $2^{10+n} = 2^{10} \cdot 2^n \equiv 1 \cdot 2^n = 2^n \pmod{11}$, остатки будут повторяться с периодом 10. Между прочим, средняя строка таблицы излишняя: в нижней строке каждое следующее число – это остаток от деления на 11 удвоенного предыдущего числа.

Как бы то ни было, $2^{10} \equiv 1 \pmod{11}$. Ничего удивительного в этом нет, это всего лишь частный случай малой теоремы Ферма. Интереснее другое: в нижней строке таблицы 10 присутствуют все ненулевые остатки от деления на 11. Например, $3 \equiv 2^8$, $5 \equiv 2^4$, $7 \equiv 2^7$, $10 \equiv 2^5 \pmod{11}$.

Другими словами, для любого целого числа a , не кратного 11, существует такое s , что $a \equiv 2^s \pmod{11}$.

А сейчас – внимание: $a^{10} \equiv (2^s)^{10} = (2^{10})^s \equiv 1^s \pmod{11}$. Таким образом, при $p = 11$ мы проверили малую теорему Ферма не только для $a = 2$, но для любого ненулевого остатка a . Красиво и неожиданно, не правда ли?

Упражнение 48. Рассматривая степени двойки, докажите малую теорему Ферма для а) $p = 13$; б) $p = 19$.

Что такое первообразный корень?

Число g называют *первообразным корнем* по модулю p , если числа g, g^2, \dots, g^{p-1} дают разные (ненулевые) остатки при делении на p . Другими словами, g – первообразный корень, если для любого целого числа a , не кратного числу p , существует такое s , что $a \equiv g^s \pmod{p}$.

Упражнение 49. а) Какие из чисел 1, 2, 3, 4 являются первообразными корнями по модулю 5? б) Какие целые числа являются первообразными корнями по модулю 7?

Изоморфизм

- *Какая разница между социализмом и капитализмом?*
- *При капитализме человек эксплуатирует человека, а при социализме – наоборот.*

В разделе «Таблицы умножения» второй части статьи мы составили таблицу умножения по модулю 11. Тот факт, что 2 – первообразный корень, позволяет нам так переставить ее столбцы и строки, что таблица приобретет гораздо более вынятный вид.

Таблица 11

×	1	2	4	8	5	10	9	7	3	6
1	1	2	4	8	5	10	9	7	3	6
2	2	4	8	5	10	9	7	3	6	1
4	4	8	5	10	9	7	3	6	1	2
8	8	5	10	9	7	3	6	1	2	4
5	5	10	9	7	3	6	1	2	4	8
10	10	9	7	3	6	1	2	4	8	5
9	9	7	3	6	1	2	4	8	5	10
7	7	3	6	1	2	4	8	5	10	9
3	3	6	1	2	4	8	5	10	9	7
6	6	1	2	4	8	5	10	9	7	3

Если $a \equiv g^s$ и $b \equiv g^t$, то $ab \equiv g^s g^t = g^{s+t} \pmod{11}$. Это сводит умножение по модулю 11 к сложению по модулю 10 (именно по этому модулю рассматриваются числа s и t). Рассмотрим таблицу 12 сложения по модулю 10.

Таблица 12

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

Таблицы 11 и 12 похожи, как близнецы! Мультипликативная¹ группа вычетов \mathbf{Z}_{11}^* (ее элементы – ненулевые классы вычетов по модулю 11, операция – умножение) изоморфна аддитивной² группе \mathbf{Z}_{10} вычетов по модулю 10 (элементы – классы вычетов по модулю 10, операция – сложение). Изоморфизм – это взаимно однозначное отображение, сохраняющее операцию. Например, изоморфизм между \mathbf{Z}_{10} и \mathbf{Z}_{11}^* можно установить, сопоставив каждому из классов $s = 0, 1, \dots, 9 \pmod{10}$

¹ Multiplitio (лат.) – умножение.

² Additio (лат.) – сложение

класс $2^s \pmod{11}$. При этом сумме $s + t \pmod{10}$ будет, как мы уже говорили, сопоставлено произведение $2^s \cdot 2^t \pmod{11}$.

Числа на окружности

Для любых трех стоящих подряд чисел a, b, c рисунка 4 разность $b^2 - ac$ кратна 11. А на рисунке 5 такие разности кратны 13. Это не случайные курьезы, а частный случай общей конструкции: для любого первообразного корня g по простому модулю p можно рассмотреть геометрическую прогрессию $g, g^2, \dots, g^{p-2}, g^{p-1}$ и выписать вдоль окружности

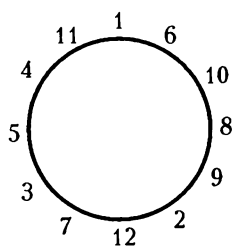


Рис. 5

остатки от деления ее членов на p . (Рисунок 4 иллюстрирует случай $g = 2$ и $p = 11$, рисунок 5 – случай $g = 6$ и $p = 13$.) Дело в том, что если числа a, b, c образуют геометрическую прогрессию, то выполнено равенство $b^2 = ac$. Поскольку мы заменяли числа на их остатки от деления на p , то вместо равенств получаем сравнения по модулю p . Следовательно, когда мы докажем, что по простому модулю p существует

первообразный корень – а мы это докажем, хотя и нескоро, – то одновременно докажем и возможность такого расположения чисел $1, 2, \dots, p-1$ вдоль окружности, при котором для любых трех стоящих подряд чисел a, b, c разность $b^2 - ac$ кратна p .

Упражнение 50. Пусть n – составное. Можно ли так расположить числа $1, 2, \dots, n-1$ вдоль окружности, чтобы для любых трех стоящих подряд чисел a, b, c разность $b^2 - ac$ была кратна n ?

Степени по модулю 17

Рассмотрим остатки от деления степеней двойки на 17:

Таблица 13

n	1	2	3	4	5	6	7	8
$2^n \pmod{17}$	2	4	8	16	15	13	9	1

Зацикливание произошло слишком рано: $2^8 \equiv 1 \pmod{17}$. Поэтому не все ненулевые остатки от деления на 17 – остатки от деления степеней двойки. Например, в нижней строке таблицы 13 нет числа 5, так что разность $2^n - 5$ не кратна 17 ни при каком натуральном n .

Давайте начнем не с двойки, а с тройки и, не забывая переходить к остатку от деления на 17, будем умножать, умножать и умножать на три: 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1. Мы получили все 16 возможных ненулевых остатков от деления на 17. Значит, 3 – первообразный корень по модулю 17.

Не для каждого простого числа p в качестве первообразного корня годится 2 или 3. Например, легко проверить, что

$$2^{11} \equiv 1 \equiv 3^{11} \pmod{23},$$

так что ни 2, ни 3 не являются первообразными корнями по модулю 23. (А вот -2 и -3 , как можно убедиться, являются.)

Упражнения

51. Ни при каком натуральном n число $1719^n - 3$ не кратно 17. Докажите это.

52. Среди чисел вида $2^n - 3$ бесконечно много чисел, кратных 5, и бесконечно много чисел, кратных 13, но нет ни одного числа, кратного $65 (= 5 \cdot 13)$. Докажите это.

53. Найдите наименьшее простое число p , для которого существует a , не сравнимое по модулю p ни с одним из чисел $-1, 0, 1$ и такое, что ни a , ни $-a$ не являются первообразными корнями по модулю p .

Когда $a^m - 1$ делится на $a^k - 1$?

От числовых примеров перейдем к более абстрактным рассуждениям. Прежде всего напомним формулы сокращенного умножения:

$$a^2 - 1 = (a - 1)(a + 1),$$

$$a^3 - 1 = (a - 1)(a^2 + a + 1),$$

и вообще,

$$a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \dots + a + 1).$$

Теорема 4. Если a, k, m – натуральные числа, $a > 1$, то $a^m - 1$ делится на $a^k - 1$ в том и только том случае, когда m делится на k .

Доказательство. Если $m = kn$, то

$$a^m - 1 = (a^k - 1)(a^{k(n-1)} + a^{k(n-2)} + \dots + a^k + 1).$$

Обратно, если m не делится на k , то разделим m на k с остатком:

$$m = kn + r,$$

где $0 < r < k$, и рассмотрим формулу

$$a^{kn+r} - 1 = a^{kn+r} - a^r + a^r - 1 = a^r(a^{kn} - 1) + (a^r - 1).$$

Число $a^r - 1$ не делится на $a^k - 1$, поскольку $0 < a^r - 1 < a^k - 1$. Теорема доказана.

Упражнения

54. Если число $a^n - 1$ простое, $a > 1$ и $n > 1$, то $a = 2$ и n – простое. Докажите это. (Не при всяком простом p число $2^p - 1$ простое: например, $2^{11} - 1 = 2047 = 23 \cdot 89$. Простые числа вида $2^p - 1$ называют числами Мерсенна³. В настоящий момент известны 43 числа Мерсенна и неизвестно, конечно или бесконечно их множество. 23 января 2006 года нашли наибольшее из известных на сегодняшний день: $2^{30402457} - 1$; его десятичная запись состоит из 9152052 цифр.)

55. Если $a^n + 1$ – простое число, a, n – натуральные числа, $a > 1$, то a четно и n – степень числа 2. Докажите это. (Простые числа вида $2^{2^n} + 1$ называют числами Ферма. Их известно всего пять: $2^{2^0} + 1 = 3$, $2^{2^1} + 1 = 5$, $2^{2^2} + 1 = 17$, $2^{2^3} + 1 = 257$ и $2^{2^4} + 1 = 65537$. Существуют ли другие, неизвестно. Неизвестно и то, конечно или бесконечно множество простых чисел вида $p = a^2 + 1$.)

56. а) Число $2^n - 1$ делится на $2^m + 1$ тогда и только тогда, когда n делится на $2m$. Докажите это.

б) Для каких натуральных чисел m существует такое натуральное n , что $2^n + 1$ делится на $2^m - 1$?

57. Натуральные числа a, b, n таковы, что $a - k^n$ кратно $k - b$ для любого натурального числа $k \neq b$. Докажите равенство $a = b^n$.

Степени числа по модулю p

Для любого целого числа a , не кратного простому p , рассмотрим числа $1, a, a^2, \dots, a^{p-1}$. Ни одно из них не кратно p . Поскольку ненулевых остатков от деления на p существует всего $p - 1$ штук, а мы рассматриваем p чисел, то какие-то два из них дают один и тот же остаток:

$$a^r \equiv a^s \pmod{p},$$

где $0 \leq r < s < p$. Сокращая на a^r , получаем:

$$a^{s-r} \equiv 1 \pmod{p},$$

³ Марен Мерсенн (1588–1648) занимался математикой, теорией музыки, физикой и философией. Он был товарищем Р.Декарта по учебе в иезуитском колледже и членом монашеского ордена минимов. Мерсенн сыграл выдающуюся роль как организатор науки. Он состоял в переписке с Р.Декартом, Ж.Робервалем, Б.Паскалем, Х.Гюйгенсом, Б.Кавальери, Френиклем де Бесси, Дж.Валлисом и др. Вокруг него образовался кружок ученых, который стал основой для создания Парижской академии наук (1666 год).

т.е. остаток от деления числа a^{s-r} на p равен 1. Значит, последовательность остатков от деления степеней числа a на p – периодическая.

Упражнения

58. а) Пусть число n нечетно и не кратно 5. Докажите, что существует кратное n число, записываемое одними единицами.

б) Если целое число a и натуральное n взаимно просты, то существует такое k , что сумма $1 + a + a^2 + \dots + a^k$ кратна n . Докажите это.

59. а) Для любого натурального n числа $8^n + 1$ и $5 \cdot 4^n + 1$ – составные. Докажите это.

б) Существует бесконечно много составных чисел вида $10^n + 3$. Докажите это. (Неизвестно, существует ли бесконечно много простых чисел вида $10^n + 3$.)

в) Пусть a, b, c – натуральные числа, $b > 1$. Докажите, что среди чисел вида $ab^n + c$ бесконечно много составных.

Что такое порядок?

Наименьшее натуральное число k , для которого $a^k \equiv 1 \pmod{p}$, называют *порядком* (не кратного p) числа a по модулю p .

Очевидно, числа $a, a^2, \dots, a^k (\equiv 1)$ дают при делении на p разные остатки, а дальше последовательность периодична: $a^{k+1} \equiv a, a^{k+2} \equiv a^2, \dots$ При этом

$$a^k \equiv a^{2k} \equiv a^{3k} \equiv \dots \equiv 1 \pmod{p},$$

а другие степени числа a не сравнимы с 1 по модулю p .

Если вместо простого числа p вы рассмотрите любое натуральное число n , то аналогичным образом сможете доказать следующую важную теорему.

Теорема 5. Если целое число a взаимно просто с натуральным числом n , то существует бесконечно много таких натуральных m , что $a^m - 1$ кратно n . Все они являются кратными наименьшего из них (которое называют порядком числа a по модулю n).

Упражнения

60. Если целое число a взаимно просто с натуральным n и если $a^r \equiv a^s \equiv 1 \pmod{n}$, то $a^{\text{НОД}(r,s)} \equiv 1 \pmod{n}$. Докажите это.

61. Зная, что порядок числа $a = 10$ по модулю $p = 19$ равен 18, выясните, при каких k число $\underbrace{11\dots1}_k$ кратно 19.

62. Если число $1000\dots01$ кратно 19, то оно кратно 13. Докажите это.

Разбиение на циклы

Пусть целое число a не кратно простому p и пусть k – порядок числа a по модулю p . Как при помощи k сформулировать малую теорему Ферма? А вот как: $p - 1$ кратно k (т.е. $p - 1 = kt$ для некоторого натурального t ; сравнение $a^{p-1} \equiv 1$ получается из сравнения $a^k \equiv 1$ возведением в t -ю степень).

Теорема 6 (Лагранж). *Порядок k не кратного простому p целого числа a является делителем числа $p - 1$.*

Доказательство. Идея в том, что все $p - 1$ ненулевых остатков от деления на p мы разобьем на циклы вида $\{x, ax, \dots, a^{k-1}x\}$. Каждый такой цикл состоит из k остатков. (Эти циклы тесно связаны с разложениями обыкновенных дробей в периодические, о которых рассказано в статье «Периодические дроби».)

Проведя от каждого ненулевого остатка x стрелочку к остатку от деления на p числа ax , мы получим граф, в котором из каждого ненулевого остатка x выходит одна стрелочка и к каждому ненулевому остатку ведет тоже ровно одна стрелочка (если бы к какому-то остатку вели стрелочки от x и y , то выполнялось бы сравнение $ax \equiv ay \pmod{p}$, откуда $x \equiv y \pmod{p}$, так что $x = y$). Теорема 6 доказана.

Рассмотрев вместо простого p любое натуральное число n , аналогичным образом можно доказать, что порядок (по модулю n) любого взаимно простого с n целого числа a – делитель числа $\varphi(n)$. При этом $a^{\varphi(n)} \equiv 1 \pmod{n}$. Последнее утверждение, как вы помните, носит имя Леонарда Эйлера.

Упражнения

63. Существует ли такое натуральное число k , что сто последних цифр десятичной записи числа 3^k совпадают со ста последними цифрами числа 7^k ?

64. Если a и b – взаимно простые натуральные числа, то $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$. Докажите это.

65. Существует бесконечно много натуральных чисел n , для которых $2^n + n^2$ кратно 100. Докажите это.

66. Для любого простого числа p существует бесконечно много чисел вида $2^n - n$, кратных p . Докажите это.

67. а) Последние две цифры квадрата любого натурального числа и его 22-й степени совпадают: $n^2 \equiv n^{22} \pmod{100}$. Докажите это.

б) Докажите, что $n^{103} \equiv n^3 \pmod{1000}$ для любого целого числа n .

68. Последние цифры чисел вида а) n^n ; б) n^{n^n} (n – натуральное)

образуют периодическую последовательность. Докажите это и найдите длину ее наименьшего периода.

69. Найдите четыре последние цифры числа а) 3^{1999} ; б) 2^{1999} ; в) $2^{3^{2000}}$.

70*. Уравнение $x^7 + y^7 = 1998^2$ не имеет решений в натуральных числах. Докажите это.

71*. Для любого целого числа $k \neq 1$ существует бесконечно много натуральных чисел n , для которых число $2^{2^n} + k$ – составное. Докажите это. (Аналогичное утверждение для $k = 1$ мы доказывать не умеем: существует или нет бесконечно много составных чисел вида $2^{2^n} + 1$, неизвестно.)

Следствия теоремы Лагранжа

Теорема Лагранжа позволяет легко решать многие задачи, которые без нее или очень трудны, или вообще недоступны. Решим первую из задач, которые были сформулированы в конце второй части статьи.

Делители чисел вида $a^4 + a^3 + a^2 + a + 1$

Если сумма $a^4 + a^3 + a^2 + a + 1$ кратна простому числу p , то число

$$a^5 - 1 = (a - 1)(a^4 + a^3 + a^2 + a + 1)$$

тоже кратно p . Рассмотрим два случая.

Пусть $a \equiv 1 \pmod{p}$. Тогда $a^4 + a^3 + a^2 + a + 1 \equiv 1^4 + 1^3 + 1^2 + 1 + 1 = 5 \pmod{p}$, так что число p должно быть делителем числа 5. Попросту говоря, $p = 5$.

Пусть теперь $a \not\equiv 1 \pmod{p}$. Тогда порядок числа a по модулю p равен 5. Поскольку порядок является делителем числа $p - 1$, то $p - 1$ делится на 5.

Итак, если простое число p является делителем числа вида $a^4 + a^3 + a^2 + a + 1$, то $p = 5$ или $p \equiv 1 \pmod{5}$.

Верно и обратное утверждение: для $p = 5$ годится $a = 1$, а для простого числа $p = 5k + 1$ годится $a = g^k$, где g – первообразный корень по модулю p (существование которого мы докажем ниже). В самом деле, $g^{5k} = g^{p-1} \equiv 1 \pmod{p}$; произведение $(a - 1)(a^4 + a^3 + a^2 + a + 1) = a^5 - 1$ кратно p . Первый множитель не делится на p , поэтому второй – делится.

Упражнения

72 (М1324). Ни при каком целом a число $a^2 + a + 1$ не кратно а) 5; б) 11; в) 17; г) $6m - 1$, где m – натуральное число. Докажите это.

73. Всякий положительный делитель числа $a^4 - a^2 + 1$ дает остаток 1 при делении на 12. Докажите это.

74. Если порядок числа a по простому модулю p равен а) 3; б) 4; в) 15, то число а) $a^2 + a + 1$; б) $a^2 + 1$; в) $a^8 - a^7 + a^5 - a^4 + a^3 - a + 1$ кратно p . Докажите это. (Тот, кто знаком с многочленами деления круга, скажет, что это упражнение – частный случай общего утверждения: число a имеет порядок k тогда и только тогда, когда k – делитель числа $p - 1$ и $\Phi_k(a) \equiv 0 \pmod{p}$.)

75. Если по простому модулю p число a имеет порядок а) 3, то порядок числа $a + 1$ равен б) 6; в) 10, то порядок числа $a^3 - a^2 + a - 1$ равен 5. Докажите это.

76. а) Если a – натуральное число, $a > 1$, p – простое, $p > 2$, то всякий простой делитель q числа $a^p \pm 1$ является делителем числа $a \pm 1$ или имеет вид $q = 2pt + 1$, где t – натуральное. Докажите это.

б) Пусть a, b – взаимно простые целые числа, n – натуральное, q – простое, $a^n - b^n$ делится на q , и пусть ни для одного отличного от n делителя m числа n разность $a^m - b^m$ не делится на q . Докажите, что $q \equiv 1 \pmod{n}$. (Биркгоф и Вандивер, используя свойства многочленов деления круга, доказали в 1902 году, что для любых (кроме одного исключительного случая, о котором сказано ниже) натуральных взаимно простых чисел a и b , где $a > b$, и для любого натурального числа $n > 2$ существует простой делитель q разности $a^n - b^n$, не являющийся делителем ни одной разности $a^m - b^m$, где $m < n$. Единственное исключение – $a = 2, b = 1, n = 6$.)

Простые делители чисел вида $a^{2^n} + 1$

Если $a^2 + 1$ делится на простое число p , $p \neq 2$, то

$$a^2 \equiv -1 \pmod{p},$$

откуда

$$a^4 = (a^2)^2 \equiv (-1)^2 = 1 \pmod{p}.$$

Значит, порядок числа a равен одному из чисел 1, 2 и 4. Первый и второй случаи невозможны, поскольку сравнение $a^2 \equiv 1 \pmod{p}$ противоречит сравнению $a^2 \equiv -1 \pmod{p}$.

В третьем случае в силу теоремы 3 имеем: $p - 1$ делится на 4. Мы доказали довольно общее и часто используемое утверждение: *любой нечетный простой делитель числа $a^2 + 1$ имеет вид $p = 4k + 1$ (а не $4k + 3$).*

Рассуждая аналогично, можно доказать, что если p – нечетный простой делитель числа $a^{2^n} + 1$, то $p - 1$ делится на 2^{n+1} .

Верно и обратное: для любого простого числа $p = 2^{n+1}k + 1$ существует кратное ему число вида $a^{2^n} + 1$. Доказать это очень легко, если знать

теорему о существовании первообразного корня g . В самом деле, пусть $a = g^k$. Тогда

$$a^{2^n} = g^{2^n k} = g^{(p-1)/2}.$$

Число $g^{(p-1)/2}$ не сравнимо с единицей по модулю p , но квадрат этого числа есть $g^{p-1} \equiv 1 \pmod{p}$. Поэтому

$$a^{2^n} = g^{(p-1)/2} \equiv -1 \pmod{p},$$

что и требовалось.

Упражнения

77. Если числа a и b взаимно просты, то всякий нечетный простой делитель p числа $a^{2^n} + b^{2^n}$ дает остаток 1 при делении на 2^{n+1} . Докажите это.

78. Если a и n — натуральные числа, причем a четно, то числа n и $a^{2^n} + 1$ взаимно просты. Докажите это.

79. Пусть a, n — натуральные числа. Докажите, что

а) если $a^n + 1$ делится на $n + 1$, то a и n нечетны;

б) если a нечетно и $a > 1$, то существует бесконечно много натуральных n , для которых $a^n + 1$ делится на $n + 1$. (Заметьте: из пункта а) следует утверждение второй задачи, сформулированной в конце второй части статьи.)

80. а) Пусть $n > 1$ и $2^n + 2$ делится на n . Докажите, что n четно.

б) Существует бесконечно много таких натуральных n , что $2^n + 2$ кратно n . Докажите это.

Когда $2^n + 1$ делится на n ?

При помощи компьютера можно выписать несколько первых таких чисел: $2^n + 1$ делится на n при $n = 1, 3, 9, 27, 81, 171$ (заметьте: предыдущие числа — степени тройки, а $171 = 19 \cdot 9$), 243, 513, 729, 1539, 2187, 3249, 4617, 6561, 9747, 13203 (впервые возник отличный от 3 и 19 простой множитель: $13203 = 163 \cdot 81$), 13851, 19683, 29241, 39609, 41553, 59049, 61731, 87723, 97641, 118827, 124659, ...

Все эти числа (кроме единицы) делятся на 3. Как это объяснить? Рассмотрим *наименьший* простой делитель p числа n . Тогда $2^n \equiv -1 \pmod{p}$. Значит, $2^{2n} \equiv 1 \pmod{p}$, и поэтому порядок числа 2 по модулю p является делителем числа $2n$. Поскольку порядок числа по модулю p не превосходит $p - 1$, а число n не имеет простых делителей, меньших p , есть единственная возможность: порядок числа 2 по модулю p равен 2. Это значит, что $2^2 \equiv 1 \pmod{p}$, т.е. $p = 3$, что и требовалось доказать.

Упражнения

81. $2^{3^k} + 1$ делится на 3^{k+1} для любого натурального числа k . Докажите это.

82. Если n кратно 3 и $2^n + 1$ кратно n , то $2^{3n} + 1$ кратно $3n$. Докажите это.

83. Пусть a, n – натуральные числа, $n > 1$. Если $a^n + 1$ делится на n , то наименьший простой делитель числа n является делителем числа $a + 1$. Докажите это.

84. Пусть n – натуральное число, $n > 3$ и $2^n + 1$ кратно n . Докажите, что

а) n кратно 9;

б) если $n > 9$, то n кратно 27 или 19;

в) если n делится на простое число $p \neq 3$, то $p \geq 19$;

г*) если m делится на простое число p , причем $p \neq 3$ и $p \neq 19$, то $p \geq 163$.

85. Если $2^a + 1$ кратно b и $2^b + 1$ кратно a , где $a > 1$ и $b > 1$, то a и b кратны 3. Докажите это.

86 (M1260*). Найдите все такие натуральные n , для которых $2^n + 1$ кратно n^2 .

87. а) Если $2^n - 1$ кратно n , то $n = 1$. Докажите это.

б) Существует бесконечно много натуральных чисел n , для которых $\text{НОД}(2^n - 1, n) > 1$. Докажите это.

в) Пусть a – натуральное число, $a > 2$. Докажите, что множество натуральных чисел n , для которых $a^n - 1$ кратно n , бесконечно.

88. Пусть a – натуральное число, $a > 1$.

а) Существует бесконечно много таких n , что $a^n + 1$ делится на n . Докажите это.

б) При каких a существует число $n > 1$ такое, что $a^n + 1$ делится на n^2 ?

Как строят большие простые числа?

Как вы помните, для криптографической системы RSA нужны большие (лучше всего – длиной в несколько сот цифр) простые числа. Сейчас мы расскажем, как можно пытаться их строить. (Метод довольно сложный, так что при первом чтении советуем сразу перейти к следующей части статьи.)

Лемма. Пусть q – нечетное простое число, r – четное натуральное, $n = qr + 1$. Если существует такое целое число a , что $a^{n-1} \equiv 1 \pmod{n}$ и $\text{НОД}(a^r - 1, n) = 1$, то каждый простой делитель p числа n удовлетворяет сравнению $p \equiv 1 \pmod{2q}$.

Доказательство. Обозначим порядок числа a по модулю p буквой k . Поскольку $a^{n-1} \equiv 1 \pmod{p}$ и $a^{(n-1)/q} = a^r \not\equiv 1 \pmod{p}$, то k делится на q . В силу теоремы 6, число $p - 1$ делится на k . Следовательно, $p - 1$ делится на q . Кроме того, $p - 1$ четно. Лемма доказана.

Следствие. Если выполнены условия леммы и $r \leq 4q + 2$, то n – простое число.

Доказательство. Пусть n является произведением не менее чем двух простых чисел. Поскольку каждое из них не меньше $2q + 1$, получаем противоречие:

$$(2q + 1)^2 \leq n = qr + 1 \leq 4q^2 + 2q + 1.$$

Покажем теперь, как, имея большое простое число q , можно пытаться строить существенно большее простое число n . Выберем случайным образом четное число r , где $q < r \leq 4q + 2$, и положим $n = qr + 1$. Затем проверим n на отсутствие малых простых делителей. (В этом месте мы чуть лукавим: следует не только делить на малые простые числа, но и применять более хитрые методы проверки на простоту, основанные на малой теореме Ферма: если для некоторого a , взаимно простого с n , число a^{n-1} не сравнимо с 1 по модулю n , то n составное.) Если при этом выяснится, что n составное, то следует выбрать новое значение r и опять повторить вычисления.

Если же есть надежда, что n простое, то можно случайным образом выбрать число a и проверить, выполнены ли для него соотношения $a^{n-1} \equiv 1 \pmod{n}$ и $\text{НОД}(a^r - 1; n) = 1$. Если выполнены, то можно утверждать, что n простое (заметьте: $n > q^2$, так что число n записывается примерно вдвое большим количеством цифр, чем q). Если же нет, то можно взять другое значение a , и так далее.

В настоящий момент нет доказательства того, что этот алгоритм работает, и тем более – что он работает достаточно быстро. Однако на практике он позволяет строить большие (порядка 10^{300}) простые числа.

Часть IV. Первообразные корни

Примеров, в том числе весьма трудных и неожиданных, мы рассмотрели много. Перейдем к теореме Гаусса о существовании первообразного корня по любому простому модулю. Начнем опять с частных случаев.

Первообразные корни по модулю 11

Как мы помним, 2 – первообразный корень по модулю 11. Какие еще есть первообразные корни по этому модулю?

Для ответа не нужно перебирать все числа 3, 4, 5, ..., 9, 10 и составлять для каждого из них таблицу вроде таблицы 1. Некоторые степени двойки можно сразу отбросить:

$$(2^2)^5 = 2^{10} \equiv 1,$$

$$(2^4)^5 = 2^{20} \equiv 1,$$

$$\begin{aligned}(2^5)^2 &\equiv 1, \\ (2^6)^5 &\equiv 1, \\ (2^8)^5 &\equiv 1 \pmod{11}.\end{aligned}$$

А вот степени двойки $2^1 \equiv 2$, $2^3 \equiv 8$, $2^7 \equiv 7$ и $2^9 \equiv 6$, показатели которых взаимно просты с 10, являются первообразными корнями. (Обдумайте это!)

И вообще, если g — первообразный корень по простому модулю p , то g^s является первообразным корнем в том и только том случае, когда s и $p - 1$ взаимно просты.

Упражнения

89. Докажите это.

90. Для того чтобы число a было первообразным корнем по простому модулю p , необходимо и достаточно, чтобы a не делилось на p и ни для какого простого делителя q числа $p - 1$ разность $a^{(p-1)/q} - 1$ не делилась на p . Докажите это.

91. Найдите наименьшее натуральное число, являющееся первообразным корнем по модулю а) 23; б) 41; в) 257.

92. а) Проверьте, что 2 не является первообразным корнем по модулю 263, а -2 — является. б) Пусть $a^3 - a$ не делится на 83. Докажите, что ровно одно из чисел a и $-a$ является первообразным корнем по модулю 83.

93. а) Пусть p — простое число, $p \equiv 1 \pmod{4}$. Докажите, что число $-a$ является первообразным корнем по модулю p тогда и только тогда, когда само число a — первообразный корень по модулю p .

б) Пусть p — простое число, $p \equiv 3 \pmod{4}$. Докажите, что число a является первообразным корнем по модулю p тогда и только тогда, когда порядок числа $-a$ по модулю p равен $(p - 1)/2$.

Порядки классов вычетов

В таблице 14 для каждого ненулевого остатка $a \pmod{11}$ указан его порядок k :

Таблица 14

a	1	2	3	4	5	6	7	8	9	10
k	1	10	5	5	5	10	10	10	5	2

Как и должно быть, порядки — делители числа 10. Давайте посчитаем, сколько раз в нижней строке таблицы 14 встречаются числа 1, 2, 5 и 10. Ответы запишем в виде таблицы 15.

Таблица 15

Порядок	1	2	5	10
Встречается	1	1	4	4

Видна закономерность? Если нет, посмотрите на таблицу 16, составленную для $p=13$.

Таблица 16

a	1	2	3	4	5	6	7	8	9	10	11	12
k	1	12	3	6	4	12	12	4	3	6	12	2

В ней порядки – делители числа 12. Посчитаем, сколько раз встречаются в нижней строке таблицы 17 числа 1, 2, 3, 4, 6 и 12:

Таблица 17

Порядок	1	2	3	4	6	12
Встречается	1	1	2	2	2	4

Если вы все еще не догадались, составьте такие таблицы для нескольких других простых чисел p , и рано или поздно увидите, что в нижних строках этих таблиц – значения функции Эйлера: $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(10) = 4$, $\varphi(12) = 4$.

Беликий немецкий математик К.Ф.Гаусс (1777–1855) в «Арифметических исследованиях», опубликованных в 1801 году, доказал, что это не случайность, а общий закон.

Теорема 7. Среди $p - 1$ ненулевых классов вычетов по простому модулю p порядок k , где k – делитель числа $p - 1$, имеют ровно $\varphi(k)$ классов вычетов. (В частности, для любого простого числа p существует $\varphi(p - 1)$ первообразных корней по модулю p .)

Для доказательства теоремы 7 мы используем теоремы 8 и 9.

Теорема Безу

Для тех, кто знаком с делением многочленов с остатком, теорему Этьена Безу (1730–1783) можно сформулировать и доказать очень коротко. В равенство

$$f(x) = (x - a)g(x) + r,$$

где $g(x)$ – многочлен (неполное частное), а r – число (остаток),

можно подставить вместо x число a . Получим:

$$f(a) = (a - a)g(a) + r = r.$$

Значит, остаток r от деления $f(x)$ на $x - a$ равен $f(a)$. Это и есть теорема Безу.

А для остальных читателей ее можно сформулировать и доказать чуть более длинным, но не менее естественным способом.

Теорема 8. Число a является корнем многочлена $f(x)$ в том и только том случае, когда $f(x)$ делится на $x - a$, т. е. когда

$$f(x) = (x - a)g(x),$$

где g — некоторый многочлен.

Доказательство. Если $f(x) = (x - a)g(x)$, то $f(a) = (a - a)g(a) = 0$. Обратно, пусть $f(a) = 0$. Подставим в многочлен

$$f(x) = k_n x^n + k_{n-1} x^{n-1} + \dots + k_2 x^2 + k_1 x + k_0$$

число a . Получим:

$$0 = f(a) = k_n a^n + k_{n-1} a^{n-1} + \dots + k_2 a^2 + k_1 a + k_0.$$

Следовательно,

$$f(x) = f(x) - f(a) =$$

$$= k_n (x^n - a^n) + k_{n-1} (x^{n-1} - a^{n-1}) + \dots + k_2 (x^2 - a^2) + k_1 (x - a).$$

Каждая из разностей $x - a$, $x^2 - a^2 = (x - a)(x + a)$, ..., $x^n - a^n = (x - a)(x^{n-1} + x^{n-2}a + \dots + xa^{n-2} + a^{n-1})$ кратна $x - a$. Теорема доказана.

Переформулировка малой теоремы Ферма

Из теоремы Безу следует, что если a_1, a_2, \dots, a_m — различные корни многочлена $f(x)$, то $f(x) = (x - a_1)(x - a_2) \dots (x - a_m)g(x)$, где g — некоторый многочлен.

Применив это соображение к многочлену $x^{p-1} - 1$, получим замечательную переформулировку малой теоремы Ферма:

$$x^{p-1} - 1 \equiv (x - 1)(x - 2) \dots (x - p + 1),$$

где знак сравнения означает, что если раскрыть все скобки в правой части и вычесть из нее левую, то получим многочлен, коэффициенты которого кратны p . Как вы помните, для частных

случаев $p = 2, 3, 5, 7$ и 11 это разложение на множители встречалось в первой части статьи.

Упражнение 94. Подставив $x = 0$, докажите теорему Вильсона: $(p-1)! \equiv -1 \pmod{p}$ для любого простого числа p .

Сравнение $x^k \equiv 1 \pmod{p}$

Если k – делитель числа $p-1$, т.е. $p-1 = km$, то

$$x^{p-1} - 1 = (x^k - 1)(x^{k(m-1)} + x^{k(m-2)} + \dots + x^k + 1).$$

Значит, многочлен $x^k - 1$ является делителем многочлена $x^{p-1} - 1$. Поскольку $x^{p-1} - 1$ разлагается в произведение многочленов первой степени, то и его делитель $x^k - 1$ является произведением k многочленов первой степени.

Немного подумав, можно сообразить, что мы доказали следующее утверждение.

Теорема 9. Если p – простое число, k – делитель числа $p-1$, то сравнению $x^k \equiv 1 \pmod{p}$ удовлетворяют ровно k классов вычетов по модулю p .

Упражнения

95. Решите сравнения а) $x^4 \equiv 1 \pmod{13}$; б) $x^{1604} \equiv 1 \pmod{17}$. (Указание. 2 и 3 – первообразные корни, соответственно, по модулю 13 и по модулю 17.)

96. Зная, что 2 – первообразный корень по модулю 29, решите сравнение $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{29}$.

97. Пусть p – простое число. При каких k сумма $1^k + 2^k + \dots + (p-1)^k$ кратна p ?

98. а) Сколько существует таких пар (a, b) натуральных чисел, что $a, b \leq 1717$ и $a^8 + b^8$ кратно 17?

б) Сколько существует таких троек (a, b, c) натуральных чисел, что $a, b, c \leq 289$ и сумма $a^{1000} + b^{3000} + c^{9000}$ кратна 17?

Доказательство теоремы 7

Мы докажем, что если k – делитель числа $p-1$, то среди ненулевых классов вычетов по простому модулю p существует ровно $\varphi(k)$ классов порядка k .

Применим индукцию. **База.** Для $k = 1$ утверждение верно.

Переход. Рассмотрим некоторый делитель k числа $p-1$. Предположим, что для любого делителя d числа k , где $d < k$, существует ровно $\varphi(d)$ классов вычетов порядка d . Найдем количество классов вычетов порядка k .

В силу теоремы 9 сравнению $x^k \equiv 1 \pmod{p}$ удовлетворяют ровно k классов вычетов. Каждое решение x этого сравнения имеет некоторый порядок по модулю p , причем этот порядок – делитель числа k . Осталось вспомнить свойство функции Эйлера (сумма значений функции Эйлера от делителей любого натурального числа равна самому этому числу) – и становится ясно, что классов порядка k существует ровно $\varphi(k)$ штук. Теорема о существовании первообразного корня доказана.

Упражнения

99. Пусть p – простое число, $p > 3$. Найдите остаток от деления на p произведения тех из чисел $1, 2, \dots, p-1$, которые являются первообразными корнями по модулю p .

100. а) Если порядки чисел a и b по модулю p равны m и n соответственно, то порядок произведения ab – делитель числа $\text{НОК}[m; n]$. Докажите это.

б) Покажите, что порядок числа ab равен m и n , если числа m и n взаимно просты, и не обязательно равен числу $\text{НОК}[m; n]$, если m и n не взаимно просты.

101. Пусть p – простое число, $p > 2$, $p-1 = q_1^{a_1} q_2^{a_2} \dots q_s^{a_s}$ – разложение числа $p-1$ в произведение степеней различных простых чисел. Пусть g_1, g_2, \dots, g_s – такие не кратные p числа, что $g_i^{(p-1)/q_i} \not\equiv 1 \pmod{p}$ при $i = 1, 2, \dots, s$. Докажите, что число $g = g_1^{(p-1)/q_1^{a_1}} g_2^{(p-1)/q_2^{a_2}} \dots g_s^{(p-1)/q_s^{a_s}}$ – первообразный корень по модулю p . (Заметьте: мы получили еще одно доказательство существования первообразного корня по простому модулю!)

Гипотеза Артина

Как мы только что доказали, для каждого простого числа p существует первообразный корень по модулю p . Интересно: какие целые числа бывают первообразными корнями, а какие не бывают?

Очевидно, -1 является первообразным корнем только по простому модулю 2 или 3. Далее, из равенства $(a^2)^{(p-1)/2} = a^{p-1}$ следует, что точный квадрат не может быть первообразным корнем ни по какому нечетному простому модулю p .

Немецкий алгебраист Эмиль Артин (1898–1962) предположил, что для любого целого числа $g \neq -1$, не являющегося квадратом целого числа, существует бесконечно много таких простых p , что g – первообразный корень по модулю p .

Более того, некоторые вероятностные соображения привели Артина к следующему уточнению его гипотезы: если k есть наибольшее такое число, что g является k -й степенью, то отношение количества $\pi_g(n)$

простых чисел, не превосходящих n , по модулю которых g является первообразным корнем, к количеству $\pi(n)$ всех простых чисел, не превосходящих n , стремится при $n \rightarrow \infty$ к зависящему только от k пределу

$$\lim_{n \rightarrow \infty} \frac{\pi_g(n)}{\pi(n)} = \prod_{k \mid q} \left(1 - \frac{1}{q-1}\right) \cdot \prod_{k \nmid q} \left(1 - \frac{1}{q(q-1)}\right),$$

где первое произведение распространено на все простые числа q , являющиеся делителями k , а второе – на все простые числа q , не являющиеся делителями k .

К настоящему времени гипотеза Артина не доказана, хотя некоторый ее аналог, относящийся к полю рациональных функций от одной переменной над конечным полем, доказать удалось.

Часть V. Функция и числа Кармайкла

Усиление теоремы Эйлера

Рассмотрим утверждение теоремы Эйлера при $n = 360$. Очевидно, $\varphi(360) = \varphi(2^3 \cdot 5 \cdot 9) = 4 \cdot 4 \cdot 6 = 96$. Значит, для любого целого числа a , взаимно простого с 360, выполнено сравнение

$$a^{96} \equiv 1 \pmod{360}.$$

А на самом деле верно даже сравнение

$$a^{12} \equiv 1 \pmod{360}.$$

Для доказательства достаточно применить теорему Эйлера по каждому из модулей 8, 5 и 9:

$$a^4 \equiv 1 \pmod{8},$$

$$a^4 \equiv 1 \pmod{5},$$

$$a^6 \equiv 1 \pmod{9},$$

и заключить, что $a^{12} \equiv 1$ по каждому из модулей 8, 5 и 9, а значит, и по модулю 360.

В общем виде это можно сформулировать следующим образом. Рассмотрим разложение

$$n = p_1^{m_1} p_2^{m_2} \dots p_s^{m_s}$$

числа n в произведение степеней различных простых множителей. Обозначим через $f(n)$ наименьшее общее кратное чисел $\varphi(p_i^{m_i})$, где $i = 1, 2, \dots, s$. Например,

$$f(360) = \text{НОК}[\varphi(2^3); \varphi(3^2); \varphi(5)] = \text{НОК}[4; 6; 4] = 12.$$

Тогда при любом целом a , взаимно простом с n , справедливы сравнения

$$a^{f(n)} \equiv 1 \pmod{p_i^{m_i}},$$

где $i = 1, 2, \dots, s$; следовательно,

$$a^{f(n)} \equiv 1 \pmod{n}.$$

Упражнение 102. а) Для каких натуральных n верно равенство $f(n) = \varphi(n)$?

б) Пусть $n > 4$ и n не представимо ни в виде p^m , ни в виде $2p^m$, где p – нечетное простое, m – натуральное. Докажите, что невозможно так расположить все $\varphi(n)$ меньших n и взаимно простых с ним натуральных чисел вдоль окружности, чтобы для любых трех стоящих подряд чисел a, b, c разность $b^2 - ac$ делилась на n .

в) Докажите, что для этих n нет первообразного корня, т.е. нет числа g , порядок которого по модулю n равен $\varphi(n)$.

Сравнения по модулю 2^m

Пусть m – натуральное число, $m \geq 3$. Теорема Эйлера утверждает, что $a^{2^{m-1}} \equiv 1 \pmod{2^m}$ для любого нечетного числа a . На самом деле верно более сильное утверждение:

$$a^{2^{m-2}} \equiv 1 \pmod{2^m}.$$

Его легко доказать по индукции. **База** – случай $m = 3$. Число $a^2 - 1 = (a - 1)(a + 1)$ кратно 8, поскольку одно из соседних четных чисел $a - 1$ и $a + 1$ кратно 4.

Переход. Пусть утверждение верно для некоторого $m \geq 3$. Рассмотрим разложение на множители:

$$a^{2^{m-1}} - 1 = (a^{2^{m-2}} - 1)(a^{2^{m-2}} + 1).$$

Поскольку первый множитель правой части делится на 2^m , а второй множитель четен, произведение делится на 2^{m+1} , что и требовалось доказать.

Упражнение 103. Пусть a нечетно, $m \geq 3$. а) Решите сравнение $x^2 \equiv a^2 \pmod{2^m}$. б) Докажите, что сравнение $x^2 \equiv a \pmod{2^m}$ разрешимо для тех и только тех a , для которых $a \equiv 1 \pmod{8}$.

Функция Кармайкла

Через $\lambda(n)$ обозначим такое наименьшее натуральное число k , что $a^k - 1$ кратно n для любого числа a , взаимно простого с n . Функцию λ называют *функцией Кармайкла*.

Теорема 10. Для любого натурального числа l , не кратного $\lambda(n)$, существует такое взаимно простое с n целое число a , что $a^l \equiv 1 \pmod{n}$.

Доказательство. Разделим с остатком l на $\lambda(n)$. Имеем:

$$l = \lambda(n)q + r,$$

где q — целое неотрицательное, $0 < r < \lambda(n)$. При этом

$$a^l = (a^{\lambda(n)})^q \cdot a^r.$$

Поскольку $r < \lambda(n)$, хотя бы для одного взаимно простого с n числа a сравнение $a^r \equiv 1 \pmod{n}$ не выполнено. Это и требовалось доказать.

Теорема 11. $\lambda(mn) = \text{НОК}[\lambda(m); \lambda(n)]$ для любых взаимно простых натуральных чисел m и n .

Доказательство. Если целое число a взаимно просто с числами m и n , то по определению

$$a^{\lambda(m)} \equiv 1 \pmod{m},$$

$$a^{\lambda(n)} \equiv 1 \pmod{n},$$

откуда для числа $k = \text{НОК}[\lambda(m); \lambda(n)]$ имеем

$$a^k \equiv 1 \pmod{m},$$

$$a^k \equiv 1 \pmod{n},$$

так что $a^k \equiv 1 \pmod{mn}$. Таким образом, $\lambda(mn) \leq k$.

Докажем «от противного», что $\lambda(mn)$ делится как на $\lambda(m)$, так и на $\lambda(n)$. Пусть, например, $l = \lambda(mn)$ не делится на $\lambda(m)$. Тогда, в силу теоремы 10, существует такое число b , взаимно простое с m , что $b^l \not\equiv 1 \pmod{m}$.

Рассмотрим число a , для которого $a \equiv b \pmod{m}$ и a взаимно просто с n . (Почему такое a существует? Например, можно рассмотреть числа вида $b + mx$, где $x = 1, 2, \dots, n$. Они дают разные остатки при делении на n . Поскольку этих чисел n — столько же, сколько классов вычетов по модулю n , то среди них найдется и нужное нам a .) Очевидно, $a^l \equiv b^l \not\equiv 1 \pmod{n}$, что и требовалось доказать.

Теорема 12. Функция Кармайкла от степеней простых чисел такова: $\lambda(2) = 1$, $\lambda(4) = 2$, $\lambda(2^m) = 2^{m-2}$ при $m \geq 3$, $\lambda(p^m) = p^{m-1}(p-1)$ для любых нечетного простого p и натурального m .

Лемма. Порядок числа 5 по модулю 2^m , где $m \geq 3$, равен 2^{m-2} . Порядок числа $1 + p$ по модулю p^n , где p — простое, причем $p > 2$, равен p^{n-1} .

Идея доказательства леммы. Индукцией по m проверяем, что $5^{2^{m-2}}$ представимо в виде $1 + 2^m a$, где a нечетно. Аналогично, при помощи формулы бинома Ньютона индукцией по n убеждаемся, что $(1 + p)^{p^n}$ представимо в виде $1 + p^{n+1}b$, где b не делится на p .

Упражнения

104. Для любого натурального n существует взаимно простое с n целое число a , порядок которого по модулю n равен $\lambda(n)$. Докажите это.

105. Если $n = 2, 4, p^m$ или $2p^m$, где p — нечетное простое, m — натуральное, то существует первообразный корень по модулю n . Докажите это.

Числа Кармайкла

В силу малой теоремы Ферма, $2^{p-1} \equiv 1 \pmod{p}$ для любого нечетного простого числа p . Существуют ли составные числа с тем же свойством? Да, существуют:

$$2^{340} \equiv 1 \pmod{341}.$$

В самом деле, $341 = 11 \cdot 31$, причем $2^{10} - 1 = 1023 = 3 \cdot 11 \cdot 31$. (Можно проверить, что число 341 — наименьшее составное число n со свойством $2^{n-1} \equiv 1 \pmod{n}$.)

Упражнение 106. а) Если $n = (4^p - 1)/3$, где p — простое число, $p > 3$, то $2^{n-1} \equiv 1 \pmod{n}$. Докажите это.

б) (**М672**) Пусть a — такое натуральное число, что $2^a - 2$ кратно a (например, $a = 3$). Определим последовательность x_1, x_2, x_3, \dots условиями $x_1 = a, x_{n+1} = 2^{x_n} - 1$. Докажите, что $2^{x_n} - 2$ кратно x_n при любом n .

Но почему мы заинтересовались именно случаем $a = 2$? Наверное, разумнее спросить: существуют ли такие составные числа n , что для любого a , взаимно простого с n , выполнено сравнение $a^{n-1} \equiv 1 \pmod{n}$? Такие числа тоже существуют! Их называют *числами Кармайкла*. Наименьшее число Кармайкла — $561 = 3 \cdot 11 \cdot 17$, следующие за ним — $1105 = 5 \cdot 13 \cdot 17$, $1729 = 7 \cdot 13 \cdot 19$, $2465 = 5 \cdot 17 \cdot 29$, $2821 = 7 \cdot 13 \cdot 31$, $6601 = 7 \cdot 23 \cdot 41$, $8911 = 7 \cdot 19 \cdot 67$, $10585 = 5 \cdot 29 \cdot 73$, $15841 = 7 \cdot 31 \cdot 73$, $29341 =$

$= 13 \cdot 37 \cdot 61$, $41041 = 7 \cdot 11 \cdot 13 \cdot 41, \dots$ В 1994 году в журнале *Annals of Mathematics* (т. 139, с. 703–722) три математика – Альфорд, Гренвилль и Померанц – опубликовали (абсолютно недоступное для школьника) доказательство бесконечности множества чисел Кармайкла.

Упражнение 107. а) Докажите, что $a^{561} - a$ кратно числу 561 при любом целом a .

б) Докажите при $n = 1105$ сравнения $2^{n-1} \equiv 1 \equiv 3^{n-1} \pmod{n}$. (Можно доказать, что число 1105 – наименьшее составное число с таким свойством.)

Очевидно, составное число n является числом Кармайкла тогда и только тогда, когда $n - 1$ делится на $\lambda(n)$.

Теорема 13. Если составное число $n = p_1^{m_1} p_2^{m_2} \cdot \dots \cdot p_s^{m_s}$, где p_1, p_2, \dots, p_s – различные простые числа, m_1, m_2, \dots, m_s – натуральные числа, то n является числом Кармайкла в том и только том случае, когда $m_1 = m_2 = \dots = m_s = 1$ и $n - 1$ кратно каждому из чисел $p_1 - 1, p_2 - 1, \dots, p_s - 1$.

Следствие. Если n – число Кармайкла, то для любого целого числа a верно сравнение $a^n \equiv a \pmod{n}$.

Доказательство теоремы 13. Пусть n – число Кармайкла. Поскольку при $n > 2$ значение функции Кармайкла $\lambda(n)$ четно, то $n - 1$ должно быть четным. Следовательно, n нечетно.

Пусть $1 \leq i \leq s$. Поскольку $\lambda(n)$ делится на $\lambda(p_i^{m_i}) = p_i^{m_i-1}(p_i - 1)$, а $n - 1$ не делится на p_i , то в случае $m_i > 1$ получаем противоречие. Следовательно, $m_1 = m_2 = \dots = m_s = 1$. Завершение доказательства теоремы предоставляем читателю.

Упражнения

108. а) Докажите, что $2^{161038} \equiv 2 \pmod{161038}$. (При помощи компьютера легко проверить, что $n = 161038 = 2 \cdot 73 \cdot 1103$ – наименьшее четное составное число, для которого $2^n \equiv 2 \pmod{n}$. Следующее такое четное число – $215326 = 2 \cdot 23 \cdot 31 \cdot 151$.)

б) Для любого целого числа $a \neq -1$ существует такое четное число $n > 2$, что $a^n \equiv a \pmod{n}$. Докажите это.

в*) Для любого натурального числа a существует бесконечно много таких четных чисел n , что $a^n \equiv a \pmod{n}$. Докажите это. (Указание. Используйте теорему Биркгофа–Вандивера, сформулированную в упражнении 76.)

109. а) Пусть $n = 3^m - 2^m$. Докажите, что если $n - 1$ кратно m , то число $3^{n-1} - 2^{n-1}$ кратно n .

б) Существует ли составное число n , для которого $3^{n-1} - 2^{n-1}$ кратно n ?

в) (М1510) Докажите, что существует бесконечно много таких составных чисел n , что $3^{n-1} - 2^{n-1}$ кратно n .

110. Докажите, что если n – составное число и $1^{n-1} + 2^{n-1} + \dots + (n-1)^{n-1} \equiv -1 \pmod{n}$, то n – число Кармайкла. (Воспользовавшись списком чисел Кармайкла, не превосходящих 10^{16} , можно при помощи компьютера проверить, что не существует ни одного удовлетворяющего этому сравнению числа, не превосходящего 10^{16} . Существуют ли такие числа, большие 10^{16} , мы не знаем.)

«Сколько пар кроликов в один год от одной пары рождается? – спрашивал в XIII веке в «Книге об абак» Леонардо Фибоначчи (Пизанский) и сам же отвечал: – Некто поместил пару кроликов в некоем месте, огороженном со всех сторон стеной, дабы узнать, сколько пар кроликов родится при этом в течение года, если природа кроликов такова, что через месяц пара кроликов производит на свет другую пару, а рожают кролики со второго месяца после своего рождения. Так как первая пара в первом месяце дает потомство, удвой, и в этом месяце окажутся 2 пары; из них одна пара, а именно первая, рождает и в следующем месяце, так что во втором месяце оказывается 3 пары; из них в следующем месяце 2 пары дадут потомство, так что в третьем месяце родятся еще 2 пары кроликов, и число пар кроликов в этом месяце достигнет 5; из них в этом же месяце дадут потомство 3 пары, и число пар кроликов в четвертом месяце достигнет 8; из них 5 пар произведут другие 5 пар, которые, сложенные с 8 парами, дадут в пятом месяце 13 пар; из них 5 пар, рожденных в этом месяце, не дают в том же месяце потомства, а остальные 8 пар рожают, так что в шестом месяце оказывается 21 пара; сложенные с 13 парами, которые родятся в седьмом месяце, они дают 34 пары; сложенные с 21 парами, рожденными в восьмом месяце, они дают в этом месяце 55 пар; сложенные с 34 парами, рожденными в девятом месяце, они дают 89 пар; сложенные вновь с 55 парами, рожденными в десятом месяце, они дают 144 пары; снова сложенные с 89 парами, которые рожаются в одиннадцатом месяце, они дают 233 пары; сложенные вновь с 144 парами, рожденными в последнем месяце, они дают 377 пар; столько пар произвела первая пара в данном месте к концу одного года.

Действительно ... мы складываем первое число со вторым, т.е. 1 и 2; и второе с третьим; и третье с четвертым; и четвертое с пятым; и так одно за другим, пока не сложим десятое с одиннадцатым, т.е. 144 с 233; и мы получим общее число упомянутых кроликов, т.е. 377; и так можно делать по порядку до бесконечного числа месяцев».

Итак, речь идет о последовательности 1, 1, 2, 3, 5, 8, ... , каждый следующий член которой равен сумме двух предыду-

щих. Формулами это можно записать так: $\varphi_1 = \varphi_2 = 1$, $\varphi_{n+2} = \varphi_{n+1} + \varphi_n$ для любого натурального n . Вычислим несколько первых членов последовательности:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
φ_n	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610	987

n	17	18	19	20	...
φ_n	1597	2584	4181	6765	

Упражнение 1. Продолжите последовательность Фибоначчи налево (определив, что такое нулевое число Фибоначчи, минус первое, минус второе и так далее), воспользовавшись рекуррентной формулой $\varphi_n = \varphi_{n+2} - \varphi_{n+1}$.

Цепные дроби

Рассмотрим цепные дроби

$$1, 1 + \frac{1}{1} = \frac{2}{1}, 1 + \frac{1}{1 + \frac{1}{1}} = \frac{3}{2},$$

$$1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}} = 1 + \frac{1}{3/2} = \frac{5}{3}, 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}}} = 1 + \frac{1}{5/3} = \frac{8}{5}, \dots$$

Неужели это дроби вида φ_{n+1}/φ_n ? Да! В самом деле,

$$1 + \frac{1}{\varphi_{n+1}/\varphi_n} = 1 + \frac{\varphi_n}{\varphi_{n+1}} = \frac{\varphi_{n+1} + \varphi_n}{\varphi_{n+1}} = \frac{\varphi_{n+2}}{\varphi_{n+1}}.$$

Доминошки

Сколькими способами можно разрезать полоску размером $2 \times n$ на доминошки — прямоугольники размером 1×2 ? При маленьких n можно все нарисовать: обозначив искомое число способов через $f(n)$, видим из рисунков 1–4, что



Рис. 1

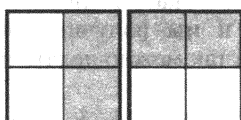


Рис. 2

$f(1) = 1$, $f(2) = 2$, $f(3) = 3$, $f(4) = 5$. Как найти $f(5)$? Левая верхняя клетка покрыта доминошкой, расположенной либо вертикально (рис.5), либо

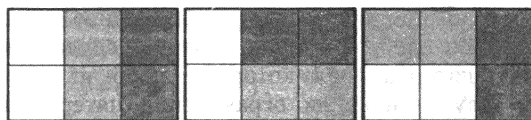


Рис. 3

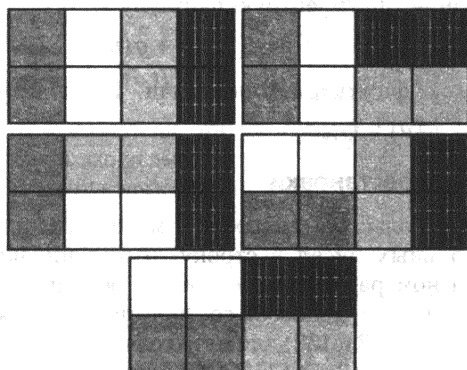


Рис. 4

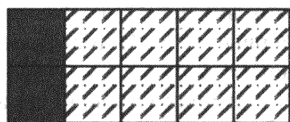


Рис. 5

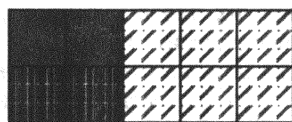


Рис. 6

горизонтально (рис.6). Значит, $f(5)$ вариантов распадаются на $f(4)$ вариантов рисунка 5 и $f(3)$ вариантов рисунка 6, т.е.

$$f(5) = f(4) + f(3) = 5 + 3 = 8.$$

Вообще, при любом $n > 1$ верна рекуррентная – выражающая следующее значение через предыдущие – формула

$$f(n+1) = f(n) + f(n-1).$$

Поскольку $f(1) = \varphi_2$ и $f(2) = \varphi_3$, то $f(n) = \varphi_{n+1}$.

Двойки и пятерки

Сколько существует n -значных чисел, составленных из цифр 2 и 5, в которых никакие две двойки не стоят рядом? Обозначим искомое количество способов через $g(n)$. Очевидно, $g(1) = 2$ и $g(2) = 3$ (годятся числа 25, 52 и 55). Легко выписать и трехзначные числа: 252, 255, 525, 552 и 555. Значит, $g(3) = 5$. Впрочем, это значение находить даже и не обязательно. Важнее

то, что любое интересующее нас $(n+1)$ -значное число начинается либо с двойки, либо с пятерки. В первом случае после двойки должна идти пятерка, после которой – любое из $g(n-1)$ чисел, во втором случае никаких ограничений пятерка не создает, получится любой из $g(n)$ вариантов.

Мы получили рекуррентную формулу

$$g(n+1) = g(n-1) + g(n),$$

совпадающую с формулой Фибоначчи. Поскольку $g(1) = \varphi_3$, $g(2) = \varphi_4$, то $g(n) = \varphi_{n+1}$.

Перестановки

Сколькими способами можно расположить первые n натуральных чисел в строку, чтобы никакое число не отличалось от номера занимаемого места больше чем на 1? Для $n=1$ и 2 ответы – 1 и 2 способа соответственно. Для $n=3$ – три перестановки 123, 213 и 132, для $n=4$ годятся пять перестановок: 1234, 1324, 2134 и 1243, 2143. Вообще, число n может стоять на n -м месте – и таких интересующих нас перестановок столько же, сколько их для $n-1$ чисел; а может на $(n-1)$ -м, и тогда на n -м месте стоит число $n-1$, а первые $n-2$ числа можно расставлять, не глядя ни на n , ни на $n-1$.

Итак, количество перестановок, в которых никакое число не сдвигается более чем на 1, – число Фибоначчи!

Упражнения

2. Докажите равенства:

- а) $\varphi_1\varphi_2 + \varphi_2\varphi_3 + \varphi_3\varphi_4 + \dots + \varphi_{2n-1}\varphi_{2n} = \varphi_{2n}^2$;
- б) $\varphi_1\varphi_2 + \varphi_2\varphi_3 + \varphi_3\varphi_4 + \dots + \varphi_{2n-1}\varphi_{2n} + \varphi_{2n}\varphi_{2n+1} = \varphi_{2n+1}^2 - 1$;
- в) $\varphi_1 + 2\varphi_2 + 3\varphi_3 + \dots + n\varphi_n = n\varphi_{n+2} - \varphi_{n+3} + 2$;
- г) $n\varphi_1 + (n-1)\varphi_2 + (n-2)\varphi_3 + \dots + 2\varphi_{n-1} + \varphi_n = \varphi_{n+4} - n - 3$.

3. По кругу выложены φ_n карточек обратной стороной вверх ($n \geq 4$). На карточках написаны неизвестные числа. Разрешено переворачивать карточки. Научитесь, перевернув не более $n-1$ карточек, находить локальный максимум – такую карточку, что написанное на ней число не меньше чисел обеих ее соседей.

Тождество Кассини

На рисунке 7 числа Фибоначчи выражают длины сторон спиральной последовательности квадратов на клетчатой бумаге. Из этого рисунка очевидна формула

$$\varphi_1^2 + \varphi_2^2 + \varphi_3^2 + \dots + \varphi_n^2 = \varphi_n\varphi_{n+1}.$$

Между числами Фибоначчи есть и другие любопытные соотношения:

$$\varphi_1 + \varphi_2 + \varphi_3 + \dots + \varphi_n = \varphi_{n+2} - 1,$$

$$\varphi_1 + \varphi_3 + \varphi_5 + \dots + \varphi_{2n-1} = \varphi_{2n},$$

$$\varphi_2 + \varphi_4 + \varphi_6 + \dots + \varphi_{2n} = \varphi_{2n+1} - 1,$$

$$\varphi_{n+1}\varphi_{n-1} - \varphi_n^2 = (-1)^n,$$

которые легко доказать по индукции. Последнее соотношение открыл в 1680 году французский астроном Джованни Доменико Кассини (1625–1712). При $n = 6$ оно превращается в числовое равенство

$$13 \cdot 5 - 8^2 = 1,$$

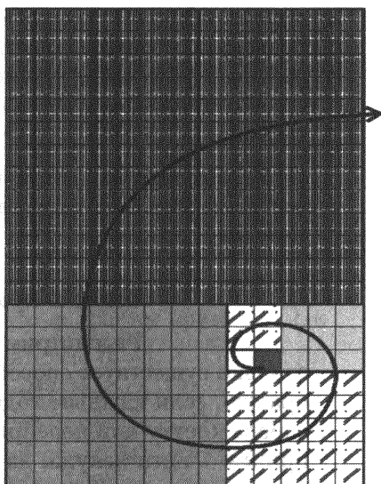


Рис. 7

которое лежит в основе геометрического парадокса: на рисунке 8 шахматная доска разрезана на четыре части, из которых на рисунке 9 сложен прямоугольник размером 5×13 . (Аналогичная конструкция при любом n разбивает квадрат со стороной φ_n на четыре части, из которых получается прямоугольник размером $\varphi_{n-1} \times \varphi_{n+1}$. Либо одна

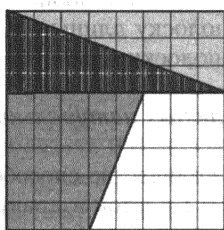


Рис. 8

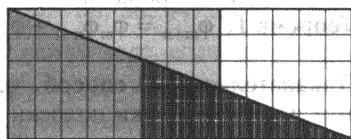


Рис. 9

клетка теряется, либо возникает лишняя — в зависимости от четности n .) Разгадка парадокса проста: на рисунке 9 линии, соединяющие левый верхний угол с нижним правым углом, на самом деле образуют не отрезок, а незаметный для глаза параллелограмм.

Если заменить в тождестве Кассини φ_{n-1} на $\varphi_{n+1} - \varphi_n$, то оно примет вид

$$\varphi_{n+1}^2 - \varphi_{n+1}\varphi_n - \varphi_n^2 = (-1)^n.$$

В статье «Уравнения Пелля» доказано, что никаких других решений в натуральных числах уравнение $x^2 - xy - y^2 = \pm 1$ не имеет. В 1970 году это и более сложные свойства были исполь-

зованы Ю.В.Матиясевичем при решении десятой проблемы Гильберта – доказательстве несуществования алгоритма, который выясняет, имеет или нет уравнение вида $P(x_1, x_2, \dots, x_n) = 0$, где P – многочлен с целыми коэффициентами, решения в целых числах.

Упражнение 4. Любой нечетный делитель d числа Фибоначчи, номер которого нечетен, удовлетворяет сравнению $d \equiv 1 \pmod{4}$. Докажите это.

Шаги и прыжки

Рассмотрим полосу из k клеток и задумаемся, сколько существует способов пройти из левой клетки полосы в правую, если каждым ходом разрешено переходить в соседнюю справа клетку или перепрыгивать через одну клетку. Очевидно, при $k = 1$ идти некуда, да и не нужно; при $k = 2$ нужно сделать ровно один шаг. Значит, при $k = 1$ или 2 число способов равно 1. Далее, если первый шаг – сдвиг на 1 клетку, то остается полоска из $k - 1$ клеток, если же первый шаг – прыжок на 2 клетки, то остается полоска из $k - 2$ клеток. Таким образом, для рассматриваемого количества способов выполнена в точности такая же рекуррентная формула, что и для чисел Фибоначчи. Поскольку и количества способов пройти полосу длины 1 или 2 равны 1, то количество способов пройти полосу длины k – в точности число Фибоначчи φ_k .

Теорема 1. $\varphi_{m+n} = \varphi_m \varphi_{n-1} + \varphi_{m+1} \varphi_n$ для любых натуральных m и n .

Доказательство. I способ. φ_{m+n} – это количество способов пройти из левой клетки полосы длиной $n + 1$ клеток в правую клетку этой же полосы, каждый раз перепрыгивая не более чем через одну клетку. Все эти способы можно разбить на два типа: $\varphi_m \varphi_{n-1}$ тех, когда перепрыгиваем через $(m + 1)$ -ю клетку, и $\varphi_{m+1} \varphi_n$ тех, когда останавливаемся на этой клетке.

II способ – индукция по n . **База.** При $n = 1$ или 2 равенства верны. **Переход.** Если верны равенства

$$\begin{cases} \varphi_{m+n} = \varphi_m \varphi_{n-1} + \varphi_{m+1} \varphi_n, \\ \varphi_{m+n+1} = \varphi_m \varphi_n + \varphi_{m+1} \varphi_{n+1}, \end{cases}$$

то

$$\begin{aligned} \varphi_{m+n+2} &= \varphi_{m+n+1} + \varphi_{m+n} = \varphi_m \varphi_n + \varphi_{m+1} \varphi_n + \varphi_m \varphi_{n-1} + \varphi_{m+1} \varphi_n = \\ &= \varphi_m (\varphi_{n-1} + \varphi_n) + \varphi_{m+1} (\varphi_n + \varphi_{n+1}) = \varphi_m \varphi_{n+1} + \varphi_{m+1} \varphi_{n+2}. \end{aligned}$$

Упражнение 5. Для любого натурального n докажите равенство:

а) $\varphi_{2n} = \varphi_{n+1}^2 - \varphi_{n-1}^2$; б) $\varphi_{3n} = \varphi_{n+1}^3 + \varphi_n^3 - \varphi_{n-1}^3$.

Формула Бине

Даниил Бернулли в 1728 году опубликовал формулу

$$\varphi_n \sqrt{5} = \left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n,$$

но о ней позабыли до 1843 г., когда ее вновь открыл француз Ж.Бине. Из этой формулы следует, что φ_n растет примерно как геометрическая прогрессия со знаменателем $\alpha = (1 + \sqrt{5})/2$, точнее, φ_n — ближайшее целое число к $\alpha^n / \sqrt{5}$.

Формулу Бине легко проверить по индукции. Но гораздо интереснее вывести ее, не зная заранее ответ. Идея излагаемого ниже способа в том, что мы временно забудем про значения $\varphi_1 = \varphi_2 = 1$ и рассмотрим всевозможные последовательности, сумма каждых двух соседних членов которых равна следующему за ними числу. Например,

$$-1, 3, 2, 5, 7, 12, 19, 31, 50, \dots$$

$$5, -1, 4, 3, 7, 10, 17, 27, 44, \dots$$

Сумма двух таких последовательностей

$$4, 2, 6, 8, 14, 22, 36, 58, 94, \dots$$

обладает тем же свойством. В самом деле, если $g_{n+2} = g_{n+1} + g_n$ и $h_{n+2} = h_{n+1} + h_n$, то $g_{n+2} + h_{n+2} = (g_{n+1} + h_{n+1}) + (g_n + h_n)$. Среди рассматриваемых последовательностей есть и геометрические прогрессии. Найдём их. Если

$$aq^{n+1} = aq^n + aq^{n-1},$$

то $q^2 = q + 1$, т.е. $q = (1 \pm \sqrt{5})/2$. Обозначим $\alpha = (1 + \sqrt{5})/2$ и $\beta = (1 - \sqrt{5})/2$. Для любых чисел a и b последовательности $a, a\alpha, a\alpha^2, a\alpha^3, \dots$ и $b, b\beta, b\beta^2, b\beta^3, \dots$ удовлетворяют рекуррентному соотношению Фибоначчи. Значит, удовлетворяет ему и последовательность $a + b, a\alpha + b\beta, a\alpha^2 + b\beta^2, a\alpha^3 + b\beta^3, \dots$

Теперь вспомним о первых двух членах: $\varphi_1 = \varphi_2 = 1$. Зная первые два члена последовательности и рекуррентное соотношение, мы можем по очереди найти их все. Поэтому если мы

подберем числа a и b так, чтобы были верны равенства $1 = a + b$ и $1 = a\alpha + b\beta$, то равенство $\varphi_n = a\alpha^{n-1} + b\beta^{n-1}$ будет верно не только для $n = 1$ или 2 , но и для любого натурального n . Очевидно, $b = 1 - a$ и $1 = a\alpha + (1 - a)\beta$, т.е. $a = \frac{1 - \beta}{\alpha - \beta} = \frac{\alpha}{\sqrt{5}}$ и $b = 1 - a = \frac{-\beta}{\sqrt{5}}$, а это и есть формула Бине.

Упражнения

6. Рассмотрим правильный пятиугольник $ABCDE$, длина стороны которого равна 1. Найдите $d = AC$.

7. Рассмотрим прямоугольник размером $1 \times d$, где $d > 1$. Отрезав от него квадрат 1×1 , получим прямоугольник размером $1 \times (d - 1)$. При каком d он подобен исходному?

8. Из равенства $\alpha^2 = \alpha + 1$ при помощи индукции выведите равенство $\alpha^n = \varphi_n \alpha + \varphi_{n-1}$.

9. В вершине A правильного восьмиугольника $AB_1C_1D_1ED_2C_2B_2$ находится лягушка. Из любой вершины восьмиугольника, кроме вершины E , она может прыгнуть в любую из двух соседних вершин. Попав в вершину E , лягушка остается там навсегда. Найдите количество способов, которыми лягушка может попасть из вершины A в вершину E ровно за n прыжков.

10 (M1053). Для любого $m > 3$ последовательность Фибоначчи содержит не менее четырех и не более пяти m -значных чисел. Докажите это.

11 (M1584). Бесконечная последовательность получается почленным сложением двух геометрических прогрессий. Может ли такая последовательность начинаться с чисел: а) 1, 1, 3 и 5; б) 1, 2, 3 и 5; в) 1, 2, 3 и 4; г) 1, 2, 3 и 2? д) Если первые четыре члена такой последовательности – рациональные числа, то и все другие члены этой последовательности – рациональные числа. Докажите это.

Производящая функция

Не менее интересен способ вывода формулы Бине, использующий производящую функцию

$$f(x) = x + x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 + 13x^7 + 21x^8 + 34x^9 + \dots$$

Домножим этот степенной ряд сначала на x , а затем еще раз на x :

$$xf(x) = x^2 + x^3 + 2x^4 + 3x^5 + 5x^6 + 8x^7 + 13x^8 + 21x^9 + 34x^{10} + \dots,$$

$$x^2f(x) = x^3 + x^4 + 2x^5 + 3x^6 + 5x^7 + 8x^8 + 13x^9 + 21x^{10} + 34x^{11} + \dots$$

Вычитая из $f(x)$ сумму $xf(x) + x^2f(x)$, получаем

$$(1 - x - x^2)f(x) = x, \text{ т.е.}$$

$$\varphi_1 x + \varphi_2 x^2 + \varphi_3 x^3 + \dots = \frac{x}{1 - x - x^2}.$$

Очевидно, $x^2 + x - 1 = (x + \alpha)(x + \beta)$. Для вывода формулы Бине достаточно разложить производящую функцию на простейшие дроби:

$$\frac{x}{1 - x - x^2} = \frac{1}{\sqrt{5}} \left(\frac{\beta}{x + \beta} - \frac{\alpha}{x + \alpha} \right)$$

и воспользоваться формулой суммы бесконечной убывающей геометрической прогрессии:

$$\frac{\beta}{x + \beta} = \frac{1}{1 - x\alpha} = 1 + x\alpha + x^2\alpha^2 + x^3\alpha^3 + x^4\alpha^4 + \dots,$$

$$\frac{\alpha}{x + \alpha} = \frac{1}{1 - x\beta} = 1 + x\beta + x^2\beta^2 + x^3\beta^3 + x^4\beta^4 + \dots$$

Заметьте: при $|x| < \frac{1}{\alpha} = \frac{\sqrt{5}-1}{2}$ ряд $x + x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 + \dots$ сходится; в частности, при $x = \frac{1}{2}$ имеем $\frac{x}{1 - x - x^2} = 2$,

поэтому

$$\frac{1}{2} + \frac{1}{4} + \frac{2}{8} + \frac{3}{16} + \frac{5}{32} + \frac{8}{64} + \frac{13}{128} + \frac{1}{256} + \dots = \sum_{n=1}^{\infty} \frac{\varphi_n}{2^n} = 2.$$

Арифметика чисел Фибоначчи

Каждое третье число Фибоначчи четно; каждое четвертое кратно 3; каждое двенадцатое оканчивается нулем.

Соседние числа Фибоначчи взаимно просты: это очевидно следует из тождества Кассини. Можно обойтись и без него: если бы φ_n и φ_{n+1} имели общий делитель $d > 1$, то на d делилось бы и предшествующее число $\varphi_{n-1} = \varphi_{n+1} - \varphi_n$, а вместе с ним $\varphi_{n-2} = \varphi_n - \varphi_{n-1}$ и так далее; но $\varphi_1 = 1$ не делится на d .

Теорема 2. $\text{НОД}(\varphi_m; \varphi_n) = \varphi_{\text{НОД}(m, n)}$, т.е. для любых натуральных m и n наибольший общий делитель чисел φ_n и φ_m — число Фибоначчи с номером $\text{НОД}(m; n)$.

Идея доказательства теоремы 2:

$$\begin{aligned} \text{НОД}(\varphi_{m+n}; \varphi_n) &= \text{НОД}(\varphi_m \varphi_{n-1} + \varphi_{m+1} \varphi_n; \varphi_n) = \\ &= \text{НОД}(\varphi_m \varphi_{n-1}; \varphi_n) = \text{НОД}(\varphi_m; \varphi_n). \end{aligned}$$

Упражнение 12. Для любого натурального m среди первых $m^2 - 1$ чисел Фибоначчи хотя бы одно число делится на m . Докажите это.

Очевидно, $\varphi_{2+1} : 2$, $\varphi_{3+1} : 3$ и $\varphi_5 : 5$. Пусть число p простое и $p > 5$. Докажем, что $\varphi_{p \pm 1} : p$, где надо брать знак $+$, если $p \equiv 2$ или $3 \pmod{5}$, и знак $-$, если $p \equiv 1$ или $4 \pmod{5}$. Доказательство использует сведения из статьи «Квадратичный закон взаимности», поэтому его лучше пропустить при первом чтении, вернувшись к нему после знакомства с символом Лежандра и с критерием Эйлера, в силу которого

$$5^{(p-1)/2} \equiv \left(\frac{5}{p}\right) \equiv \mp 1 \pmod{p}.$$

Воспользуемся формулой Бине и сравнением $(x + y)^p \equiv x^p + y^p$, которое выполнено по простому модулю в силу того, что биномиальные коэффициенты C_p^k , где $1 \leq k < p$, делятся на p :

$$\begin{aligned} \varphi_{p \pm 1} &= \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^p \alpha^{\pm 1} - \left(\frac{1 - \sqrt{5}}{2} \right)^p \beta^{\pm 1} \right) \equiv \\ &= \frac{1}{2^p \sqrt{5}} \left((1 + 5^{(p-1)/2} \sqrt{5}) \alpha^{\pm 1} - (1 - 5^{(p-1)/2} \sqrt{5}) \beta^{\pm 1} \right) \equiv \\ &\equiv \frac{1}{2^p \sqrt{5}} \left((1 \mp \sqrt{5}) \alpha^{\pm 1} - (1 \pm \sqrt{5}) \beta^{\pm 1} \right) \pmod{p}. \end{aligned}$$

Если $p \equiv 1$ или $4 \pmod{5}$, то

$$\varphi_{p-1} \equiv \frac{2}{2^p \sqrt{5}} \left((1 + \sqrt{5}) \alpha^{-1} - (1 - \sqrt{5}) \beta^{-1} \right) = 0 \pmod{p}.$$

Аналогично,

$$\varphi_{p+1} \equiv \frac{2}{2^p \sqrt{5}} \left((1 - \sqrt{5}) \alpha - (1 + \sqrt{5}) \beta \right) = 0 \pmod{p}$$

при $p \equiv 2$ или $3 \pmod{5}$.

Некоторые числа Фибоначчи кратны своему номеру: например, $\varphi_5 : 5$ и $\varphi_{12} = 144 : 12$. Много ли таких чисел?

Теорема 3. Для любого натурального числа n существует такое натуральное число m , что φ_m делится на m , а m , в свою очередь, делится на n .

Доказательство. Если $\varphi_{m_1} : m_1 : n_1$ и $\varphi_{m_2} : m_2 : n_2$, то вследствие теоремы 2 и определения наименьшего общего кратного

$$\varphi_{\text{НОК}[m_1, m_2]} : \text{НОК}[m_1, m_2] : \text{НОК}[n_1, n_2].$$

Поэтому теорему 3 достаточно доказать для степеней простых чисел.

Начнем со степеней числа 2. В силу теоремы 1,

$$\varphi_{2n} = \varphi_{n+n} = \varphi_n(\varphi_{n-1} + \varphi_{n+1}) = \varphi_n(2\varphi_{n-1} + \varphi_n).$$

Поскольку $\varphi_{12} : 2^4$, по индукции получаем: $\varphi_{3 \cdot 2^k} : 3 \cdot 2^{k+2}$ при $k \geq 2$.

Упражнение 13. Частное φ_{2n}/φ_n нечетно, если φ_n нечетно; частное не делится на 4, если φ_n делится на 4; наконец, φ_{2n}/φ_n делится на 4, если φ_n четно, но не делится на 4. Докажите это.

Другие степени простых чисел рассмотрим при помощи следующей теоремы.

Теорема 4. Если $\varphi_n : p$, где p – простое число, $p > 2$, то φ_{pn} делится на $p\varphi_n$, но не делится на $p^2\varphi_n$.

Лемма 1. $\varphi_{kn-1} \equiv \varphi_{n-1}^k$, $\varphi_{kn} \equiv k\varphi_n\varphi_{n+1}^{k-1}$ и $\varphi_{kn+1} \equiv \varphi_{n+1}^k \pmod{\varphi_n^2}$.

Доказательство леммы 1 – индукция по k . База тривиальна, переход основан на делимости числа φ_{kn} на φ_n и формуле теоремы 1 (все сравнения – по модулю φ_n^2):

$$\varphi_{(kn-1)+n} = \varphi_{kn-1}\varphi_{n-1} + \varphi_{kn}\varphi_n \equiv \varphi_{n-1}^k\varphi_{n-1} = \varphi_{n-1}^{k+1},$$

$$\begin{aligned} \varphi_{n+kn} &= \varphi_n\varphi_{kn-1} + \varphi_{n+1}\varphi_{kn} \equiv \varphi_n\varphi_{n-1}^k + \varphi_{n+1}k\varphi_n\varphi_{n+1}^{k-1} \equiv \\ &\equiv \varphi_n\varphi_{n+1}^k + k\varphi_n\varphi_{n+1}^k = (k+1)\varphi_n\varphi_{n+1}^k, \end{aligned}$$

$$\varphi_{n+(kn+1)} = \varphi_n\varphi_{kn} + \varphi_{n+1}\varphi_{kn+1} \equiv \varphi_{n+1}\varphi_{n+1}^k = \varphi_{n+1}^{k+1}.$$

Лемма 2. $\varphi_{kn} \equiv \varphi_{n+1}^k - \varphi_{n-1}^k \pmod{\varphi_n^3}$ для любых натуральных n и k .

Доказательство леммы 2 – тоже индукция по k , почти как в лемме 1. База тривиальна, да и переход несложен:

$$\begin{aligned} \varphi_{kn+n} &= \varphi_{kn}\varphi_{n-1} + \varphi_{kn+1}\varphi_n \equiv (\varphi_{n+1}^k - \varphi_{n-1}^k)\varphi_{n-1} + \varphi_{n+1}^k\varphi_n = \\ &= \varphi_{n+1}^k\varphi_{n-1} - \varphi_{n-1}^{k+1} + \varphi_{n+1}^k\varphi_n = \\ &= \varphi_{n+1}^k(\varphi_{n-1} + \varphi_n) - \varphi_{n-1}^{k+1} = \varphi_{n+1}^{k+1} - \varphi_{n-1}^{k+1} \pmod{\varphi_n^3}. \end{aligned}$$

Доказательство теоремы 4. В силу леммы 2, по модулю φ_n^3 – а значит и по модулю $p^2\varphi_n$ – верно сравнение

$$\begin{aligned} \varphi_{np} &\equiv \varphi_{n+1}^p - \varphi_{n-1}^p = \\ &= (\varphi_{n+1} - \varphi_{n-1}) \left(\varphi_{n+1}^{p-1} + \varphi_{n+1}^{p-2}\varphi_{n-1} + \dots + \varphi_{n+1}\varphi_{n-1}^{p-2} + \varphi_{n-1}^{p-1} \right). \end{aligned}$$

Первый множитель равен φ_n . Поскольку $\varphi_{n+1} = \varphi_{n-1} + \varphi_n \equiv \varphi_{n-1} \pmod{p}$, второй множитель сравним с $p\varphi_{n-1}^{p-1} \equiv 0 \pmod{p}$. Докажем, что второй множитель не делится на p^2 . Поскольку числа φ_{n+1} и φ_{n-1} не кратны p , то существует такое целое число a , что $\varphi_{n+1} \equiv a\varphi_{n-1} \pmod{p^2}$. При этом второй множитель сравним по модулю p^2 с числом $\varphi_{n-1}^{p-1} (a^{p-1} + a^{p-2} + \dots + a + 1)$, где, очевидно, $a \equiv 1 \pmod{p}$. Применение леммы 2 статьи «Периодические дроби» завершает доказательство теоремы 4.

По индукции из теоремы 4 получаем: $\varphi_{5^n} : 5^n$ и $\varphi_{3 \cdot 4^n} : 3^n \cdot 4$ для любого натурального n . Таким образом, утверждение теоремы 3 мы уже доказали для степеней простых чисел 2, 3 и 5.

Завершим доказательство теоремы 3 индукцией по наибольшему простому числу, входящему в разложение на простые множители числа n . Очевидно, как только мы для некоторого простого числа p нашли такое кратное p натуральное число m , что $\varphi_m : m$ и $m : p$, так вследствие теоремы 4 имеем $\varphi_{mp^r} : mp^r$ и $mp^r : p^{r+1}$ для любого натурального r . Таким образом, показатель степени, с которым входит число p в разложение числа m на простые множители, можно взять сколь угодно большим, если он хоть раз оказался положительным.

Как же сделать его положительным? При $p > 5$, как доказано выше, φ_{p-1} или φ_{p+1} кратно простому числу p . Числа $p+1$ и $p-1$ четные, поэтому в их разложениях на простые множители все сомножители меньше p . Следовательно, можно пользоваться индукционным предположением: можно считать, что существует такое m , что $\varphi_m : m : (p \pm 1)$, где знак выбран должным образом. Очевидно, число $\varphi_{p \cdot \text{НОК}[m, p \pm 1]}$ делится на число $p \cdot \text{НОК}[m, p+1]$, которое, в свою очередь, делится на p .

Упражнения

14. φ_{kn} делится на φ_n^2 тогда и только тогда, когда k делится на φ_n . Докажите это. (Это – тоже одно из утверждений, использованных Ю.В.Матиясевичем в его доказательстве диофантовости перечислимых подмножеств множества целых чисел.)

15. Если p и q – простые числа, причем φ_n делится на q , то φ_{np}/φ_n не делится на q . Докажите это.

Замечание. В книге Н.Н. Воробьева «Числа Фибоначчи» при помощи этого и аналогичных утверждений доказано, что любое число Фибоначчи, кроме $\varphi_1 = \varphi_2 = 1$, $\varphi_6 = 8$ и $\varphi_{12} = 144$, имеет хотя бы один простой делитель, которым не обладает ни одно из предыдущих чисел Фибоначчи.

Многие полагают: чтобы найти что-нибудь необыкновенное, надо отправиться очень далеко, лучше всего в космос. В обыденной жизни вокруг нас все хорошо известно, и ничего интересного нет. Какое заблуждение! Мы окружены загадочными явлениями, но в упор не замечаем большинство из них. Как известно, Архимед нашел для числа π приближенное значение $22/7$. Почему он предпочел седьмые доли, а не восьмые или десятые? Почему високосные годы наступают раз в четыре года? Как искать наименьшее решение уравнения Пелля? На эти и многие другие вопросы отвечают цепные дроби.

Приблизить действительное число α дробью со знаменателем n — это значит из всех дробей со знаменателями n найти ближайшую к числу α . Если на числовой оси нанесены все дроби со знаменателем n , то число α лежит между какими-то двумя дробями, т.е. для некоторого целого k имеем

$$\frac{k}{n} \leq \alpha < \frac{k+1}{n}.$$

Из этих двух дробей можно выбрать ту дробь $\frac{m}{n}$, которая ближе к α : если точка α ближе к левому концу отрезка $\left[\frac{k}{n}; \frac{k+1}{n}\right]$, разумно взять $m = k$; если ближе к правому концу, то $m = k + 1$; если же α — середина отрезка, можно условиться выбирать $m = k$, хотя это несущественно.

Процесс замены числа α его приближенным значением называют *аппроксимацией*. Для аппроксимации можно использовать дроби с любым знаменателем. На практике чаще всего используют десятичные дроби. Однако во времена Архимеда их еще не изобрели, он мог выбрать любые доли. Он выбрал седьмые. Почему? Скоро мы в этом разберемся.

При аппроксимации действительного числа α дробью $\frac{m}{n}$ возникает абсолютная погрешность $\Delta = \left| \alpha - \frac{m}{n} \right|$. Она не превышает $\frac{1}{2n}$. (Если бы мы договорились всегда брать приближение с недостатком или всегда — с избытком, то верхняя граница

абсолютной погрешности равнялась бы $1/n$.) Абсолютная погрешность достигает верхней границы $\frac{1}{2n}$, когда α – середина отрезка $[k/n; (k+1)/n]$.

Приближение «выгодное», если при не очень большом знаменателе n оно дает высокую точность. Чтобы охарактеризовать степень выгоды приближения, разумно разделить Δ на $1/n$, т.е. вычислить

$$h = \left| \alpha - \frac{m}{n} \right| : \frac{1}{n} = |n\alpha - m|.$$

Назовем h качеством приближения. Очевидно, $h \leq \frac{1}{2}$. Если h близко к нулю, то число α близко к одному из концов отрезка $\left[\frac{k}{n}; \frac{k+1}{n} \right]$. Чем ближе h к $\frac{1}{2}$, тем ближе α к середине отрезка.

Эксперимент с числом π

Не следует думать, что чем больше n , тем меньше h . Проведем опыт с числом π , аппроксимируя его разными дробями:

m/n	3/1	6/2	9/3	13/4	16/5	19/6
Δ	0,1416	0,1416	0,1416	0,1084	0,0584	0,0251
h	0,1416	0,2832	0,4248	0,4336	0,2920	0,1504

m/n	22/7	25/8	28/9	31/10	35/11	314/100
Δ	0,0013	0,0166	0,0305	0,0402	0,0402	0,0016
h	0,0089	0,1327	0,2743	0,4159	0,4424	0,1593

Седьмые доли гораздо выгоднее ближайших соседей. Если бы нам приказали приблизить π , чтобы абсолютная погрешность не превзошла 0,0013, какое n выбрали бы мы? Записав

условие $\frac{1}{2n} \leq 0,0013$, получили бы $n \geq 385$, а Архимед достиг той же точности, взяв гораздо меньший знаменатель. Теперь мы убедились, что Архимед выбрал седьмые доли не случайно?

Голландец А.Меций предлагал приближенное значение $\pi \approx 355/113$. Число Меция обладает тем же свойством, что и число Архимеда: знаменатель 113 выгоднее, чем меньшие знаменатели.

Десятичные и цепные дроби

Преимущества десятичной системы не математические, а зоологические. Если бы у нас на руках было не десять пальцев, а восемь, то человечество пользовалось бы восьмеричной системой. Поэтому откажемся от десятичных дробей и рассмотрим не зависящий от количества пальцев на руках способ приближенного представления чисел – цепные дроби.

Разложить данное число α в цепную дробь – это значит прежде всего выделить его целую часть, т.е. представить его в виде $\alpha = [\alpha] + \{\alpha\}$, где $[\alpha]$ – такое целое число, что $[\alpha] \leq \alpha < [\alpha] + 1$. Обозначаем: $a_0 = [\alpha]$. Если α – целое число, то $\{\alpha\} = 0$, процесс разложения в цепную дробь на этом обрывается. Если же $\{\alpha\} > 0$, то число α можно представить в виде $\alpha = a_0 + \frac{1}{\alpha_1}$, где $\alpha_1 > 1$. Записав $\alpha_1 = [\alpha_1] + \{\alpha_1\}$, найдем следующее неполное частное $a_1 = [\alpha_1]$. Если $\{\alpha_1\} = 0$, то разложение получено. Если же $\{\alpha_1\} > 0$, то $\alpha_1 = a_1 + \frac{1}{\alpha_2}$, где $\alpha_2 > 1$. И так далее, пока очередное число не окажется целым или – до бесконечности (точнее, пока не наступит конец света).

Если исходное число α иррационально, то и α_1 , и α_2 , и все возникающие далее такие числа иррациональны, так что процесс разложения в цепную дробь никогда не остановится и даст бесконечную последовательность a_0, a_1, a_2, \dots элементов цепной дроби – так называемых неполных частных.

Процесс разложения любого рационального числа в цепную дробь заканчивается, поскольку знаменатель разлагаемого числа все время уменьшается. Для любого нецелого рационального числа изложенная конструкция приводит к представлению, последнее неполное частное которого больше 1.

Обратите внимание: $\frac{1}{6 + \frac{1}{4}} = \frac{1}{6 + \frac{1}{3 + \frac{1}{1}}}$, или, в сокращенных

обозначениях, $[0; 6, 4] = [0; 6, 3, 1]$. Такому преобразованию (отделению единицы от последнего элемента) можно подвергнуть любую конечную цепную дробь, последний элемент которой отличен от единицы. Если же последний элемент равен единице, то его, наоборот, можно присоединить (прибавить) к пред-

последнему. Например, $[8; 10, 3, 6, 1] = [8; 10, 3, 7]$. Легко доказать, что это — единственная причина неоднозначного представления рационального числа цепной дробью.

Подходящие дроби

Цепную дробь можно оборвать, оставив элементы a_0, a_1, \dots, a_n и отбросив все остальные. Полученное таким образом число $[a_0; a_1, \dots, a_n]$ называют n -й подходящей дробью. В частности, при $n = 0$ имеем нулевую подходящую дробь $a_0/1$.

Пример.

$$\frac{61}{27} = 2 + \frac{7}{27} = 2 + \frac{1}{27/7} = 2 + \frac{1}{3 + \frac{6}{7}} = 2 + \frac{1}{3 + \frac{1}{7/6}} = 2 + \frac{1}{3 + \frac{1}{1 + \frac{1}{6}}}.$$

Следовательно, подходящие дроби таковы:

$$\frac{p_0}{q_0} = \frac{2}{1}, \quad \frac{p_1}{q_1} = 2 + \frac{1}{3} = \frac{7}{3}, \quad \frac{p_2}{q_2} = [2; 3, 1] = 2 + \frac{1}{[3; 1]} = \frac{9}{4},$$

наконец, $\frac{p_3}{q_3} = [2; 3, 1, 6] = \frac{61}{27}$. Обратите внимание:

$$\frac{2}{1} < \frac{9}{4} < \frac{61}{27} < \frac{7}{3}.$$

Следующий пример — число

$$\pi = 3 + 0,14159265\dots = 3 + \frac{1}{7 + 0,00885145\dots}.$$

Очевидно, $\frac{p_0}{q_0} = 3$ и $\frac{p_1}{q_1} = 3\frac{1}{7}$. Продолжив вычисления, можно найти $\pi = [3; 7, 15, 1, 288, \dots]$, так что $p_2/q_2 = 333/106$ и $p_3/q_3 = 355/113$.

Можно ли считать, что Архимед и Меций разоблачены: они использовали первую и третью подходящие дроби? Нет, во всяком случае про Архимеда это сказать нельзя. Мы решили математическую, но не историческую задачу. Скорее всего, Архимед использовал цепные дроби, но доказать это по дошедшим до нас работам нельзя; историки не пришли к единому мнению. Преимущество дроби $22/7$ нетрудно обнаружить и перебором.

Проще обстоит дело с Мецием. Очень трудно (хотя все равно можно!) найти дробь $335/113$ без теории. Вероятно, Меций

пользовался цепными дробями. Понятно, почему он остановился на этой дроби: следующие слишком громоздки, чтобы их можно было практически использовать.

Продолжительность года

Сутки – это период обращения Земли вокруг своей оси. Год – период обращения Земли вокруг Солнца – равен $365^d 5^h 48^m 46^s$ (т.е. 365 суток 5 часов 48 минут 46 секунд). Узаконить в обыденной жизни такую длину года невозможно. Если считать, что год – это 365^h , за четыре года отставание составит почти сутки. С зимы 1 января постепенно сместится на осень, а потом и на лето. Периодические мероприятия (посев, начало учебного года) нельзя будет связывать с определенными календарными датами.

Выход известен: некоторые года состоят из 365^d , а некоторые – високосные – из 366^d . Первым такую систему придумал для Юлия Цезаря александрийский астроном Созиген: каждый четвертый год – високосный. В христианском летоисчислении високосные годы – те, номера которых делятся на 4. Средняя длина юлианского года равна $365^d 6^h$, что больше истинной на $11^m 14^s$.

В 1582 г. папа Григорий XIII дополнил закон чередования обычных и високосных лет правилом: если номер года оканчивается двумя нулями, а число сотен не делится на 4, то год обычный (например, 2000 г. – високосный, а 1900 г. – обычный). Кроме того, считая, что от начала летоисчисления (от «рождества Христова») уже накопилась ошибка в 10^d , Григорий XIII сразу прибавил 10^d . С тех пор накопились еще 3^d (в 1700, 1800 и 1900 годах). Поэтому сейчас расхождение между юлианским и григорианским календарями составляет 13^d .

Средняя длина григорианского года равна $\left(365 \frac{97}{400}\right)^d = 365^d 5^h 49^m 12^s$, что больше истинной на 26^s . Простыми средствами достигнута хорошая точность.

В России до 1917 г. пользовались юлианским календарем. Один из немногих положительных итогов революции 1917 года – введение декретом Совета Народных Комиссаров в 1918 году григорианского календаря.

Длительность года измеряют астрономы и физики. Поэтому говорить о ее рациональности или иррациональности бессмысленно. Для наших целей можно считать, что год длится в

точности $365^d 5^h 48^m 46^s$. Рассмотрим цепную дробь: $[365; 4, 7, 1, 3, 5, 20, 6, 12]$.

Каждая из подходящих дробей: $365, 365\frac{1}{4}, 365\frac{7}{29}, 365\frac{8}{33}, 365\frac{31}{128}$ решает проблему календаря. Например, $365\frac{1}{4}$ соответствует юлианскому календарю. Пользоваться приближением $365\frac{7}{29}$ никто не предлагал (следующее приближение $365\frac{8}{33}$ немного сложнее, но значительно точнее). Календарь, по которому високосные восемь лет из каждых тридцати трех, предлагал Омар Хайям (1040–1123).

Приближение	Средняя продолжительность года	Погрешность
$1/4$	$365^d 6^h 0^m 0^s$	$-11^m 14^s$
$7/29$	$365^d 5^h 47^m 35^s$	$1^m 11^s$
$8/33$	$365^d 5^h 49^m 5^s$	-19^s
$31/128$	$365^d 5^h 48^m 45^s$	1^s

Четвертый вариант исключительно точен. В 1864 г. астроном Медлер предлагал в юлианском календаре каждые 128 лет пропускать один високосный год (ибо по юлианскому календарю на 128 лет приходится 32, а не 31 високосных).

Средняя длина григорианского года отличается от истинной на 26^s . Выходит, Григорий XIII изобрел календарь более сложный и менее точный, чем хайямовский? Его советники были плохими математиками?

Нет. Тогда продолжительность года была известна не столь точно, как сейчас. Комиссия Григория XIII пользовалась астрономическими таблицами, составленными королем Кастилии Альфонсом X (1221–1284). В них дана следующая продолжительность года: $365^d 5^h 49^m 16^s$.

На основании этих таблиц комиссия считала, что предложенная ей средняя длина года на 4^s отличается от истинной. Если бы она была знакома с предложением Хайяма, то заключила бы, что его календарь дает ошибку в 11^s .

Нет оснований предполагать, что комиссия Григория XIII использовала цепные дроби. Она кропотливо подбирала соотно-

шение обычных и високосных лет. Историки думают, что Хайям владел чем-то вроде цепных дробей: в его эпоху восточная наука во многих отношениях стояла выше европейской.

Цепная дробь числа $\sqrt{2}$

Очевидно, $(\sqrt{2} - 1)(\sqrt{2} + 1) = 2 - 1 = 1$ и, следовательно, $\sqrt{2} - 1 = \frac{1}{1 + \sqrt{2}}$. Воспользуемся этой формулой многократно:

$$\begin{aligned}\sqrt{2} &= 1 + (\sqrt{2} - 1) = 1 + \frac{1}{1 + \sqrt{2}} = 1 + \frac{1}{2 + (\sqrt{2} - 1)} = \\ &= 1 + \frac{1}{2 + \frac{1}{1 + \sqrt{2}}} = [1; 2, 2, 2, \dots].\end{aligned}$$

Подходящие дроби $1/1$, $[1; 2] = 3/2$, $[1; 2, 2] = 7/5$, $[1; 2, 2, 2] = 17/12$ встретятся вам в статье «Уравнения Пелля» (настоятельно рекомендуем вам ознакомиться хотя бы с первой частью этой статьи – см. «Квант» №3 за 2002 г.). Это не случайное совпадение: если n -этажная дробь (в которой n двоек) приводится к несократимому виду x/y , то $(n+1)$ -этажная дробь равна

$$1 + \frac{1}{1 + \frac{x}{y}} = 1 + \frac{y}{x + y} = \frac{x + 2y}{x + y}.$$

Очевидно,

$$\text{НОД}(x + 2y; x + y) = \text{НОД}(y; x + y) = \text{НОД}(x; y),$$

так что дробь $\frac{x + 2y}{x + y}$ тоже несократима. Поэтому увеличение количества дробных черт на единицу – это переход от несократимой дроби $\frac{x}{y}$ к несократимой дроби $\frac{x + 2y}{x + y}$; а это и есть формулы статьи «Уравнения Пелля».

Упражнение 1. Если x/y – подходящая дробь числа $\sqrt{2}$, то $|x^2 - 2y^2| = 1$. Докажите это.

Подходящие дроби $1/1$, $3/2$, $7/5$, $17/12$, ... замечательны тем, что дают (попеременно, слева и справа) весьма точные

приближения числа $\sqrt{2}$. А именно,

$$\frac{1}{1} < \frac{7}{5} < \frac{41}{29} < \frac{239}{169} < \dots < \sqrt{2} < \dots < \frac{577}{408} < \frac{99}{70} < \frac{17}{12} < \frac{3}{2}.$$

Оценить погрешность приближения несложно:

$$\left| \frac{x}{y} - \sqrt{2} \right| = \left| \frac{(x - y\sqrt{2})(x + y\sqrt{2})}{y(x + y\sqrt{2})} \right| = \left| \frac{x^2 - 2y^2}{y^2 \left(\frac{x}{y} + \sqrt{2} \right)} \right| = \frac{1}{y^2 \left(\frac{x}{y} + \sqrt{2} \right)}.$$

Например,

$$0 < \frac{17}{12} - \sqrt{2} = \frac{1}{12^2 \left(\sqrt{2} + \frac{17}{12} \right)} < \frac{1}{12^2 \cdot 2\sqrt{2}} < 0,0025,$$

$$0 < \sqrt{2} - \frac{41}{29} = \frac{1}{29^2 \left(\sqrt{2} + \frac{41}{29} \right)} < \frac{1}{12^2 \cdot 2 \cdot \frac{41}{29}} < 0,00042.$$

Цепная дробь числа $\sqrt{3}$

Аналогично числу $\sqrt{2}$, разложим в цепную дробь число $\sqrt{3}$. Очевидно,

$$\begin{aligned} \sqrt{3} &= 1 + (\sqrt{3} - 1) = 1 + \frac{1}{(\sqrt{3} + 1)/2} = \\ &= 1 + \frac{1}{1 + \frac{\sqrt{3} - 1}{2}} = 1 + \frac{1}{1 + \frac{1}{\sqrt{3} + 1}} = 1 + \frac{1}{1 + \frac{1}{2 + (\sqrt{3} - 1)}} = \\ &= [1; 1, 2, 1, 2, 1, 2, \dots]. \end{aligned}$$

Подходящие дроби: $[1] = \frac{1}{1}$, $[1; 1] = \frac{2}{1}$, $[1; 1, 2] = \frac{5}{3}$, $[1; 1, 2, 1] = \frac{7}{4}$, $[1; 1, 2, 1, 2] = \frac{19}{11}$, $[1; 1, 2, 1, 2, 1] = \frac{26}{15}$. Заметьте: $1^2 - 3 \cdot 1^2 = -2$, $2^2 - 3 \cdot 1^2 = 1$, $5^2 - 3 \cdot 3^2 = -2$, $7^2 - 3 \cdot 4^2 = 1$, $19^2 - 3 \cdot 11^2 = -2$, $26^2 - 3 \cdot 15^2 = 1$, так что половина дробей «лишние» — они дают решения не уравнения $x^2 - 3y^2 = 1$, а уравнения $x^2 - 3y^2 = -2$. (Подходящие дроби числа $\sqrt{2}$ обладают аналогичным свойством.) Мы вскоре докажем, что если $x^2 - dy^2 = 1$ и x, y —

натуральные числа, то x/y – подходящая дробь числа \sqrt{d} ; значит, для поиска решения $(x; y)$ уравнения Пелля следует перебирать лишь подходящие дроби числа \sqrt{d} . А вот обратное утверждение, как видно на примерах $d = 2$ и $d = 3$, ложно: не каждая подходящая дробь соответствует решению уравнения Пелля.

Правило Эйлера

Примеры убедили вас в полезности цепных дробей. Поэтому мы займемся их систематическим изучением. Рассмотрим иррациональное число α , разложим его в цепную дробь $\alpha = [a_0; a_1, a_2, a_3, \dots]$ и образуем одну за другой подходящие дроби

$$\frac{p_0}{q_0} = \frac{a_0}{1}, \quad \frac{p_1}{q_1} = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} \quad \text{и}$$

$$\frac{p_2}{q_2} = a_0 + \frac{1}{[a_1; a_2]} = a_0 + \frac{a_2}{a_1 a_2 + 1} = \frac{a_0 a_1 a_2 + a_0 + a_2}{a_1 a_2 + 1}.$$

Далее,

$$\begin{aligned} \frac{p_3}{q_3} &= a_0 + \frac{1}{[a_1; a_2, a_3]} = \\ &= a_0 + \frac{a_2 a_3 + 1}{a_1 a_2 a_3 + a_1 + a_3} = \frac{a_0 a_1 a_2 a_3 + a_0 a_1 + a_0 a_3 + a_2 a_3 + 1}{a_1 a_2 a_3 + a_1 + a_3}. \end{aligned}$$

Обозначим $p_n = [a_0, a_1, \dots, a_n]$ и $[] = 1$. Очевидно, $q_n = [a_1, \dots, a_n]$ и

$$[a_0; a_1, a_2, \dots, a_n] = \frac{p_n}{q_n} = \frac{[a_0, a_1, \dots, a_n]}{[a_1, \dots, a_n]}.$$

n	0	1	2	3
p_n	a_0	$a_0 a_1 + 1$	$a_0 a_1 a_2 + a_0 + a_2$	$a_0 a_1 a_2 a_3 + a_0 a_1 + a_0 a_3 + a_2 a_3 + 1$
q_n	1	a_1	$a_1 a_2 + 1$	$a_1 a_2 a_3 + a_1 + a_3$

Из равенства

$$\begin{aligned} [a_0; a_1, a_2, \dots, a_n] &= a_0 + \frac{1}{[a_1; a_2, \dots, a_n]} = \\ &= a_0 + \frac{[a_2, \dots, a_n]}{[a_1, a_2, \dots, a_n]} = \frac{a_0 [a_1, a_2, \dots, a_n] + [a_2, \dots, a_n]}{[a_1, a_2, \dots, a_n]} \end{aligned}$$

получаем формулу

$$[a_0, a_1, a_2, \dots, a_n] = a_0 [a_1, a_2, \dots, a_n] + [a_2, \dots, a_n]. \quad (*)$$

Это рекуррентное соотношение позволяет по очереди вычислять числители и знаменатели подходящих дробей. Если пристмотреться, однако, можно обнаружить явную формулу – *правило Эйлера*. Рассмотрим произведение $a_0 a_1 \dots a_n$, затем – всевозможные произведения, которые можно получить, вычеркнув пару рядом стоящих букв, затем – произведения, получаемые вычеркиванием двух пар рядом стоящих букв, и так далее. Сумма всех таких произведений и равна $[a_0, a_1, \dots, a_n]$. (Если $n + 1$ четно, на последнем шаге отбрасыванием всех элементов получаем произведение нуля множителей; оно по определению равно 1.)

Суть доказательства правила Эйлера в том, что выражение $[a_2, \dots, a_n]$ состоит из тех слагаемых суммы $[a_0, a_1, a_2, \dots, a_n]$, в которых вычеркнута пара $a_0 a_1$, а произведение $a_0 [a_1, a_2, \dots, a_n]$ – из тех, где эта пара не вычеркнута.

Рекуррентные формулы

Из правила Эйлера следует, что величина $[a_0, a_1, \dots, a_n]$ не меняется, если записать числа в обратном порядке: $[a_0, a_1, \dots, a_n] = [a_n, \dots, a_1, a_0]$.

Теорема 1. $p_n = a_n p_{n-1} + p_{n-2}$ и $q_n = a_n q_{n-1} + q_{n-2}$. (Чтобы эти равенства были верны и для $n = 1$, считаем по определению $p_{-1} = 1$ и $q_{-1} = 0$.)

Доказательство. В силу (*) имеем

$$\begin{aligned} p_n &= [a_0, \dots, a_{n-1}, a_n] = [a_n, a_{n-1}, \dots, a_0] = \\ &= a_n [a_{n-1}, \dots, a_0] + [a_{n-2}, \dots, a_0] = a_n [a_0, \dots, a_{n-1}] + [a_0, \dots, a_{n-2}] = \\ &= a_n p_{n-1} + p_{n-2}. \end{aligned}$$

Доказательство равенства $q_n = a_n q_{n-1} + q_{n-2}$ аналогично.

Теорема 2. $p_{n-1} q_n - p_n q_{n-1} = (-1)^n$.

Доказательство – индукция по n . **База.** $p_0 q_1 - p_1 q_0 = a_0 a_1 - (a_0 a_1 + 1) \cdot 1 = -1$ (или, если угодно, $p_{-1} q_0 - p_0 q_{-1} = 1 \cdot 1 - a_0 \cdot 0 = 1$).

Переход. Если для некоторого n равенство верно, то

$$\begin{aligned} p_n q_{n+1} - p_{n+1} q_n &= p_n \cdot (a_{n+1} q_n + q_{n-1}) - (a_{n+1} p_n + p_{n-1}) q_n = \\ &= p_n q_{n-1} - p_{n-1} q_n = -(-1)^n = (-1)^{n+1}. \end{aligned}$$

Теорема 3. $\frac{p_{n-1}}{q_{n-1}} - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n q_{n-1}}$ и $\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{(-1)^n a_n}{q_n q_{n-2}}$.

Доказательство. Первое равенство прямо следует из теоремы 2, а второе получаем при помощи теоремы 1 естественным вычислением:

$$\begin{aligned} p_n q_{n-2} - p_{n-2} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-2} - p_{n-2} (a_n q_{n-1} + q_{n-2}) = \\ &= a_n p_{n-1} q_{n-2} - p_{n-2} a_n q_{n-1} = a_n (-1)^n. \end{aligned}$$

Подходящие дроби

Подходящие дроби $p_0/q_0, p_2/q_2, p_4/q_4, \dots$ иррационального числа α в силу теоремы 3 образуют возрастающую последовательность, а подходящие дроби $p_1/q_1, p_3/q_3, p_5/q_5, \dots$ – убывающую. Значение цепной дроби заключено между этими двумя последовательностями:

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \dots < \alpha < \dots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

Таким образом, α лежит любыми двумя последовательными подходящими дробями и, следовательно,

$$\left| \alpha - \frac{p_n}{q_n} \right| < \left| \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} \right| = \frac{1}{q_{n+1} q_n}.$$

Поскольку $q_{n+1} = a_{n+1} q_n + q_{n-1} > a_{n+1} q_n$, то

$$\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{a_{n+1} q_n^2} \leq \frac{1}{q_n^2}.$$

Далее, для любого n дробь p_{n+2}/q_{n+2} лежит между α и p_n/q_n , следовательно,

$$\left| \alpha - \frac{p_n}{q_n} \right| > \left| \frac{p_{n+2}}{q_{n+2}} - \frac{p_n}{q_n} \right| = \frac{|p_{n+2} q_n - p_n q_{n+2}|}{q_{n+2} q_n} = \frac{a_{n+2}}{q_{n+2} q_n} \geq \frac{1}{(q_{n+1} + q_n) q_n},$$

поскольку $a_{n+2} (q_{n+1} + q_n) \geq a_{n+2} q_{n+1} + q_n = q_{n+2}$.

Таким образом, $|q_n \alpha - p_n| > \frac{1}{q_{n+1} + q_n}$. Как вы помните,

$|q_{n+1} \alpha - p_{n+1}| < \frac{1}{q_{n+2}} \leq \frac{1}{q_{n+1} + q_n}$. Поэтому с ростом номера подходящей дроби величина h уменьшается. Приближения становятся все качественнее!

Теорема 4. Если p, q – целые числа, причем $1 \leq q < q_n$, то

$|q\alpha - p| > |p_n\alpha - q_n|$ и, следовательно,

$$\left| \alpha - \frac{p}{q} \right| = \frac{|q\alpha - p|}{q} > \frac{|q_n\alpha - p_n|}{q_n} = \left| \alpha - \frac{p_n}{q_n} \right|.$$

Доказательство. Дробь p/q расположена либо левее числа a_0 , и тогда

$$q \left| \alpha - \frac{p}{q} \right| > q |\alpha - a_0| \geq |1 \cdot \alpha - a_0| = |q_0\alpha - p_0| \geq |q_n\alpha - p_n|;$$

либо p/q расположена между двумя промежуточными дробями p_{k-1} и p_{k+1} с номерами одной четности, и тогда имеем

$$\frac{1}{qq_{k-1}} \leq \frac{|pq_{k-1} - qp_{k-1}|}{qq_{k-1}} = \left| \frac{p}{q} - \frac{p_{k-1}}{q_{k-1}} \right| < \left| \frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} \right| = \frac{1}{q_k q_{k-1}},$$

откуда $q > q_k$ и поэтому $n > k$, и

$$q \left| \alpha - \frac{p}{q} \right| \geq q \left| \frac{p}{q} - \frac{p_{k+1}}{q_{k+1}} \right| = \frac{|pq_{k+1} - qp_{k+1}|}{q_{k+1}} \geq |q_k\alpha - p_k| > |q_n\alpha - p_n|;$$

либо число p/q расположено правее числа p_1/q_1 , и тогда

$$q \left| \alpha - \frac{p}{q} \right| > q \left| \frac{p_1}{q_1} - \frac{p}{q} \right| = \frac{|p_1q - q_1p|}{q_1} \geq \frac{1}{q_1} > \\ > |1 \cdot \alpha - a_0| = |q_0\alpha - p_0| \geq |q_n\alpha - p_n|.$$

Таким образом, получив, например, для числа $\sqrt{2}$ подходящую дробь $\frac{p_3}{q_3} = [1; 2, 2, 2] = \frac{17}{12}$, мы можем быть уверены, что точнее приблизить число $\sqrt{2}$ дробью со знаменателем, меньшим 12, невозможно.

Теорема Гурвица-Бореля

Подходящие дроби, как мы только что доказали, являются наилучшими приближениями. Насколько точны эти приближения?

Теорема 5. Для любого натурального n верно хотя бы одно из неравенств

$$\left| \alpha - \frac{p_{n-1}}{q_{n-1}} \right| < \frac{1}{2q_{n-1}^2} \quad \text{и} \quad \left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{2q_n^2}.$$

Доказательство. Поскольку число α расположено между p_{n-1}/q_{n-1} и p_n/q_n , то

$$\left| \frac{p_{n-1}}{q_{n-1}} - \alpha \right| + \left| \alpha - \frac{p_n}{q_n} \right| = \left| \frac{p_{n-1}}{q_{n-1}} - \frac{p_n}{q_n} \right| = \frac{1}{q_n q_{n-1}} < \frac{1}{2q_n^2} + \frac{1}{2q_{n-1}^2}$$

(последнее неравенство выражает собой тот факт, что среднее геометрическое величин $1/q_n^2$ и $1/q_{n-1}^2$ меньше их среднего арифметического; равенство могло бы выполняться лишь при $q_{n-1} = q_n$, что в данном случае невозможно). Отсюда, очевидно, непосредственно следует утверждение теоремы 5.

Теорема 6 (Гурвиц и Борель). Для любого натурального n верно хотя бы одно из неравенств $\left| \alpha - \frac{p_{n-1}}{q_{n-1}} \right| < \frac{1}{\sqrt{5}q_{n-1}^2}$, $\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{\sqrt{5}q_n^2}$ и $\left| \alpha - \frac{p_{n+1}}{q_{n+1}} \right| < \frac{1}{\sqrt{5}q_{n+1}^2}$.

Доказательство. Для любого натурального k имеем

$$\alpha = [a_0; a_1, a_2, \dots, a_k, a_{k+1}] = \frac{\alpha_{k+1}p_k + p_{k-1}}{\alpha_{k+1}q_k + q_{k-1}}.$$

(Эта формула еще не раз пригодится нам.) Значит,

$$\left| \alpha - \frac{p_k}{q_k} \right| = \left| \frac{\alpha_{k+1}p_k + p_{k-1}}{\alpha_{k+1}q_k + q_{k-1}} - \frac{p_k}{q_k} \right| = \frac{1}{(\alpha_{k+1}q_k + q_{k-1})q_k}.$$

Обозначим $\Psi_k = \alpha_{k+1} + \frac{q_{k-1}}{q_k}$.

Лемма. Если $\Psi_k \leq \sqrt{5}$ и $\Psi_{k+1} \leq \sqrt{5}$, то $\frac{q_k}{q_{k+1}} > \frac{\sqrt{5}-1}{2}$.

Доказательство. Обозначим $x = q_k/q_{k+1}$. Неравенство $\Psi_{k+1} \leq \sqrt{5}$ запишем в виде $\alpha_{k+2} \leq \sqrt{5} - x$, а неравенство $\Psi_k \leq \sqrt{5}$ преобразуем так:

$$\sqrt{5} \geq \alpha_{k+1} + \frac{q_{k-1}}{q_k} = \frac{1}{\alpha_{k+2}} + a_{k+1} + \frac{q_{k-1}}{q_k} = \frac{1}{\alpha_{k+2}} + \frac{q_{k+1}}{q_k},$$

т.е. $\frac{1}{\alpha_{k+2}} \leq \sqrt{5} - \frac{1}{x}$. Перемножая, получаем

$$1 = \alpha_{k+2} \cdot \frac{1}{\alpha_{k+2}} \leq (\sqrt{5} - x) \left(\sqrt{5} - \frac{1}{x} \right),$$

т.е. $0 \leq 5 - \sqrt{5} \left(x + \frac{1}{x} \right)$, $x^2 - x\sqrt{5} + 1 \leq 0$,

$$\left(x - \frac{\sqrt{5}-1}{2} \right) \cdot \left(x - \frac{\sqrt{5}+1}{2} \right) \leq 0,$$

наконец, $\frac{\sqrt{5}-1}{2} \leq x \leq \frac{\sqrt{5}+1}{2}$. Первое из этих неравенств и требовалось доказать. (Равенство невозможно, ибо число $x = q_k/q_{k+1}$ рациональное.)

Применяя лемму при $k = n-1$ и $k = n$, получаем противоречащее натуральности числа a_{n+1} неравенство

$$a_{n+1} = \frac{q_{n+1}}{q_n} - \frac{q_{n-1}}{q_n} < \frac{2}{\sqrt{5}-1} - \frac{\sqrt{5}-1}{2} = 1.$$

Теорему 5 можно частично обратить.

Теорема 7. *Всякая несократимая дробь a/b , удовлетворяющая неравенству $\left| \alpha - \frac{a}{b} \right| < \frac{1}{2b^2}$, является более качественным приближением, чем все дроби с меньшими знаменателями, и поэтому — подходящей дробью числа.*

Доказательство. Пусть $|d\alpha - c| \leq |b\alpha - a|$, где $\frac{a}{b} \neq \frac{c}{d}$. Очевидно,

$$\frac{1}{bd} \leq \frac{|bc - ad|}{bd} = \left| \frac{c}{d} - \frac{a}{b} \right| \leq \left| \frac{c}{d} - \alpha \right| + \left| \alpha - \frac{a}{b} \right| < \frac{1}{2bd} + \frac{1}{2b^2} = \frac{b+d}{2b^2d},$$

откуда $2b < b + d$, т.е. $b < d$, что и требовалось доказать.

Следствие. *Если x , y , d — натуральные числа, причем $x^2 - dy^2 = 1$, то x/y — подходящая дробь числа \sqrt{d} .*

Доказательство.
$$\frac{x}{y} - \sqrt{d} = \frac{x^2 - dy^2}{y(x + y\sqrt{d})} = \frac{1}{y(x + y\sqrt{d})} < \frac{1}{2y^2}.$$

Все цепные дроби чисел \sqrt{d} , где d — не являющееся квадратом натуральное число, при $d \leq 48$, как видно из таблицы, периодические.

d	Цепная дробь числа \sqrt{d}	x	y	$x^2 - dy^2$
2	1; 2 , 2,2,2,2,2,2,2,2,2,2	1	1	-1
3	1; 1,2 , 1,2,1,2,1,2,1,2,1,2	2	1	1
5	2; 4 , 4,4,4,4,4,4,4,4,4,4	2	1	-1
6	2; 2,4 , 2,4,2,4,2,4,2,4,2,4	5	2	1
7	2; 1,1,1,4 , 1,1,1,4,1,1,1,4	8	3	1
8	2; 1,4 , 1,4,1,4,1,4,1,4,1,4	3	1	1
10	3; 6 , 6,6,6,6,6,6,6,6,6,6	3	1	-1
11	3; 3,6 , 3,6,3,6,3,6,3,6,3,6	10	3	1
12	3; 2,6 , 2,6,2,6,2,6,2,6,2,6	7	2	1
13	3; 1,1,1,1,6 , 1,1,1,1,6,1,1	18	5	-1
14	3; 1, 2,1,6 , 1,2,1,6,1,2,1,6	15	4	1
15	3; 1,6 , 1,6,1,6,1,6,1,6,1,6	4	1	1
17	4; 8 , 8,8,8,8,8,8,8,8,8,8	4	1	-1
18	4; 4,8 , 4,8,4,8,4,8,4,8,4,8	17	4	1
19	4; 2,1,3,1,2,8 , 2,1,3,1,2,8	170	39	1
20	4; 2,8 , 2,8,2,8,2,8,2,8,2,8	9	2	1
21	4; 1,1,2,1,1,8 , 1,1,2,1,1,8	55	12	1
22	4; 1,2,4,2,1,8 , 1,2,4,2,1,8	197	42	1
23	4; 1,3,1,8 , 1,3,1,8,1,3,1,8	24	5	1
24	4; 1,8 , 1,8,1,8,1,8,1,8,1,8	5	1	1
26	5; 10 , 10,10,10,10,10,10,10	5	1	-1
27	5; 5,10 , 5,10,5,10,5,10,5,10	26	5	1
28	5; 3,2,3,10 , 3,2,3,10,3,2,3	127	24	1
29	5; 2,1,1,2,10 , 2,1,1,2,10,2	70	13	-1
30	5; 2,10 , 2,10,2,10,2,10,2,10	11	2	1
31	5; 1,1,3,5,3,1,1,10 , 1,1,3,5	1520	273	1
32	5; 1,1,1,10 , 1,1,1,10,1,1,1	17	3	1
33	5; 1,2,1,10 , 1,2,1,10,1,2,1	23	4	1
34	5; 1,4,1,10 , 1,4,1,10,1,4,1	35	6	1
35	5; 1,10 , 1,10,1,10,1,10,1,10	6	1	1
37	6; 12 , 12,12,12,12,12,12,12	6	1	-1
38	6; 6,12 , 6,12,6,12,6,12,6,12	37	6	1
39	6; 4,12 , 4,12,4,12,4,12,4,12	25	4	1
40	6; 3,12 , 3,12,3,12,3,12,3,12	19	3	1
41	6; 2,2,12 , 2,2,12,2,2,12,2,2	32	5	-1
42	6; 2,12 , 2,12,2,12,2,12,2,12	13	2	1
43	6; 1,1,3,1,5,1,3,1,1,12 , 1,1	3482	531	1
44	6; 1,1,1,2,1,1,1,12 , 1,1,1,2	199	30	1
45	6; 1,2,2,2,1,12 , 1,2,2,2,1	161	24	1
46	6; 1,3,1,1,2,6,2,1,1,3,1,12	24335	3588	1
47	6; 1,5,1,12 , 1,5,1,12,1,5,1	48	7	1
48	6; 1,12 , 1,12,1,12,1,12,1,12	7	1	1

Теорема 8 (Ж. Л. Лагранж, 1770 г.). *Всякая периодическая цепная дробь – квадратичная иррациональность, а всякая квадратичная иррациональность – периодическая цепная дробь.*

Доказательство. Для числа α , изображаемого цепной дробью с периодом длины r и предпериодом длины s , верно равенство $\alpha_{r+s} = \alpha_s$. Выражая из равенств $\alpha = \frac{p_{s-1}\alpha_s + p_{s-2}}{q_{s-1}\alpha_s + q_{s-2}}$ и $\alpha = \frac{p_{r+s-1}\alpha_{r+s} + p_{r+s-2}}{q_{r+s-1}\alpha_{r+s} + q_{r+s-2}}$ числа α_s и α_{r+s} через α , получаем уравнение $\frac{p_{s-2} - q_{s-2}\alpha}{q_{s-1}\alpha - p_{s-1}} = \frac{p_{r+s-2} - q_{r+s-2}\alpha}{q_{r+s-1}\alpha - p_{r+s-1}}$, откуда, освобождаясь от знаменателей, приходим к квадратному уравнению.

Упражнение 2. Докажите, что после освобождения от знаменателей и приведения подобных получаем именно квадратное уравнение, а не тождество $0 = 0$.

Докажем периодичность цепной дроби квадратичной иррациональности α . Подставив $\alpha = \frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}}$ в квадратное уравнение $ax^2 + bx + c = 0$ с целыми коэффициентами a, b, c , которому удовлетворяет число α , получаем уравнение $A_n\alpha^2 + B_n\alpha + C_n = 0$, где

$$A_n = ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2,$$

$$C_n = ap_{n-2}^2 + bp_{n-2}q_{n-2} + cq_{n-2}^2,$$

$$B_n = 2ap_{n-1}p_{n-2} + b(p_{n-1}q_{n-2} + p_{n-2}q_{n-1}) + 2cq_{n-1}q_{n-2}.$$

Поскольку $\left| \alpha - \frac{p_{n-1}}{q_{n-1}} \right| < \frac{1}{q_{n-1}^2}$, то $p_{n-1} = \alpha q_{n-1} + \epsilon$, где $|\epsilon| < \frac{1}{q_{n-1}}$. Следовательно,

$$\begin{aligned} A_n &= a(\alpha q_{n-1} + \epsilon)^2 + b(\alpha q_{n-1} + \epsilon)q_{n-1} + cq_{n-1}^2 = \\ &= (a\alpha^2 + b\alpha + c)q_{n-1}^2 + 2a\alpha\epsilon q_{n-1} + a\epsilon^2 + b\epsilon q_{n-1}, \end{aligned}$$

откуда $|A_n| = |2a\alpha\epsilon q_{n-1} + a\epsilon^2 + b\epsilon q_{n-1}| < 2|a\alpha| + |a| + |b|$. Таким образом, A_n (а в силу равенства $C_n = A_{n-1}$ таким свойством обладает и C_n) при изменении n может принимать лишь конечное множество значений.

Дискриминант квадратного уравнения не меняется ни при параллельном переносе графика вдоль оси абсцисс, ни при

замене старшего коэффициента на свободный член и одновременной замене свободного члена на старший коэффициент. Поэтому $B_n^2 - 4A_nC_n = b^2 - 4ac$ и для B_n имеем лишь конечное множество возможных значений. Таким образом, множество возможных троек $(A_n; B_n; C_n)$ конечно. Поскольку n можно брать сколь угодно большим, то для некоторых r и s имеем $\alpha_s = \alpha_{r+s}$, а это и означает, что цепная дробь числа α периодическая.

Замечание. На компьютере можно вычислить: $\sqrt[3]{2} = [1; 3, 1, 5, 1, 1, 4, 1, 1, 8, 1, 14, 1, 10, 2, 1, 4, 12, 2, 3, 2, 1, 3, 4, 1, 1, 2, 14, 3, 12, 1, 15, 3, 1, 4, 534, 1, 1, 5, 1, 1, 121, 1, 2, 2, 4, 10, 3, 2, 2, 41, 1, 1, 1, 3, 7, 2, 2, 9, 4, 1, 3, 7, 6, 1, 1, 2, 9, 2, 3, 3, 1, 1, 69, 1, 12, \dots]$. Ограничена или нет последовательность неполных частных цепной дроби числа $\sqrt[3]{2}$ (или любого алгебраического числа степени выше 2), неизвестно.

Теорема Галуа

Какие квадратичные иррациональности разлагаются в чисто периодические цепные дроби? На этот вопрос ответил Эварист Галуа в 1828 г.

Определение. Корень α квадратного уравнения с целыми коэффициентами называют приведенной квадратичной иррациональностью, если $\alpha > 1$, а второй корень того же уравнения лежит на интервале $(0; -1)$.

Теорема 9. В чисто периодические цепные дроби разлагаются приведенные квадратичные иррациональности и только они.

Доказательство. Пусть α — чисто периодическая цепная дробь: $\alpha = \alpha_r$, где $r > 0$. Тогда $a_0 = a_r \geq 1$ и поэтому $\alpha > 1$.

Кроме того, $\alpha = \frac{p_{r-1}\alpha_r + p_{r-2}}{q_{r-1}\alpha_r + q_{r-2}} = \frac{p_{r-1}\alpha + p_{r-2}}{q_{r-1}\alpha + q_{r-2}}$, откуда

$$q_{r-1}\alpha^2 + (q_{r-2} - p_{r-1})\alpha - p_{r-2} = 0.$$

Рассмотрим число $\beta = [a_{r-1}; a_{r-2}, \dots, a_0, q_{r-1}, \dots, a_1, a_0, \dots]$; например, если $\alpha = [4; 3, 2, 1, 4, 3, 2, 1, \dots]$, то $\beta = [1; 2, 3, 4, 1, 2, 3, 4, \dots]$. Очевидно, $\beta > 1$ и

$$\begin{aligned} \beta &= \frac{[a_{r-1}, a_{r-2}, \dots, a_1, a_0]\beta + [a_{r-1}, a_{r-2}, \dots, a_1]}{[a_{r-2}, \dots, a_1, a_0]\beta + [a_{r-2}, \dots, a_1]} = \\ &= \frac{[a_0, a_1, \dots, a_{r-1}]\beta + [a_1, \dots, a_{r-2}, a_{r-1}]}{[a_0, a_1, \dots, a_{r-2}]\beta + [a_1, \dots, a_{r-2}]} = \frac{p_{r-1}\beta + q_{r-1}}{p_{r-2}\beta + q_{r-2}}, \end{aligned}$$

откуда $p_{r-2}\beta^2 + (q_{r-2} - p_{r-1})\beta - q_{r-1} = 0$. Обозначив $\gamma = -1/\beta$, имеем $-1 < \gamma < 0$ и

$$p_{r-2}\left(\frac{-1}{\gamma}\right)^2 + (q_{r-2} - p_{r-1})\left(\frac{-1}{\gamma}\right) - q_{r-1} = 0,$$

т.е. $q_{r-1}\gamma^2 + (q_{r-2} - p_{r-1})\gamma - p_{r-2} = 0$. Значит, γ — корень того же квадратного уравнения, что и α . В одну сторону теорема Галуа доказана.

Рассмотрим уравнение $ax^2 - bx + c = 0$, где a, b, c — целые числа, $a > 0$. Пусть α — его корень, γ — сопряженное число, $-1 < \gamma < 0$. Обозначим $d = b^2 - 4ac$. Поскольку $0 > \gamma = \frac{b - \sqrt{d}}{2a}$, то $b < \sqrt{d}$. Из неравенства $0 < \alpha + \gamma = \frac{b}{a}$ имеем $b > 0$. Наконец, $a = \frac{b + \sqrt{d}}{2\alpha} < \sqrt{d}$.

Очевидно, если α — приведенная квадратичная иррациональность, то $\alpha_1, \alpha_2, \alpha_3, \dots$ — тоже, причем дискриминанты всех соответствующих квадратных уравнений равны d . Их старшие коэффициенты и взятые со знаком минус коэффициенты при x — натуральные числа, меньшие \sqrt{d} . Поскольку свободный член выражается через старший член, взятый со знаком минус коэффициент при x и дискриминант d , то множество интересующих нас квадратных уравнений конечно. Следовательно, $\alpha_s = \alpha_{r+s}$ для некоторых $r > 0$ и s .

Если $s > 0$, то $-1 < a_{s-1} + \frac{1}{\gamma_s} < 0$. Этими неравенствами число a_{s-1} определено однозначно. Поскольку $\gamma_s = \gamma_{s+r-1}$, то определяемое аналогичными неравенствами число a_{s+r-1} равно a_{s-1} . Значит, $\alpha_{s-1} = a_{s-1} + \frac{1}{\alpha_s} = a_{s+r-1} + \frac{1}{\alpha_{s+r}} = \alpha_{r+s-1}$. Таким же образом можно уменьшить s еще на единицу и так далее до тех пор, пока не приходим к равенству $s = 0$.

Теорема Лагранжа

Теорема Лагранжа — непосредственное следствие теоремы Галуа. В самом деле, для любой квадратичной иррациональности α имеем $\alpha_n > 1$ при любом натуральном n .

$$\text{Из равенства } \alpha = \frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}} \text{ находим } \alpha_n = \frac{p_{n-2} - q_{n-2}\alpha}{q_{n-1}\alpha - p_{n-1}}.$$

Обозначая сопряжение чертой над числом, имеем

$$\overline{\alpha_n} = -\frac{q_{n-2}}{q_{n-1}} \cdot \frac{\bar{\alpha} - \frac{p_{n-2}}{q_{n-2}}}{\bar{\alpha} - \frac{p_{n-1}}{q_{n-1}}}.$$

Разумеется, $q_{n-2} < q_{n-1}$. В случае $\bar{\alpha} < \alpha$ воспользуемся тем, что при любом достаточно большом четном n дробь p_{n-2}/q_{n-2} лежит между $\bar{\alpha}$ и α , а дробь p_{n-1}/q_{n-1} больше числа α ; таким образом, неравенства $-1 < \alpha_n < 0$ очевидны. А если $\alpha > \alpha$, достаточно рассмотреть любое достаточно большое n .

Цепные дроби чисел вида \sqrt{d}

Объясним специфический вид цепных дробей чисел вида \sqrt{d} , где d — натуральное число, не являющееся квадратом. Обозначим $[\sqrt{d}] = k$. Число $k + \sqrt{d}$ — приведенная квадратичная иррациональность. Пусть $[a_0; a_1, a_2, \dots, a_{r-2}, a_{r-1}, \dots]$ — ее цепная дробь, r — длина периода. По теореме Галуа имеем

$$[a_{r-1}; a_{r-2}, a_{r-3}, \dots, a_1, a_0, \dots] = -\frac{1}{k - \sqrt{d}} = \frac{1}{\sqrt{d} - k}, \text{ так что}$$

$$k + \sqrt{d} = 2k + \frac{1}{[a_{r-1}; a_{r-2}, a_{r-3}, \dots, a_1, a_0, \dots]} =$$

$$= [2k; a_{r-1}, a_{r-2}, a_{r-3}, \dots, a_1, a_0, \dots].$$

Следовательно, $a_r = a_0 = 2k$, $a_1 = a_{r-1}$, $a_2 = a_{r-2}$, ... Период цепной дроби числа \sqrt{d} оканчивается на число $2[\sqrt{d}]$, а после отбрасывания этого числа становится палиндромом: читается слева направо так же, как справа налево.

КВАДРАТИЧНЫЙ ЗАКОН ВЗАИМНОСТИ

Рассмотрим таблицу значений многочлена $n^2 - 2$.

n	$n^2 - 2$
3	7
4	$14 = 2 \cdot 7$
5	23
6	$34 = 2 \cdot 17$
7	47
8	$62 = 2 \cdot 31$
9	79
10	$98 = 2 \cdot 7^2$
11	$119 = 7 \cdot 17$
12	$142 = 2 \cdot 71$
13	167
14	$194 = 2 \cdot 97$
15	223

Среди простых делителей этих значений есть простые числа 7, 17, 23, 31, 47, 71, 79, 97, 167 и 223. А вот числа 5 среди них нет. Для доказательства достаточно перебрать все остатки (0, 1, 2, 3 и 4), которые может дать целое число при делении на 5, вычислить для каждого из них величину $n^2 - 2$ и убедиться, что полученное значение не делится на 5. Можно чуть сократить вычисления, заметив, что по модулю 5 число n сравнимо либо с 0, либо с 1 или -1 , либо с 2 или -2 , но ни одно из чисел $0^2 - 2 = -2$, $1^2 - 2 = -1$ и $2^2 - 2 = 2$ не делится на 5.

Какие же простые числа p являются делителями чисел вида $n^2 - 2$? Смотрите: $7 = 8 - 1$, $17 = 2 \cdot 8 + 1$, $23 = 3 \cdot 8 - 1$, $31 = 4 \cdot 8 - 1$, ..., $167 = 21 \cdot 8 - 1$ и $223 = 28 \cdot 8 - 1$. Это простые числа вида $p = 8n \pm 1$.

А нечетные простые делители $p > 2$ чисел вида $n^2 + 2$ — это, как можно догадаться при помощи аналогичного эксперимента, числа вида $p = 8m + 1$ или $p = 8m + 3$. Казалось бы, при чем здесь 8?..

Объяснение дает квадратичный закон взаимности. Его пытались доказать Эйлер, Лагранж и Лежандр, а доказал 8 апреля 1796 года (в 19 лет!) Карл Фридрих Гаусс. Он не-

однократно возвращался к этому закону, придумав несколько разных доказательств. Мы разберем самое элементарное из них в виде, который ему придал Фердинанд Георг Фробениус (1849–1917).

Всюду в этой статье буква p обозначает простое число, причем $p > 2$.

Символ Лежандра

По определению, $\left(\frac{a}{p}\right) = 1$, если a – квадратичный вычет по модулю p , т.е. если существует такое не кратное числу p целое x , что

$$x^2 \equiv a \pmod{p}.$$

Далее, $\left(\frac{a}{p}\right) = 0$, если a кратно числу p . Наконец, $\left(\frac{a}{p}\right) = -1$, если a – квадратичный невычет по модулю p , т.е. если ни для какого целого x разность $x^2 - a$ не делится на p .

Вычетов и невычетов – поровну

Рассмотрим числа $1^2, 2^2, \dots, (p-2)^2, (p-1)^2$. Поскольку остатки от деления чисел x^2 и $(p-x)^2 = p(p-2x) + x^2$ на p совпадают, при любом p строка остатков симметрична: читается слева направо так же, как справа налево.

А остатки от деления чисел $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$ на p все разные. Ведь если бы какие-то числа r^2 и s^2 , где $1 \leq r < s \leq \frac{p-1}{2}$, давали одинаковые остатки, то разность $s^2 - r^2 = (s-r)(s+r)$ делилась бы на p . Но ни $s-r$, ни $s+r$ не делятся на p . Значит, действительно существует ровно $(p-1)/2$ квадратичных вычетов и $(p-1)/2$ невычетов.

Критерий Эйлера

Возведем обе части сравнения $a \equiv x^2 \pmod{p}$, где x не делится на p , в $(p-1)/2$ -ю степень:

$$a^{(p-1)/2} \equiv x^{p-1} \pmod{p}.$$

В силу малой теоремы Ферма $x^{p-1} \equiv 1 \pmod{p}$. Поскольку в

рассматриваемом случае $\left(\frac{a}{p}\right) = 1$, то

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) (\text{mod } p).$$

Критерий Эйлера гласит: последнее сравнение верно для *любого* целого числа a , а не только для квадратичных вычетов.

Докажем его. Все $(p-1)/2$ квадратичных вычетов удовлетворяют сравнению

$$x^{(p-1)/2} \equiv 1 (\text{mod } p).$$

Поскольку многочлен не может иметь больше корней, чем его степень, то никакой другой класс вычетов этому сравнению не удовлетворяет. Таким образом, для любого квадратичного невычета b имеем

$$b^{(p-1)/2} - 1 \not\equiv 0 (\text{mod } p).$$

Поскольку

$$0 \equiv b^{p-1} - 1 = (b^{(p-1)/2} - 1)(b^{(p-1)/2} + 1) (\text{mod } p),$$

то $b^{(p-1)/2} + 1 \equiv 0 (\text{mod } p)$, так что

$$b^{(p-1)/2} \equiv -1 = \left(\frac{b}{p}\right) (\text{mod } p).$$

Критерий Эйлера доказан. Подставив $b = -1$, имеем:

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

Таким образом, существование такого m , что $m^2 + 1$ делится на p , равносильно сравнению $p \equiv 1 (\text{mod } 4)$. Это называют первым дополнением к квадратичному закону взаимности.

Мультипликативность символа Лежандра

Для любых двух целых чисел x и y имеем

$$\left(\frac{xy}{p}\right) \equiv (xy)^{(p-1)/2} = x^{(p-1)/2} y^{(p-1)/2} \equiv \left(\frac{x}{p}\right) \cdot \left(\frac{y}{p}\right) (\text{mod } p).$$

Следовательно, $\left(\frac{x}{p}\right) \cdot \left(\frac{y}{p}\right) \equiv \left(\frac{xy}{p}\right) (\text{mod } p)$. Поскольку $p > 2$, а

символ Лежандра может равняться лишь 0, 1 или -1 , то

$$\left(\frac{x}{p}\right) \cdot \left(\frac{y}{p}\right) = \left(\frac{xy}{p}\right).$$

Упражнение 1. Для любого простого числа p существует такое целое число x , что

$$(x^2 - 2)(x^2 - 3)(x^2 - 6)$$

кратно p . Докажите это.

Критерий Гаусса

Начнем с численного примера:

$$\begin{aligned} 3^8 \cdot 8! &= (3 \cdot 1)(3 \cdot 2)(3 \cdot 3)(3 \cdot 4)(3 \cdot 5)(3 \cdot 6)(3 \cdot 7)(3 \cdot 8) = \\ &= 3 \cdot 6 \cdot 9 \cdot 12 \cdot 15 \cdot 18 \cdot 21 \cdot 24 = 3 \cdot 6 \cdot (-8) \cdot (-5) \cdot (-2) \cdot 1 \cdot 4 \cdot 7 = \\ &= -8! \pmod{17}, \end{aligned}$$

откуда $3^8 \equiv -1 \pmod{17}$ и, в силу критерия Эйлера, $\left(\frac{3}{17}\right) = -1$.

Аналогично,

$$\begin{aligned} \left(\frac{2}{13}\right) &\equiv 2^6 = \frac{2^6 \cdot 6!}{6!} = \frac{2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdot 12}{6!} \equiv \\ &\equiv \frac{2 \cdot 4 \cdot 6 \cdot (-5) \cdot (-3) \cdot (-1)}{6!} = -1 \pmod{13}. \end{aligned}$$

Перейдем к общим рассуждениям. Числа $0, 1, 2, \dots, p-1$ образуют полную систему вычетов по модулю p . Другими словами, любое целое число сравнимо по модулю p с одним и только одним из этих чисел. Полную систему вычетов образуют и числа $0, \pm 1, \pm 2, \dots, \pm(p-1)/2$. Иначе говоря, любой ненулевой класс вычетов сравним по модулю p с одним из чисел от 1 до $n = (p-1)/2$ или с одним из чисел от -1 до $-n$.

Полусистемой вычетов по модулю p называют любой набор из $n = (p-1)/2$ ненулевых классов вычетов a_1, a_2, \dots, a_n , обладающий тем свойством, что для любого ненулевого класса вычетов $x \pmod{p}$ выполнено одно из сравнений $x \equiv a_k$ или $x \equiv -a_k \pmod{p}$, где $1 \leq k \leq n$.

Другими словами, полусистема вычетов — это такое множество из n ненулевых классов вычетов, что ни при каких k и j

сумма $a_k + a_j$ не делится на p . Читатель, знакомый с понятиями теории групп, скажет, что для получения полусистемы надо выбрать по одному элементу из каждого класса смежности $\mathbf{Z}_{p-1}^*/\{\pm 1\}$.

Для любой полусистемы и любого ненулевого класса вычетов x составим таблицу, в верхней строке которой – полусистема вычетов a_1, a_2, \dots, a_n ; в средней строке – числа xa_1, xa_2, \dots, xa_n , каждое из которых представлено в виде $xa_k \equiv \epsilon_k a_{f(k)}$, где $1 \leq k \leq n$; в нижней строке – числа $\epsilon_k = \pm 1$. В рассмотренном выше примере $p = 17$ и $x = 3$, полусистема вычетов состоит из первых 8 натуральных чисел, а таблица выглядит так:

$a_k = k$	1	2	3	4	5	6	7	8
xa_k	3	6	$9 \equiv -8$	$12 \equiv -5$	$15 \equiv -2$	$18 \equiv 1$	$21 \equiv 4$	$24 \equiv 7$
ϵ_k	1	1	-1	-1	-1	1	1	1

Как нетрудно убедиться, для любой полусистемы вычетов a_1, a_2, \dots, a_n и любого x , не делящегося на p , числа xa_1, xa_2, \dots, xa_n тоже образуют полусистему вычетов, т.е. в качестве $a_{f(k)}$, где $1 \leq k \leq n$, побывают по одному разу все числа a_1, a_2, \dots, a_n . Таким образом,

$$xa \cdot xa_2 \cdot \dots \cdot xa_n \equiv \epsilon_1 a_{f(1)} \epsilon_2 a_{f(2)} \dots \epsilon_n a_{f(n)} \pmod{p}.$$

Сократив обе части на $a_1 a_2 \dots a_n$, получаем: $x^n \equiv \epsilon_1 \epsilon_2 \dots \epsilon_n \pmod{p}$. В силу критерия Эйлера,

$$\left(\frac{x}{p}\right) \equiv x^n = \epsilon_1 \epsilon_2 \dots \epsilon_n = \pm 1,$$

откуда $\left(\frac{x}{p}\right) = \epsilon_1 \epsilon_2 \dots \epsilon_n$. Это и есть критерий Гаусса.

Доказательство Фробениуса

Пусть p, q – простые нечетные числа, $p \neq q$. Как мы только что доказали, $\left(\frac{p}{q}\right) = (-1)^k$, где k – количество таких целых x , что $1 \leq x \leq n$ и абсолютно наименьший вычет числа qx отрицателен, т.е.

$$-\frac{p}{2} < qx - py < 0$$

для некоторого целого y . Если эти неравенства выполнены для некоторого x , то величина y определена однозначно, причем

$py > qx > 0$ и $py < qx + \frac{p}{2} < q \cdot \frac{p}{2} + \frac{p}{2} = p \cdot \frac{q+1}{2}$. Поскольку число y целое, то $1 \leq y \leq m = \frac{q-1}{2}$.

Поэтому можно сказать, что k есть количество пар натуральных чисел $(x; y)$, удовлетворяющих неравенствам $x \leq n$, $y \leq m$ и

$$-\frac{p}{2} < qx - py < 0.$$

Аналогично, $\left(\frac{p}{q}\right) = (-1)^K$, где K — количество пар натуральных чисел $(x; y)$, удовлетворяющих неравенствам $x \leq n$, $y \leq m$ и $-\frac{q}{2} < py - qx < 0$. Последнее неравенство можно записать в виде

$$0 < qx - py < \frac{q}{2}.$$

Поскольку равенство $qx - py = 0$ при рассматриваемых значениях x и y невозможно, то

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{k+K},$$

где $k + K$ — это количество пар натуральных чисел $(x; y)$, удовлетворяющих неравенствам $x \leq n$, $y \leq m$ и

$$-\frac{p}{2} < qx - py < \frac{q}{2}.$$

Последнее неравенство задает на координатной плоскости внутреннюю часть полосы, которая ограничена параллельными прямыми

$qx - py = -\frac{p}{2}$ и $qx - py = \frac{q}{2}$. А неравенства $0 < x < \frac{p+1}{2}$

и $0 < y < \frac{q+1}{2}$ задают внутренность прямоугольника с центром

$$S\left(\frac{p+1}{4}; \frac{q+1}{4}\right).$$

Таким образом, $k + K$ — это количество целочисленных точек, расположенных в пересечении полосы и прямоугольника.

Полоса симметрична относительно точки S . В этом можно убедиться, рассматривая точки пересечения прямых, ограничивающих полосу, со сторонами прямоугольника, или исходя из

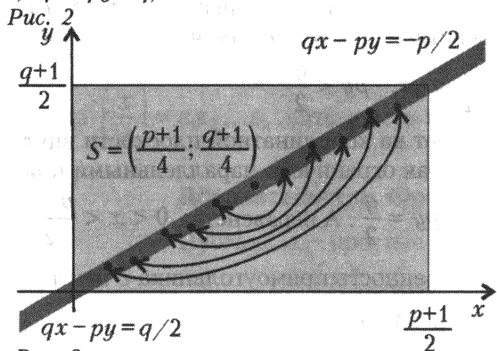
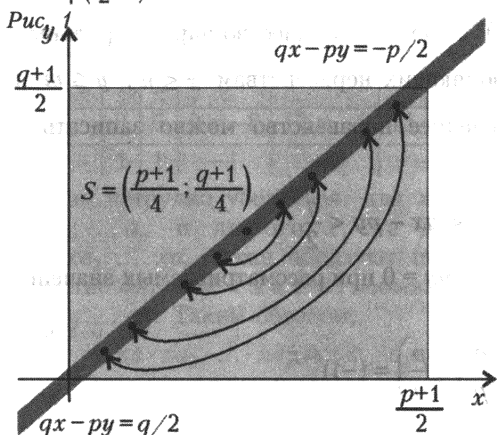
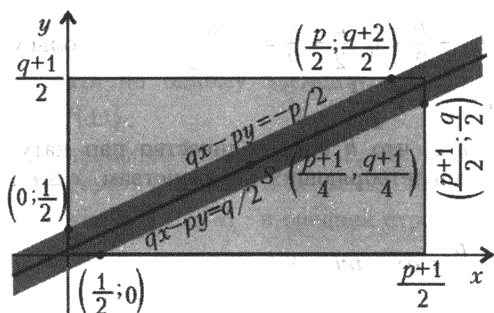


Рис. 3

того, что средняя линия полосы задана уравнением

$$qx - py = \frac{1}{2} \left(-\frac{p}{2} + \frac{q}{2} \right) = \frac{q-p}{4}$$

и, поскольку

$$q \cdot \frac{p+1}{4} - p \cdot \frac{q+1}{4} = \frac{q-p}{4},$$

проходит через точку S (рис. 1).

При центральной симметрии относительно точки S любая точка $(x; y)$ с целыми координатами переходит в точку с целыми координатами

$$\left(\frac{p+1}{2} - x; \frac{q+1}{2} - y \right).$$

Таким образом точки разбиваются на пары, а точка S симметрична сама себе. Число $k + K$ нечетно, если обе координаты точки S целые, т.е. если

число $\frac{p-1}{2} \cdot \frac{q-1}{2}$ нечетно, как, например,

в случае $p = 23$ и $q = 19$ (рис. 2). Число $k + K$ четно, если хотя бы одна координата точки S не целая, т.е. если число $\frac{p-1}{2} \cdot \frac{q-1}{2}$ четно, как в случае $p = 23$ и $q = 13$ (рис. 3). Мы доказали

квадратичный закон взаимности:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{k+K} = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}.$$

Упражнения

2. В силу формулы бинома Ньютона и делимости на p всех чисел p -й строки треугольника Паскаля, кроме двух крайних чисел $C_p^0 = C_p^p = 1$, имеем

$$(1+i)^p = 1 + C_p^1 i + C_p^2 i^2 + \dots + C_p^{p-2} i^{p-2} + C_p^{p-1} i^{p-1} + i^p \equiv 1 + i^p \pmod{p}.$$

Воспользуйтесь этим для доказательства второго дополнения к квадратичному закону взаимности.

3. Символ Якоби $\left(\frac{a}{n}\right)$ определен для любого нечетного натурально-го числа $n = p_1 p_2 \dots p_k$, где p_1, p_2, \dots, p_k – простые числа, и любого целого числа a , взаимно простого с n , формулой

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \left(\frac{a}{p_2}\right) \dots \left(\frac{a}{p_k}\right).$$

а) Докажите, что квадратичный закон взаимности верен и для символа Якоби: для любых нечетных взаимно простых натуральных чисел a и b имеем

$$\left(\frac{a}{b}\right) \left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2} \frac{b-1}{2}}.$$

б) Докажите для символа Якоби оба дополнения к квадратичному закону взаимности:

$$\left(\frac{-1}{b}\right) = (-1)^{(b-1)/2} \quad \text{и} \quad \left(\frac{2}{b}\right) = (-1)^{(b^2-1)/8}.$$

Замечание. Символ Якоби помогает при вычислении символа Лежандра: например,

$$\begin{aligned} \left(\frac{103}{1999}\right) &= \left(\frac{1999}{103}\right) (-1)^{\frac{1999-1}{2} \frac{103-1}{2}} = \\ &= -\left(\frac{1999}{103}\right) = -\left(\frac{42}{103}\right) = -\left(\frac{2}{103}\right) \left(\frac{21}{103}\right) = -(-1)^{\frac{103^2-1}{8}} \left(\frac{103}{21}\right) (-1)^{\frac{21-1}{2} \frac{103-1}{2}} = \\ &= -\left(\frac{-2}{21}\right) = -\left(\frac{-1}{21}\right) \cdot \left(\frac{2}{21}\right) = -(-1)^{\frac{21-1}{4}} \cdot (-1)^{\frac{21^2-1}{8}} = 1. \end{aligned}$$

Индукция

1. База: $1 = 1^2$. Переход: $n^2 + (2n + 1) = (n + 1)^2$.

2. Для любого натурального n число $(n + 1)(n + 2) \dots (2n)$ делится на 2^n и не делится на 2^{n+1} . Это легко доказать по индукции, проверив базу и заметив, что

$$\frac{(n + 2)(n + 3) \dots (2n)(2n + 1)(2n + 2)}{(n + 1)(n + 2) \dots (2n)} = \frac{(2n + 1)(2n + 2)}{n + 1} = 2(2n + 1)$$

делится на 2 и не делится на 4.

Можно обойтись и без индукции:

$$\begin{aligned} \frac{(n + 1) \dots (2n - 1) \cdot 2n}{2^n} &= \frac{1 \cdot 2 \cdot \dots \cdot n(n + 1) \dots (2n - 1) \cdot 2n}{1 \cdot 2 \cdot \dots \cdot n \cdot 2^n} = \\ &= \frac{1 \cdot 3 \cdot 5 \cdot \dots \cdot (2n - 1) \cdot 2 \cdot 4 \cdot 6 \cdot \dots \cdot 2n}{2 \cdot 4 \cdot \dots \cdot 2n} = 1 \cdot 3 \cdot \dots \cdot (2n - 1) \end{aligned}$$

– нечетное число.

Алгоритм Евклида

1. а) 10 и 3; б) -11 и 9.

2. В двоичной системе 3542 имеет вид $\overline{11011010110}$, а $2492 = \overline{100110111100}$. Следовательно,

$$\begin{aligned} \text{НОД}(3542; 2492) &= 2 \cdot \text{НОД}(\overline{1101101011}; \overline{10011011110}) = \\ &= 2 \cdot \text{НОД}(\overline{1101101011}; \overline{1001101111}). \end{aligned}$$

Вычисление наибольшего общего делителя чисел $1771 = \overline{11011101011}$ и $623 = \overline{1001101111}$ представим в виде таблицы, в левом столбце которой – числа в десятичной системе счисления, а в правом – в двоичной:

(1771; 623)	(1101101011; 1001101111)
(1148; 623)	(10001111100; 1001101111)
(574; 623)	(1000111110; 1001101111)
(287; 623)	(100011111; 1001101111)

(287;336)	(100011111; 101010000)
(287;168)	(100011111; 10101000)
(287;84)	(100011111;1010100)
(287;42)	(100011111;101010)
(287;21)	(100011111;10101)
(266;21)	(100001010;10101)
(133;21)	(10000101;10101)
(112;21)	(1110000;10101)
(56;21)	(111000;10101)
(28;21)	(11100;10101)
(14;21)	(1110;10101)
(7;21)	(111;10101)
(7;14)	(111;1110)
(7;7)	(111;111)

Ответ очевиден: $\text{НОД}(1771;623) = 7$ и, значит, $\text{НОД}(3542;2492) = 2 \cdot 7 = 14$.

3. Пусть в одном из сосудов a литров воды, во втором — b , в третьем — c , причем $a \leq b \leq c$. Разберем сначала случай $a = 1$. Если доливать воду несколько раз подряд только в первый сосуд, то при первом переливании в него нужно долить 1 литр, при втором — 2, при третьем — 4, и так далее по степеням двойки. Представим число b в виде степени двойки или суммы нескольких разных степеней двойки. Используя для отсутствующих степеней двойки третий сосуд, мы можем опустошить весь второй сосуд.

Если же $a > 1$, аналогичная конструкция позволяет добиться того, что во втором сосуде окажется столько литров воды, каков остаток от деления b на a . Таким образом мы будем уменьшать и уменьшать наименьшее из количеств воды в сосудах до тех пор, пока один из сосудов не опустеет.

4. Пусть $n > 1$. Меньшее из искоемых чисел должно оканчиваться на несколько девяток, а следующее — на столько же нулей. Рассмотрим число $\underbrace{11\dots1}_{n-1}\underbrace{99\dots99}_x$ и следующее за ним число $\underbrace{11\dots11}_{n-2}\underbrace{200\dots00}_x$. Их суммы цифр равны $n - 1 + 9x$ и n соответственно.

Лемма. Если n не делится на 3, то уравнение $9x - 1 = ny$ имеет решение в натуральных числах x и y .

Доказательство. Если n при делении на 9 дает остаток 1, 2, 4, 5, 7 или 8, то можно взять соответственно $y = 8, 4, 2, 7, 5$ или 1.

7. После каждой операции разрезания количество кусков

увеличивается на 5 или на 11; после m разрезов на 6 кусков и n разрезов на 12 кусков имеем $1 + 5m + 11n$ кусков.

а) Перебрав значения $m = 0, 1, 2$ и 3 , убеждаемся, что ни при каких целых неотрицательных m и n величина $1 + 5m + 11n$ не равна 40.

б) Очевидно, $1 + 5 \cdot 8 + 11 \cdot 0 = 41$, $1 + 5 \cdot 6 + 11 \cdot 1 = 42$, $1 + 5 \cdot 4 + 11 \cdot 2 = 43$, $1 + 5 \cdot 2 + 11 \cdot 3 = 44$ и $1 + 5 \cdot 0 + 11 \cdot 4 = 45$. Поскольку $1 + 5(m + 1) + 11n = (1 + 5m + 11n) + 5$, любое большее 40 натуральное число можно получить, начав с одного из чисел 41, 42, 43, 44, 45 и прибавив нужное количество пятерок.

8. $ab - a - b$. *Указание.* Воспользуйтесь теоремой 3 и тем, что наименьшее целое число, представимое в виде $ax + by$, где x и y — неотрицательные целые числа, равно 0.

Периодические дроби

2. Длина периода равна 6. При делении на 6 число 100 дает остаток 4. Поэтому сотая после запятой цифра такая же, как четвертая. *Ответ:* 5.

4. 6) *Указание.* $0,(845) + 0,(49) = 0,(845845) + 0,(494949)$. Поскольку сумма $845845 + 494\,949 = 1340794$ — семизначное число, возникают переносы «в предыдущий период».

в) Очевидно, $2,70(584) = 2,705(845)$. Расширив периоды до длины, равной наименьшему общему кратному периодов слагаемых, получим: $2,705(845) + 6,917(49) = 2,705(845845) + 6,917(494949) = 9,623(340795)$.

5. а) $0,(23)$; б) $0,(001234)$.

6. а) $0,(012) = 12/999 = 4/333$;

$$б) 3,1(3) = 3 + 0,1 + 0,0(3) = 3,1 + \frac{1}{10} \cdot 0,(3) = 3,1 + \frac{1}{10} \cdot \frac{3}{9} = \frac{47}{15};$$

$$в) 1,93(173) = 1,93 + \frac{1}{100} \cdot 0,(173) = 1,93 + \frac{1}{100} \cdot \frac{173}{999} = 9649/4995.$$

7. *Указание.* Сумма (произведение, разность) двух обыкновенных дробей (рациональных чисел) — обыкновенная дробь.

$$9. 0,(692307) = 7,(692307) - 7 = \frac{100}{13} - 7 = \frac{9}{13}.$$

$$10. а) \frac{12}{85} = \frac{24}{170} = \left(1 + \frac{7}{17}\right) : 10 = 0,1(4117647058823529);$$

$$б) \frac{3}{68} = \frac{75}{1700} = \left(4 + \frac{7}{17}\right) : 100 = 0,04(4117647058823529).$$

11. Предположим противное: пусть $n \leq 100$ и дробь m/n содержит цифры 167 в своем периоде. Тогда, домножив дробь на степень десятки и вычтя образовавшуюся целую часть, получим дробь, в которой цифры 167 идут сразу после запятой. Домножим такую дробь на 6. Поскольку $167 \cdot 6 = 1002$ и $168 \cdot 6 = 1008$, получим число, которое больше 1 и меньше $1,008 < 1,01$. При умножении на n получаем (целое!) число, которое больше n и меньше $n + 0,01n \leq n + 1$. Но такого целого числа не существует.

13. $[100/6] = 16$.

14. Число $\underbrace{11\dots1}_n$ кратно 7 тогда и только тогда, когда n кратно 6. Число 111111 кратно и 11, и 13, и $15873 = 111111/7$.

15. При k , кратных 6.

16. Подумайте, что происходит при делении «уголком».
Ответ: $n = 2$, а m — четное число.

17. а) По условию, $10^n - 1$ не кратно числу p , а $10^{2n} - 1 = (10^n - 1)(10^n + 1)$ кратно p . Следовательно, $10^n + 1$ кратно p . Пусть $1/p = (10^n a + b)/(10^{2n} - 1)$, где $0 \leq a, b < 10^n$. Тогда $(10^n a + b)/(10^n - 1) = (10^n + 1)/p$ — целое число. Поскольку $10^n a + b = (10^n - 1)a + (a + b)$ кратно числу $(10^n - 1)$, то сумма $a + b$ тоже кратна числу $10^n - 1$. Заметив, что $0 < a + b < 2(10^n - 1)$, заключаем: $a + b = 10^n - 1$.

18. а) 15; б) нет.

19. а) Поскольку $1986 = 2 \cdot 3 \cdot 331$, число $A = \underbrace{11\dots1}_{1986}$ имеет кроме числа 1 и самого A еще шесть делителей из одних единиц: 11, 111, 111111, $\underbrace{11\dots1}_{331}$, $\underbrace{11\dots1}_{662}$ и $\underbrace{11\dots1}_{993}$.

б) Поскольку $111111 = 111 \cdot 1001 = 3 \cdot 37 \cdot 7 \cdot 11 \cdot 13$ и поскольку число $10^{993} + 1$ кратно числу $10^3 + 1 = 1001$, а число $10^{993} - 1$ кратно числу $10^3 - 1 = 999$, то, обозначив $a = 10^{331}$, получаем:

$$A = (a^6 - 1)/9 = (a^3 + 1)(a^3 - 1)/9 = 3 \cdot 37 \cdot 7 \cdot 11 \cdot 13 \cdot \frac{a^3 + 1}{1001} \cdot \frac{a^3 - 1}{999}.$$

Произведение любого набора из этих семи множителей является делителем числа A («пустому набору» соответствует 1). Таким образом, мы нашли $2^7 = 128$ делителей. Все они различны, поскольку семь выписанных множителей попарно взаимно просты. (В самом деле, остаток от деления числа a на $m = 10^6 - 1$

равен 10, поскольку $10^{331} - 10 = 10(10^{655} - 1)$ кратно m ; поэтому $a^3 \pm 1$ при делении на m дает остаток $10^3 \pm 1$, так что числа $(a^3 + 1)/1001$ и $(a^3 - 1)/999$ взаимно просты с m и, очевидно, взаимно просты друг с другом.)

в) Продолжим разложение:

$$A = 3 \cdot 37 \cdot 7 \cdot 11 \cdot 13 \cdot \frac{a+1}{11} \cdot \frac{a^2 - a + 1}{91} \cdot \frac{a-1}{9} \cdot \frac{a^2 + a + 1}{111}.$$

Значит, A имеет не менее $2^9 = 512$ делителей. В силу малой теоремы Ферма число $9A = 10^{1986} - 1$ кратно простому числу 1987. Таким образом, один из четырех последних сомножителей разложения кратен 1987, а значит, A имеет не менее $2^{10} = 1024$ делителей.

21. а) 4 или 12; б) 15, 30 или 60.

22. а) Обозначим ПЛОМБ = x . Тогда $(10x + A) \cdot 5 = 100000 \cdot A + x$, откуда $49x = 99995A$. Ответ: ПЛОМБА = 142857.

в) В словах ребуса использованы два слога: НИК и ЕЛЬ. Обозначив НИК = x и ЕЛЬ = y , получаем уравнение $6000x + 6y = 1000y + x$, т.е. $5999x = 994y$. Сокращая на НОД(5999; 994) = 7, получаем уравнение $859x = 142y$, т.е. $x = 142$ и $y = 859$.

г) Да, таково число 142857.

д) 102564, 128205, 142857, 153846, 179487, 205128 и 230769.

23. Указание. Если $10000a + b$ кратно 41, то $10(10000a + b) = 99999a + a + 10b = 41 \cdot 2439a + (10b + a)$ тоже кратно 41.

24. 105263157894736842.

25. Указание. Записав числители в системе счисления с основанием a и «прокрутив», мы разобьем дроби на циклы по n дробей в каждом.

26. а) 81; б) 9^9 ; в) $2 \cdot 11^{10}$; г) $2 \cdot 3^k \cdot 7^{l-1}$.

29. При делении «уголком» 1 на 3^{100} получаем периодическую десятичную дробь с периодом длины $M = 3^{98}$. Поэтому в процессе деления всего встретятся M различных остатков. Первый из остатков равен 1, а каждый следующий получается из предыдущего умножением на 10 (= 9 + 1) и вычитанием числа, кратного 3^{100} . Эти процедуры не меняют остаток от деления на 9. Поэтому появляющиеся в процессе деления остатки имеют вид $9q + 1$, где $0 \leq q < M$. Поскольку чисел такого вида ровно M штук, все они встретятся в качестве остатков.

Остальное просто. Пусть $a = 0, a_1 a_2 \dots a_{46}$ – десятичная дробь, $b = a + 10^{-46}$. Поскольку $3^{100} > 10^{47}$, разность чисел $3^{100}b$ и $3^{100}a$ больше 10. Следовательно, между ними найдется число вида $9q + 1$. Поскольку $a < \frac{9q+1}{3^{100}} < b$, в процессе деления, начиная с остатка $9q + 1$, будут получены все 46 цифр $a_1 a_2 \dots a_{46}$.

30. а) Если m четно, $m = 2n$, то $p^n = 2s + 1$, где $s > 1$. Поскольку $p^{2n} = 4s^2 + 4s + 1$, то $p^m + 1 = 2(2s^2 + 2s + 1)$ и $p^m - 1 = 4s(s + 1)$. Число $2s^2 + 2s + 1$ и хотя бы одно из чисел s и $s + 1$ не является степенью двойки.

Если m нечетно, то $p^m - 1 = (p - 1)(p^{m-1} + p^{m-2} + \dots + p + 1)$ и $p^m + 1 = (p + 1)(p^{m-1} - p^{m-2} + \dots - p + 1)$. Вторые множители в этих разложениях – суммы нечетного количества нечетных слагаемых. Поэтому они нечетны и не являются степенями двойки.

б) Для целых неотрицательных чисел a, b, c и d из равенства $2^a \cdot 5^b + 1 = 2^c \cdot 5^d$ следует, что $a = d = 0$ или $b = c = 0$. Вследствие утверждения пункта а) уравнение $5^x \pm 1 = 2^y$ при $x > 1$ решений не имеет. Осталось заметить, что $5^1 + 1$ – не степень двойки, а $5^1 - 1 = 2^2$. *Ответ: $n = 4$.*

в) *Ответ: $x = 1$ и $y = 2$.*

г) *Ответ: $x = 1$ и $y = 1$ или $x = 2$ и $y = 3$.*

31. Известны два таких простых числа, 487 и 56598313. Неизвестно, бесконечно ли множество простых чисел со свойством $L(p) = L(p^2)$. Неизвестно и то, существует ли хотя бы одно простое число $p > 5$, для которого $L(p) = L(p^3)$.

Малая теорема Ферма

$$1. \quad a^3 + 5a = (a^3 - a) + 6a. \quad 2. \quad x \equiv 71 \pmod{101}.$$

$$3. \quad x \equiv 0 \pmod{6}.$$

6. а) В произведении четырех последовательных целых чисел обязательно есть множитель, кратный 4. Кроме него, есть еще один четный множитель.

$$\begin{aligned} \text{в) } a^5 - 5a^3 + 4a &= a(a^2 - 1)(a^2 - 4) = \\ &= (a - 2)(a - 1)a(a + 1)(a + 2). \end{aligned}$$

8. Указание. Если числа m, n не кратны 5, то $(m^4 - 1) - (n^4 - 1)$ кратно 5 вследствие малой теоремы Ферма.

9. $k^4 - 1 = (k - 1)(k + 1)(k^2 + 1)$. Все сомножители четны; при этом одно из чисел $k - 1$ и $k + 1$ кратно 4. Делимость $k^2 - 1$ на 3 и делимость $k^4 - 1$ на 5 следуют из малой теоремы Ферма.

10. Первый способ. Поскольку $2222 = 7 \cdot 317 + 3$ и $5555 = 7 \cdot 793 + 4$, имеем:

$$\begin{aligned} 2222^{5555} + 5555^{2222} &\equiv 3^{5555} + 4^{2222} = 3^{6 \cdot 925 + 5} + 4^{6 \cdot 370 + 2} = \\ &= (3^6)^{925} \cdot 3^5 + (4^6)^{370} \cdot 4^2 \equiv 1^{925} \cdot 243 + 1^{370} \cdot 16 = 259 = 7 \cdot 37 \equiv \\ &\equiv 0 \pmod{7}. \end{aligned}$$

Второй способ. Число $(2222^5)^{1111} + (5555^2)^{1111}$ кратно числу $2222^5 + 5555^2 \equiv 3^5 + 4^2 \equiv 0 \pmod{7}$.

11. $11^{10} - 1 = (11 - 1)(11^9 + 11^8 + \dots + 11 + 1)$.

12. а) Ответ: $a = 10k \pm 3$.

13. $(-1)^n - (-1) = 2$.

14. Указание. Поскольку число $2^n - 2$ является одним из значений многочлена $a^n - a$, наибольший общий делитель чисел вида $a^n - a$ не превосходит $2^n - 2$ (и является делителем числа $2^n - 2$). Для любого целого числа a существует хотя бы одно число в пределах от 1 до $2^n - 2$, сравнимое с a по модулю $2^n - 2$.

15. Да, существует.

18. Ответ: 15. **Решение:**

$$\begin{aligned} 3^{2000} &= 3^{47 \cdot 42 + 26} = \\ &= (3^{47})^{42} \cdot 3^{26} \equiv 3^{26} = 9^{13} = 9 \cdot 9^{12} = 9 \cdot 81^6 \equiv 9 \cdot (-5)^6 = \\ &= 9 \cdot 125^2 \equiv 9 \cdot (-4)^2 = 9 \cdot 16 = 144 \equiv 15 \pmod{43}. \end{aligned}$$

19. $a^{16} - 1 = (a^8 - 1)(a^8 + 1)$.

20. $56786730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 61$.

21. $5^{p^2} + 1 = (5^p)^p + 1 \equiv 5^p + 1 \equiv 5 + 1 = 6 \pmod{p}$. **Ответ:** $p = 2$ и 3 .

24. Обозначим первую цифру буквой a , а число, получаемое из исходного шестизначного числа вычеркиванием первой циф-

ры, через b . Тогда исходное число равно $100000a + b$, а полученное из него число равно $10x + b$. Осталось заметить, что

$$(100\,000a + b) \cdot 10 = 10^6 a + 10b =$$

$$= (10^6 - 1)a + 10b + a \equiv 10b + a \pmod{7}.$$

25. $\underbrace{11\dots1}_{p-1} = \underbrace{99\dots9}_{p-1} / 9 = (10^{p-1} - 1) / 9$. Число $10^{p-1} - 1$ кратно p по малой теореме Ферма.

26*. При $p = 3$ воспользуйтесь признаком делимости на 3. При $p = 2$ или 5 утверждение следует из того, что рассматриваемое число оканчивается той же самой цифрой, что и число 123456789. Пусть $p \neq 2, 3, 5$. Докажем, что разность $\underbrace{aa\dots a}_p \underbrace{00\dots0}_{(9-a)p} - a \underbrace{00\dots0}_{9-a}$, где $1 \leq a \leq 9$, кратно p . В силу предыдущего упражнения, число $\underbrace{aa\dots a}_{p-1}$ кратно p . Поэтому достаточно

заметить, что число

$$a \underbrace{00\dots0}_{(9-a)p} - a \underbrace{00\dots0}_{9-a} = a \cdot 10^{(9-a)p} - a \cdot 10^{9-a} = a \left((10^{9-a})^p - 10^{9-a} \right)$$

кратно p по малой теореме Ферма.

27. Если p — простой делитель составного числа n , то число $C_n^p / n = (n-1)(n-2)\dots(n-p+1)/(p!)$ не целое, поскольку делимое не кратно p .

28. а) $a + \frac{a^p - a}{p} + \frac{a^{p^2} - a^p}{p^2};$

б) $a + \frac{a^p - a}{p} + \frac{a^q - a}{q} + \frac{a^{pq} - a^p - a^q + a}{pq}.$

30. а) Поскольку $\phi(9) = 6$, для любого не кратного 3 числа k , по теореме Эйлера, $k^6 - 1$ кратно 9. Далее, $k^6 - 1 = (k^3 - 1)(k^3 + 1)$, причем числа $k^3 - 1$ и $k^3 + 1$ отличаются на 2 и потому не могут одновременно быть кратны 3.

31. а) В силу предыдущего упражнения, куб не кратного трем числа сравним с 1 или -1 по модулю 9. Сумма трех чисел, каждое из которых равно 1 или -1 , не может быть кратна 9.

32. Указание. Поскольку $7^4 \equiv 1 \pmod{10}$, последняя цифра числа 7^k определяется остатком от деления числа k на 4. Далее, $7^{2m+1} = (8-1)^{2m+1} \equiv (-1)^{2m+1} = -1 \pmod{4}.$

33. Применим теорему Эйлера: $7^{400} \equiv 1 \pmod{1000}$. Следовательно, $7^{10000} = (7^{400})^{25} \equiv 1^{25} = 1 \pmod{1000}$. Поскольку произведение $7 \cdot 7^{9999} = 7^{10000}$ оканчивается цифрами 001, то последняя цифра числа 7^{9999} равна 3. Значит, из разряда единиц в разряд десятков при умножении 7^{9999} на 7 переносится 2. Поэтому предпоследняя цифра числа 7^{9999} равна 4, и из разряда десятков в разряд сотен переносится 3. Теперь ясно, что в предпредпоследнем разряде числа 7^{9999} находится цифра 1. *Ответ:* 7^{9999} оканчивается на 143.

35. Поскольку $\varphi(n) \leq n$, число $n!$ делится на $\varphi(n)$. Поэтому $2^{n!} - 1$ кратно разности $2^{\varphi(n)} - 1$, которая в силу теоремы Эйлера кратна n .

36*. Если n – нечетное число, то можно сгруппировать первое слагаемое с последним, второе с предпоследним и так далее:

$$(1^n + (n-1)^n) + (2^n + (n-2)^n) + \dots + \left(\left(\frac{n-1}{2} \right)^n + \left(\frac{n+1}{2} \right)^n \right).$$

Поскольку $k^n + (n-k)^n \equiv k^n + (-k)^n = 0$, при нечетном n рассматриваемая сумма кратна n .

Если же n четно, пусть 2^s – наивысшая степень двойки, на которую n делится нацело. Тогда для любого четного числа k , очевидно, $k^n \equiv 0 \pmod{2^s}$; а для любого нечетного числа k , по теореме Эйлера, $k^n = \left(k^{n/2^{s-1}} \right)^{2^{s-1}} \equiv 1 \pmod{2^s}$. В таком случае, $1^n + 2^n + \dots + (n-1)^n \equiv \frac{n}{2} \not\equiv 0 \pmod{2^s}$. А если сумма не кратна 2^s , то она тем более не кратна числу n .

37*. Пусть $s = 2^a \cdot 5^b \cdot t$, где a, b – целые неотрицательные числа, t – натуральное число, не кратное ни 2, ни 5. Существует такое натуральное число r , что $10^r \equiv 1 \pmod{t}$. Пусть $n = 10^{\max(a,b)} \cdot (1 + 10^r + 10^{2r} + \dots + 10^{(s-1)r})$. Очевидно, сумма цифр числа n равна s . Поскольку $10^{\max(a,b)}$ делится нацело на $2^a \cdot 5^b$ и $10^r + 10^{2r} + \dots + 10^{sr} \equiv s \equiv 0 \pmod{t}$, число n кратно s .

39. а) $\varphi(pq) = pq - q - p + 1 = (p-1)(q-1)$.

40. а) $x = 3$; б) $x = 3, y = 2$.

42. $\varphi(n)/2$.

43. а) Пусть простое число p входит в разложения чисел m и n на простые множители, соответственно, в s -й и t -й степенях. Для определенности, пусть $s \leq t$. Если $s > 0$, то число p входит в разложения на простые множители чисел $\text{НОК}[m; n]$ и $\text{НОД}(m; n)$ в t -й и s -й степенях. Значит, если $s > 0$, то благодаря числу p при подсчете функции Эйлера от чисел $\varphi(m)$, $\varphi(n)$, $\varphi(\text{НОК}[m; n])$ и $\varphi(\text{НОД}(m; n))$ возникнут, соответственно, множители $p^{s-1}(p-1)$, $p^{t-1}(p-1)$, $p^{t-1}(p-1)$ и $p^{s-1}(p-1)$.

Если же $s = 0$, то p не входит в разложение на простые множители чисел m и $\text{НОД}(m; n)$, а в разложения чисел n и $\text{НОК}[m; n]$ оно входит в одной и той же степени.

б) Разложения чисел mn и $\text{НОК}[m; n]$ состоят из одних и тех же простых множителей.

в) Следует из пунктов а) и б).

г) Поскольку $\text{НОД}(m; n) > \varphi(\text{НОД}(m; n))$, из равенства предыдущего пункта следует, что $\varphi(m)\varphi(n) < \varphi(mn)$.

44. а) $x = 19, 38, 27$ или 54 .

б) $x = 13, 26, 21, 42, 28$ или 36 .

в) Так как при $x > 2$ число $\varphi(x)$ четно, то четным должно быть и само число x . Поскольку каждое второе натуральное число четно, $\varphi(x) \leq x/2$. Следовательно, $12 = x - \varphi(x) \geq x - \frac{x}{2} = \frac{x}{2}$, откуда $x \leq 24$. *Ответ:* $x = 18, 20$ или 22 .

г) *Ответ:* x – простое число. *Указание.* Если p – простое число, m – натуральное число, то $\varphi(p^{2m}) = p^{2m} - p^{2m-1} \leq p^{2m} - p^m$, причем неравенство обращается в равенство лишь при $m = 1$. Далее, для любых отличных от 1 натуральных чисел x и y докажете неравенство

$$(x^2 - x)(y^2 - y) < (xy)^2 - xy.$$

Теперь легко доказать, что $\varphi(x^2) < x^2 - x$ для любого составного числа x .

д) $x = 2^m$, где m – натуральное число.

е) Число x кратно 3. Поэтому его можно представить в виде $x = 3^m y$, где m – натуральное число, а y не кратно 3. Поскольку $\varphi(3^m y) = \varphi(3^m)\varphi(y) = 2 \cdot 3^{m-1}\varphi(y)$, то уравнение $\varphi(x) = x/3$ принимает вид $2\varphi(y) = y$. Последнему уравнению удовлетворяют степени двойки. *Ответ:* $x = 2^k \cdot 3^m$, где k, m – натуральные числа.

ж) *Указание.* Если бы в разложении числа x на простые множители содержалось два или более нечетных простых числа, то степень двойки в левой части равенства была бы выше, чем в правой. Если $x = 2^k p^m$, где p – нечетное простое число, k, m – натуральные числа, то $\varphi(x) = 2^{k-1}(p-1)p^{m-1}$, и уравнение $\varphi(x) = x/n$ можно записать в виде $p-1 = 2p/n$. *Ответ:* решений нет.

з) В силу пункта в) предыдущего упражнения, $\varphi(nx) \geq \varphi(n)\varphi(x)$. Следовательно, $\varphi(n) \leq 1$, т.е. $n = 2$. При $n = 2$ в качестве x можно взять любое нечетное число.

46. *Ответ:* $\varphi(n)/2$. *Указание.* Если $\text{НОД}(a; n) = 1$, то и $\text{НОД}(n-a; n) = 1$.

47. в) Задачу удобно решать с конца, т. е. искать кратчайший способ получения нуля из произвольного числа n с помощью двух операций – вычитания единицы и деления пополам. Пусть $f(n)$ – число операций в таком кратчайшем способе.

Если $n = 2k + 1$ – нечетное число, то делить его пополам нельзя, так что $f(2k+1) = 1 + f(2k)$.

Докажем индукцией по k , что $f(2k) = 1 + f(k)$. Для $k = 1$ это ясно. Пусть утверждение доказано для всех $k < K$. Если из числа $2K$ сначала вычесть единицу, то для получения нуля потребуется как минимум $1 + f(2K-1) = 2 + f(2K-2) = 3 + f(K-1)$ операций. Если же сначала разделить $2K$ пополам, то потребуется лишь $1 + f(K) \leq 2 + f(K-1)$ операций.

Теперь индукцией по m легко доказать, что $f(n) = m + a_m + a_{m-1} + \dots + a_1 + a_0$.

а), б) В частности, $f(100) = f(1100100_2) = 6 + 1 + 1 + 0 + 0 + 1 + 0 + 0 = 9$ и $f(9907) = f(10011010110011_2) = 13 + 1 + 0 + 0 + 1 + 1 + 0 + 1 + 0 + 1 + 1 + 0 + 0 + 1 + 1 = 21$.

48. а) В последовательности $2, 4, 8, 16 \equiv 3, 6, 12, 24 \equiv 11, 22 \equiv 9, 18 \equiv 5, 10, 20 \equiv 7, 14 \equiv 1$ встречаются все остатки от 1 до 12.

49. а) 2 и 3; б) числа вида $3 + 7n$ и числа вида $5 + 7n$, где n – целое.

50. Нельзя. Составное число n делится на некоторое простое число $q < n$. Рассмотрим то место на окружности, где находится q , и возьмем его в качестве первого из трех чисел a, b, c . Имеем:

$$b^2 \equiv ac \equiv 0 \pmod{q},$$

так что b делится на q . Двигаясь далее вдоль окружности и рассуждая аналогично, приходим к абсурду: все числа $1, 2, \dots, n-1$ должны делиться на q .

52. Указание. Во-первых, $2^n \equiv 3 \pmod{5}$ при $n \equiv 3 \pmod{4}$. Во-вторых, $2^n \equiv 3 \pmod{13}$ при $n \equiv 4 \pmod{12}$. В первом случае n должно быть нечетным числом, а во втором – четным.

53. $p = 13$.

56. б) $m = 1$ или 2 .

57. Поскольку $a - b^n = (a - k^n) + (k^n - b^n)$ кратно $k - b$, то $a - b^n$ делится на любое натуральное число. Следовательно, $a - b^n = 0$, что и требовалось доказать.

58. а) Рассмотрим остатки от деления чисел $1, 11, 111, \dots$ на n . Какие-то два из них равны; разность соответствующих чисел кратна n ; эта разность оканчивается на несколько нулей, которые можно отбросить, поскольку n взаимно просто с 10 .

59. а) $8^n + 1 = (2^n)^3 + 1^3$ кратно числу $2^n + 1$; $5 \cdot 4^n + 1 = 5 \cdot (3+1)^n + 1 \equiv 5 + 1 \equiv 0 \pmod{3}$.

б) Таковы, например, числа вида $10^{12k+1} + 3 \equiv 10 + 3 \equiv 0 \pmod{13}$. Составными являются и все числа вида $10^{6k+4} + 3$, поскольку $10^{6k+4} + 3 = (10^6)^k \cdot 10^4 + 3 \equiv 1 \cdot 3^4 + 3 = 84 \equiv 0 \pmod{7}$.

в) **Указание.** Пусть p – простой делитель числа $ab + c$. Существует бесконечно много таких натуральных n , что $b^n \equiv b \pmod{p}$.

60. Порядок числа a является делителем чисел r и s и потому является делителем числа $\text{НОД}(r; s)$.

61. При k , кратных 18 .

63. Например, $k = \varphi(10^{100})$.

65. Указание. $2^6 + 6^2 = 100$. Докажите, что если число n обладает нужным свойством, то число $n + 100$ тоже обладает им.

66. При $p = 2$ годится любое четное n . Пусть $p > 2$ и $n = (p-1)t$. Тогда $2^n \equiv 1$ и $n \equiv -t \pmod{p}$, так что в качестве m можно взять любое натуральное число вида $m = ps - 1$, где $s = 1, 2, 3, \dots$

68. а) 20 ; б) 20 .

69. а) **Указание.** Поскольку 2000 делится и на $\varphi(2^4) = 8$, и на $\varphi(5^4) = 4 \cdot 5^3$, имеем: $3^{2000} \equiv 1$ и по модулю 2^4 , и по модулю

5^4 . Следовательно, $3^{2000} \equiv 1 \pmod{10000}$. Ответ: $3^{1999} = \dots 6667$.

б) Поскольку $\varphi(5^4) = 5^3 \cdot (5 - 1) = 500$, то $2^{2000} = (2^{500})^4 \equiv 1 \equiv -624 \pmod{5^4}$, так что $2^{1999} = -624/2 = -312 \equiv 313 \pmod{5^4}$. Осталось подобрать такое целое x , что $313 + 625x$ делится на 16. Это легко: $313 = 320 - 7 \equiv -7$ и $625 = 624 + 1 \equiv 1 \pmod{16}$, так что годится $x = 7$. Значит, 2^{1999} оканчивается теми же четырьмя цифрами, что и число $313 + 625 \cdot 7 = 4688$.

в) Указание. $10000 = 16 \cdot 625$. Число $2^{3^{2000}}$ кратно 16. В силу теоремы Эйлера остаток от деления 3^{2000} на 500 равен 1; поскольку $\varphi(625) = 500$, имеем: $2^{3^{2000}} \equiv 2 \pmod{625}$. Осталось подобрать такое целое x , что $2 + 625x$ делится на 16.

Ответ: 8752.

70. Достаточно разобрать случай $x \neq y$. Поскольку $1998 = 2 \cdot 3^3 \cdot 37$, достаточно доказать отсутствие решений в натуральных взаимно простых числах x, y , где $x \neq y$, и целых неотрицательных числах a, b, c уравнения $x^7 + y^7 = 2^a \cdot 3^b \cdot 37^c$. Обозначим $N = 2^a \cdot 3^b \cdot 37^c$ и $t = \varphi(N)$. Поскольку f не делится на 7, существует такое натуральное число t , что $7t \equiv 1 \pmod{f}$.

Возводя сравнение $x^7 \equiv -y^7 \pmod{N}$ в t -ю степень, получаем: $x^{7t} \equiv (-y^7)^t$. Очевидно, число t нечетно (ибо f четно). Поэтому $x \equiv x^{7t} \equiv (-y^7)^t = -y^{7t} \equiv -y \pmod{N}$, так что $x + y$ делится на $N = x^7 + y^7$, что невозможно из-за неравенства $x + y < x^7 + y^7$.

71. Пусть $k - 1$ делится на 2^s и не делится на 2^{s+1} . Предположим, что при всех достаточно больших натуральных l число $p = 2^{2^l} + k$ простое. Очевидно, если $2^l > s$, то $p - 1 = 2^{2^l} + k - 1 = 2^s h$, где h нечетно.

В силу теоремы Эйлера, $2^{\varphi(h)} \equiv 1 \pmod{h}$. Поэтому $2^{s+\varphi(h)} \equiv 2^s \pmod{2^s h}$. Следовательно, при $l \geq s$ имеем $2^{l+\varphi(h)} \equiv 2^l \pmod{p-1}$.

В силу малой теоремы Ферма,

$$2^{2^{l+\varphi(h)}} + k \equiv 2^{2^l} + k \equiv 0 \pmod{p}.$$

Поскольку $2^{2' + \varphi(h)} + k > 2^{2'} + k = p$, то число $2^{2' + \varphi(h)} + k$ составное. Задача решена.

72. г) Всякое натуральное число вида $6m - 1$ имеет хотя бы один простой делитель вида $p = 6k - 1$. Пусть $a^2 + a + 1$ кратно p . Тогда $a^3 - 1 = (a - 1)(a^2 + a + 1)$ тоже кратно p . Если $a \equiv 1 \pmod{p}$, то $a^2 + a + 1 \equiv 1^2 + 1 + 1 = 3$, что невозможно, ибо $p \neq 3$. Значит, порядок числа a по модулю p равен 3, откуда $p - 1$ кратно 3. Но $p - 1 = 6k - 2$ не кратно 3.

73. Указание. $a^{12} - 1 = (a^6 - 1)(a^4 - a^2 + 1)$.

74. в) Указание.

$$a^{15} - 1 = (a - 1)(a^2 + a + 1)(a^4 + a^3 + a^2 + a + 1)(a^8 - a^7 + a^5 - a^4 + a^3 - a + 1).$$

75. Указания. а) В силу предыдущего упражнения $a + 1 \equiv -a^2 \pmod{p}$.

б) Докажите, что $a^3 - a^2 + a - 1 \equiv a^4 \pmod{p}$.

77. Указание. Существует такое целое c , что $bc \equiv 1 \pmod{p}$. Число $(ac)^{2^n} + 1$ кратно p .

78. Указание. Если p — простой общий делитель чисел n и $a^{2^n} + 1$, то $p \leq n$ и $p = 2^{n+1}k + 1 > 2^{n+1} > n$.

79. а) Пусть n четно и a^{n+1} делится на $n + 1$. Записав $n = 2^m k$, где k — нечетное, имеем: любой простой делитель числа $a^n + 1 = (a^k)^{2^m} + 1$ сравним с 1 по модулю 2^{m+1} .

Поскольку произведение чисел, сравнимых с 1 по модулю 2^{m+1} , тоже сравнимо с 1 по этому модулю, и поскольку $n + 1 = 2^m k + 1 \not\equiv 1 \pmod{2^{m+1}}$, получаем противоречие.

Итак, n нечетно. Теперь очевидно, что a тоже нечетно.

б) **Указание.** Рассмотрите $n = a^{a^m}$.

80. а) Следует из предыдущего упражнения. б) Убедитесь, что если $2^n + 2$ кратно n и если $2^n + 1$ кратно $n - 1$ (это верно, например, для $n = 2$), то $2^{2^n+2} + 2$ кратно $2^n + 2$ и $2^{2^n+2} + 1$ кратно числу $2^n + 1$.

81. Примените индукцию и разложение суммы кубов в произведение их суммы и неполного квадрата их суммы.

82. $2^{3n} + 1 = (2^n + 1)((2^n)^2 - 2^n + 1)$; первый множитель кратен n , а второй кратен 3, поскольку из условия $2^n \equiv -1 \pmod{n}$ имеем $2^n \equiv -1 \pmod{3}$, откуда $(2^n)^2 - 2^n + 1 \equiv (-1)^2 - (-1) + 1 \equiv 0 \pmod{3}$.

84. Примените утверждение предыдущего упражнения: а) при $a = 8$; б) при $a = 512$.

85. Достаточно разобрать случай $a \neq b$. Числа a и b нечетны. Обозначим буквой n их наименьшее общее кратное. Тогда $2^n + 1$ кратно числу $2^a + 1$, которое кратно числу b . Аналогично, $2^n + 1$ кратно $2^b + 1$, которое кратно a . Значит, $2^n + 1$ кратно как a , так и b , а значит, и их наименьшему общему кратному n . Поскольку $n > 3$, то в силу пункта а) предыдущего упражнения n кратно 9.

Предположим для определенности, что a не кратно 3. Тогда легко проверить, что $2^a + 1$ не делится на 9. Это противоречит тому, что b делится на 9.

86. $n = 1$ или 3. *Указание.* Пусть $n > 3$ и $2^n + 1$ кратно n^2 . Представим n в виде $n = 3^a m$, где m не кратно 3. Тогда $a > 1$. Индукцией по a при помощи формулы суммы кубов можно доказать, что $(2^m)^{3^a} + 1$ не делится на 3^{a+2} . Число n^2 делится на 3^{2a} . Очевидно, $2a \geq a + 2$. Значит, $2^n + 1$ не делится на n^2 при $n > 3$.

87. а) Пусть $2^n - 1$ кратно n , причем $n > 1$. Тогда n нечетно. Рассмотрим наименьший простой делитель p числа n . Порядок числа 2 по модулю p не превосходит $p - 1$ и является делителем числа n . Поскольку этот порядок больше 1, мы получили противоречие.

б) Например, числа вида $n = 6k$.

в) Рассмотрите последовательность, заданную своим первым членом $n_1 = 1$ и соотношением $n_{k+1} = a^{n_k} - 1$.

88. а) *Указание.* Если a четно, то $a^{a+1} + 1$ делится на $a + 1$. Если же a нечетно, то $a^2 + 1$ четно, но не делится на 4, так что $a^{a^2+1} + 1$ делится на $a^2 + 1$. Значит, хотя бы одно n , для которого $a^n + 1$ кратно n , существует.

Чтобы построить бесконечное множество, докажите, что если $a^n + 1$ кратно n , то $a^{a^n+1} + 1$ кратно $a^n + 1$. (Для доказательства разберите два случая: n нечетно и n четно.)

б) *Ответ:* при всех a , кроме чисел вида 3, 7, 15, ..., $2^n - 1$, ... *Указание.* Если $a + 1$ делится на простое нечетное

число p , то $a^p + 1$ делится на p^2 . Если же $a + 1$ — степень двойки, $n > 1$ и $a^n + 1$ делится на n^2 , то в силу упражнения 83 число n четно; а при четном n число $a^n + 1$ не делится на 4.

89. Если $\text{НОД}(s, p-1) = d > 1$, то $(g^s)^{(p-1)/d} = (g^{s/d})^{p-1} \equiv 1 \pmod{p}$. Поскольку $(p-1)/d < p-1$, мы доказали, что число g^s не является первообразным корнем по модулю p .

Осталось доказать, что если $\text{НОД}(s, p-1) = 1$, то g^s — первообразный корень. Это можно делать разными способами. Можно доказывать, что числа $s, 2s, 3s, \dots, (p-1)s$ дают разные остатки при делении на $p-1$ (докажите!). А можно рассуждать «от противного»: если бы g^s не было первообразным корнем, то существовало бы натуральное число $r < p-1$, для которого $(g^s)^r \equiv 1 \pmod{p}$; но тогда sr должно делиться на $p-1$, что невозможно из-за взаимной простоты чисел s и $p-1$.

91. а) 5; б) 6; в) 3. Так как $257 = 2^8 + 1$, то $2^{16} - 1$ делится на 257. Следовательно, порядок числа 2 по модулю 257 не превосходит $16 < 256$. Проверим, что 3 — первообразный корень: $3^8 \equiv 136$, $3^{16} \equiv 249 \equiv -2^3$, $3^{64} \equiv 2^{12} = 1024 \cdot 4 \equiv (-4) \cdot 4 = -16$, следовательно, $3^{128} - 1 = (3^{64} - 1)(3^{64} + 1) \not\equiv 0 \pmod{257}$.

92. а) $2^8 \equiv -7 \pmod{263}$, $2^{16} \equiv 49$, $2^{32} \equiv 34$, $2^{64} \equiv 104$, $2^{128} \equiv 33$; следовательно, $2^{131} = 2^3 \cdot 2^{128} \equiv 8 \cdot 33 \equiv 1$. Значит, 2 не является первообразным корнем, а -2 — является: $(-2)^{131} \equiv -1 \not\equiv 1$ и $(-2)^2 \not\equiv 1 \pmod{263}$.

б) *Указание.* Если $a^3 \not\equiv a$, то $a \not\equiv 0$ и $(\pm a)^2 \not\equiv 1$. $a^{82} - 1 = (a^{41} - 1)(a^{41} + 1)$. Значит, для всякого $a (\not\equiv 0)$ либо $a^{41} \equiv 1$, либо $a^{41} \equiv -1$. И вообще, для всякого простого числа $p = 2q + 1$, где q — тоже простое, $q > 2$, ровно одно из чисел a и $-a$, где $a^3 \not\equiv a \pmod{p}$, является первообразным корнем по модулю p .

95. а) $x \equiv 1$, $2^3 \equiv 8$, $2^6 \equiv 12$ или $2^9 \equiv 5 \pmod{13}$.

96. *Указание.* $x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$.

Ответ: $x \equiv 2^4, 2^8, 2^{12}, 2^{16}, 2^{20}$ или $2^{24} \pmod{29}$. (Этот же ответ можно записать иначе: $x \equiv 16, 24, 7, 25, 23$ или 20 .)

97. Если k делится на $p-1$, то все слагаемые сравнимы с 1 по модулю p и потому сумма сравнима с $p-1 \not\equiv 0 \pmod{p}$.

Если же k не делится на $p - 1$, то существует такое не кратное p число x , что $x^k \not\equiv 1 \pmod{p}$. Обозначим $S = 1^k + 2^k + \dots + (p-1)^k$. Сумма $x^k + (2x)^k + \dots + ((p-1)x)^k = x^k S$ сравнима с S по модулю p , поскольку (после взятия остатков от деления на p) ряд чисел $x, 2x, 3x, \dots, (p-1)x$ отличается от ряда $1, 2, \dots, p-1$ только перестановкой, а от перемены мест слагаемых сумма не меняется. Значит, $x^k S \equiv S \pmod{p}$, откуда $(x^k - 1)S \equiv 0$, т.е. $S \equiv 0 \pmod{p}$.

Если пользоваться существованием первообразного корня, то доказывать, что при k , не кратных $p - 1$, сумма S кратна p , можно и при помощи формулы суммы геометрической прогрессии:

$$1^k + g^k + g^{2k} + \dots + g^{(p-2)k} = \frac{1 - g^{(p-1)k}}{1 - g^k} \equiv 0 \pmod{p}.$$

Ответ. При k , не кратных $p - 1$.

98. а) $101^2(1 + 2 \cdot 8^2) = 1315929$; б) $17^3(1 + 6 \cdot 8^2) = 1891505$.

99. *Ответ:* 1. *Указание.* Для каждого из чисел $a = 1, 2, \dots, p - 1$ существует и единственно такое число b , что $ab \equiv 1 \pmod{p}$ и $1 \leq b \leq p - 1$. Это число b является первообразным корнем тогда и только тогда, когда a — первообразный корень.

100. б) *Указание.* Пусть для определенности q — простой делитель числа m . Тогда $(ab)^{mn/q} = a^{mn/q} \cdot (b^n)^{m/q} \equiv a^{mn/q} \not\equiv 1 \pmod{p}$, ибо mn/q не кратно числу m .

Далее, при $p = 5$ порядки чисел 2 и 3 равны 4, а порядок произведения $2 \cdot 3 \equiv 1 \pmod{5}$ равен 1.

102. а) $n = 1$, p^m или $2p^m$, где p — простое, m — натуральное.

103. а) *Ответ:* $x \equiv \pm a$ или $2^{m-1} \pm a \pmod{2^m}$. *Указание.* Поскольку $(x + a) - (x - a) = 2a$, числа $x - a$ и $x + a$ не могут оба делиться на 4. Значит, либо одно из них делится на 2^m , либо одно делится на 2^{m-1} , а другое четно.

106. а) *Указание.* $n - 1$ кратно числу $2p$. *Замечание.* Все числа $n = (4^p - 1)/3$, где $p > 3$, — составные. При $p = 5$ получаем $n = 341$.

108. б) При $a = 0$ или 1 годится $n = 4$; при $a = -2$ — число $n = 6$; при $a = 2$ — указанное в пункте а) число $a = 161038$. Если $|a| > 2$, то годится $n = |a|$, если a четно, и $n = 2|a|$, если a нечетно.

в) Можно считать, что $a > 1$. Пусть $a^n \equiv a \pmod{n}$, причем m – чётно, $m > 2$. Рассмотрим такое (существующее по теореме Биркгофа–Вандивера) простое число p , что $a^{n-1} - 1$ кратно p , но ни при каком $m < n - 1$ разность $a^m - 1$ не кратна p . В силу теоремы 6 число $p - 1$ делится на $n - 1$. Следовательно, $p \geq n$. Поскольку n чётно, то $p > n$.

Поскольку $np - 1 = n - 1 + n(p - 1)$ делится на $n - 1$, то $a^{np-1} - 1$ делится на $a^{n-1} - 1$. По малой теореме Ферма, $a^{np-1} = a^{n(p-1)} \cdot a^{n-1} \equiv 1 \pmod{p}$.

Следовательно, разность $a^{np} - a$ делится и на n , и на p , а потому и на np . Строя таким образом все новые и новые числа, мы доказываем утверждение задачи.

109. б) Нетрудно проверить, что $n = 65$ – наименьшее составное натуральное число, для которого $3^{n-1} \equiv 2^{n-1} \pmod{n}$.

в) Если пользоваться бесконечностью множества чисел Кармайкла, то достаточно рассмотреть $n = 3^k - 2^k$, где k – число Кармайкла, и применить утверждение пункта а).

Можно обойтись и без этого, рассмотрев $n = 3^{2^t} - 2^{2^t}$. Тогда числа $3^{2^t} - 1$ и 2^{2^t} кратны 2^t , так что опять применимо утверждение пункта а).

110. Указание. Для любого числа a , взаимно простого с n , рассмотрите сумму $S = a^{n-1} + (2a)^{n-1} + \dots + ((n-1)a^{n-1})$. Докажите, что $S \equiv 1^{n-1} + 2^{n-1} + \dots + (n-1)^{n-1} \equiv -1$ и $S \equiv a^{n-1} (1^{n-1} + 2^{n-1} + \dots + (n-1)^{n-1}) \equiv -a^{n-1} \pmod{n}$.

Числа Фибоначчи

1. $\varphi_0 = 0, \varphi_{-1} = 1, \varphi_{-2} = -1, \varphi_{-3} = 2, \dots$, и вообще, $\varphi_{-n} = (-1)^{n+1} \varphi_n$.

3. Лемма. Если известны числа a , b и c , причем $c \geq a$ и $c \geq b$, а расположены они вдоль прямой так:

$$\underbrace{a, \dots, c}_{\varphi_k}, \underbrace{c, \dots, b}_{\varphi_{k-1}},$$

т.е. сначала a , затем $\varphi_k - 1$ неизвестных чисел, затем c , еще $\varphi_{k-1} - 1$ неизвестных чисел и, наконец, b , то можно найти локальный максимум за $k - 2$ переворачивания.

Доказательство – индукция по k . **База.** $k = 2$ – ничего переворачивать не надо. **Переход.** Перевернем карточку d , расположенную на расстояниях φ_{k-1} и φ_{k-2} от a и c соответ-

ственно:

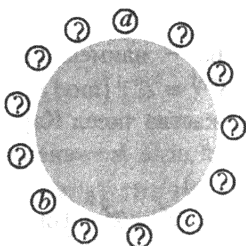
$$\underbrace{a, \dots, d}_{\Phi_{k-1}}, \underbrace{\dots, c}_{\Phi_{k-2}}, \underbrace{\dots, b}_{\Phi_{k-1}}.$$

Если $d > c$ (или $d \leq c$, выбросим все числа, расположенные справа от c (соответственно, слева от d), и воспользуемся предположением индукции. Лемма доказана.

Вернемся к задаче. Поскольку

$$\varphi_n = \varphi_{n-1} + \varphi_{n-2} = 2\varphi_{n-2} + \varphi_{n-3},$$

мы перевернем две карточки a и b , между которыми $\varphi_{n-2} - 1$ других карточек. Пусть для определенности $a \leq b$. Разобьем



окружность на три дуги, в которых φ_{n-2} , φ_{n-3} и φ_{n-2} карточек соответственно, причем пусть a и b — начальные (для определенности, при движении вдоль окружности против часовой стрелки; на рисунке $n = 7$) карточки первых двух дуг. Перевернем начальную карточку третьей дуги и обозначим ее число буквой c . Если $c \leq b$, применяем лемму к дуге $a \dots b \dots c$; если же $c > b$, то к дуге $a \dots c \dots b$.

4. Если n четно, то соотношение Кассини можно записать в виде $\varphi_{n-1}\varphi_{n+1} = \varphi_n^2 + 1$. Поскольку число -1 не является квадратичным вычетом ни по какому простому модулю p , где $p \equiv 3 \pmod{4}$, то ни φ_{n-1} , ни φ_{n+1} не делится на p .

5. а) $\varphi_{2n} = \varphi_{n+n} = \varphi_n\varphi_{n-1} + \varphi_{n+1}\varphi_n = (\varphi_{n+1} + \varphi_{n-1})\varphi_n = (\varphi_{n+1} + \varphi_{n-1})(\varphi_{n+1} - \varphi_{n-1}) = \varphi_{n+1}^2 - \varphi_{n-1}^2$.

6. Рассмотрим параллелограмм $CDEF$. Треугольник ABC подобен треугольнику AFB , следовательно, $\frac{1}{d} = \frac{d-1}{1}$, т.е.

$d^2 - d = 1$, откуда $d = \frac{1 + \sqrt{5}}{2}$ — так называемое золотое сечение.

7. $\frac{1}{d} = \frac{d-1}{1}$. Опять золотое сечение!

9. Раскрасим вершины восьмиугольника через одну в синий и зеленый цвета. Поскольку при каждом прыжке цвет вершины меняется, то за нечетное число прыжков в вершину E из вершины A не попасть. Обозначим через b_n и d_n количества способов, которыми можно за $2n - 1$ прыжок попасть из A , соответственно, в B_1 и D_1 (разумеется, столькими же способами можно попасть из A в B_2 и D_2). Очевидно, за $2n$ прыжков

лягушка может попасть из A в E ровно $2d_n$ способами. Обозначим через a_n количество способов, которыми за $2n$ прыжков можно, начав движение в вершине A , вернуться в нее, а через c_n — число способов за $2n$ прыжков припрыгать в вершину C_1 (столько же способов — в C_2).

Поскольку $a_n = 2b_n$, $c_n = b_n + d_n$ и $b_{n+1} = a_n + c_n$, $d_{n+1} = c_n$, то $b_{n+1} = a_n + c_n = 2b_n + b_n + d_n = 3b_n + d_n$ и $d_{n+1} = c_n = b_n + d_n$. Рассмотрим таблицу

n	1	2	3	4	5
b_n	1	3	10	34	116
d_n	0	1	4	14	48

Нетрудно угадать и доказать по индукции закономерности $b_{n+2} = 4b_{n+1} - 2b_n$ и $d_{n+2} = 4d_{n+1} - 2d_n$. Найдем все геометрические прогрессии a , aq , aq^2 , aq^3 , ..., удовлетворяющие этому рекуррентному соотношению:

$$aq^{n+1} = 4aq^n - 2aq^{n-1},$$

откуда $q^2 - 4q + 2 = 0$, т.е. $q = 2 \pm \sqrt{2}$. Подберем такие числа α и β , что $d_n = \alpha(2 + \sqrt{2})^n + \beta(2 - \sqrt{2})^n$. Для этого составим уравнения для $n = 1$ и 2 :

$$\begin{cases} 0 = \alpha(2 + \sqrt{2}) + \beta(2 - \sqrt{2}), \\ 1 = \alpha(2 + \sqrt{2})^2 + \beta(2 - \sqrt{2})^2. \end{cases}$$

Решив эту систему, находим $\alpha = 1/(4 + 4\sqrt{2})$ и $\beta = 1/(4 - 4\sqrt{2})$. Следовательно,

$$2d_n = \frac{1}{\sqrt{2}} \left((2 + \sqrt{2})^{n-1} - (2 - \sqrt{2})^{n-1} \right).$$

10. Пользуясь разложением частного двух последовательных чисел Фибоначчи в цепную дробь, докажите, что при $n \geq 3$ частное от деления φ_{n+1} на φ_n не меньше 1,5 и не больше 1,7. Затем воспользуйтесь следующими оценками: $\varphi_{n+5} = \varphi_{n+4} + \varphi_{n+3} = 2\varphi_{n+3} + \varphi_{n+2} = 3\varphi_{n+2} + 2\varphi_{n+1} = 5\varphi_{n+1} + 3\varphi_n \geq 5 \cdot 1,5\varphi_n + 3\varphi_n > 10\varphi_n$ и $\varphi_{n+3} = \varphi_{n+2} + \varphi_{n+1} = 2\varphi_{n+1} + \varphi_n = 3\varphi_n + 2\varphi_{n-1} \leq 3 \cdot 1,7\varphi_{n-1} + 2\varphi_{n-1} < 10\varphi_{n-1}$.

11. Если первая прогрессия имеет вид u , ux , ux^2 и ux^3 , а вторая — v , vy , vy^2 и vy^3 , то из уравнений $a = u + v$, $b = ux +$

$+vy$, $c = ux^2 + vy^2$, $d = ux^3 + vy^3$ для нахождения величин $p = x + y$ и $q = xy$ получаем систему уравнений $bp - aq = (ux + vy)(x + y) - (u + v)xy = c$ и $cp - bq = (ux^2 + vy^2)(x + y) - (ux + vy)xy = d$. Решив эту систему линейных относительно p и q уравнений, мы затем должны найти x и y как корни так называемого характеристического уравнения $z^2 - pz + q = 0$. Теперь легко разобраться со всеми пунктами задачи.

а) Может: решив уравнения, получаем последовательность $2^n + \frac{(-1)^n}{3}$.

б) Может: это последовательность Φ_{n+1} .

в) Не может: характеристическое уравнение $z^2 - 2z + 1 = 0$ имеет кратные корни.

г) Характеристическое уравнение $z^2 - 4z + 5 = 0$ имеет невещественные корни $q = 2 \pm i$. Поэтому если ограничиваться прогрессиями с вещественными членами, ответ отрицательный, а если допустить комплексные — утвердительный.

д) Равенство $(ux^{n+2} + vy^{n+2}) = (ux^{n+1} + vy^{n+1})p - (ux^{n+1} + vy^{n+1})q$ доказывает, что если p и q рациональны, то из рациональности двух соседних членов последовательности следует, что и следующий член тоже является рациональным числом.

12. Для каждого $k = 1, 2, \dots, m^2$ рассмотрим пару остатков $(\varphi_k \bmod m; \varphi_{k+1} \bmod m)$. Вследствие взаимной простоты соседних чисел Фибоначчи пара $(0; 0)$ невозможна. Количество остатков от деления на m равно m , поэтому количество пар остатков равно m^2 . Следовательно, какая-то пара остатков встречается как минимум дважды:

$$(\varphi_k \bmod m; \varphi_{k+1} \bmod m) = (\varphi_{k+r} \bmod m; \varphi_{k+r+1} \bmod m), (*)$$

где $1 \leq k < k+r \leq m^2 + 1$. Очевидно, $\varphi_{k-1} = \varphi_{k+1} - \varphi_k \equiv \varphi_{k+r+1} - \varphi_{k+r} = \varphi_{k+r-1} \pmod{m}$, так что $\varphi_{k-1} \bmod m = \varphi_{k+r-1} \bmod m$. Поэтому если $k > 1$, то можно вместо k рассмотреть $k - 1$, свойство $(*)$ сохранится. Уменьшая и уменьшая таким образом величину k , мы доведем ее до минимально возможного значения $k = 1$ и таким образом получим равенство $(1; 1) = (\varphi_{1+r} \bmod m; \varphi_{1+r+1} \bmod m)$, откуда $\varphi_r = \varphi_{r+2} - \varphi_{r+1} \equiv 1 - 1 = 0 \pmod{m}$.

13. Частное $\varphi_{2n}/\varphi_n = \varphi_{n-1} + \varphi_{n+1} = 2\varphi_{n-1} + \varphi_n$ нечетно, если φ_n нечетно.

Если же φ_n четно, то φ_{n-1} нечетно (соседние числа Фибоначчи взаимно просты и поэтому не могут быть оба четны). Если $\varphi_n \div 4$, то $\varphi_{2n}/\varphi_n = 2\varphi_{n-1} + \varphi_n$ не делится на 4; если же φ_n не делится на 4, то сумма $2\varphi_{n-1} + \varphi_n$ двух четных чисел, не делящихся на 4, кратна 4.

14. В силу леммы 1 имеем $\varphi_{kn} \equiv k\varphi_n\varphi_{n+1}^{k-1} \pmod{\varphi_n^2}$. Поскольку число φ_{n+1} взаимно просто с φ_n , то φ_{kn} делится на φ_n^2 тогда и только тогда, когда k делится на φ_n .

15. В силу леммы 1 имеем $\varphi_{np} \equiv p\varphi_n\varphi_{n+1}^{p-1} \pmod{\varphi_n^2}$. Ни p , ни φ_{n+1} не кратны q .

Квадратичный закон взаимности

1. Для $p = 2$ или 3 годится $x = 2$ или 3 соответственно. Пусть $p > 3$. Пусть ни для какого целого числа x ни $x^2 - 2$, ни $x^2 - 3$ не делятся на p . Тогда $\left(\frac{2}{p}\right) = -1$ и $\left(\frac{3}{p}\right) = -1$. Следовательно,

$$\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right) \cdot \left(\frac{3}{p}\right) = (-1) \cdot (-1) = 1,$$

так что существует целое число x , для которого $x^2 \equiv 6 \pmod{p}$.

2. Очевидно,

$$(1+i)^p \equiv 1 + i^{8n+1} = 1 + i \cdot (i^4)^{2n} = 1 + i \pmod{p},$$

откуда, сокращая на $1 + i$ обе части сравнения, получаем

$$(1+i)^{p-1} \equiv 1 \pmod{p}.$$

Поскольку $(1+i)^2 = 2i$, имеем

$$2^{(p-1)/2} = (2i)^{4n} = (1+i)^{4n} \equiv 1 \pmod{p}.$$

Вспомнив критерий Эйлера, мы видим, что $\left(\frac{2}{p}\right) = 1$ при $p = 8n + 1$. Аналогично можно разобрать случаи $p = 8n + 3$, $8n + 5$ или $8n + 7$.

Александр Васильевич Спивак

Арифметика

Библиотечка «Квант». Выпуск 102

Приложение к журналу «Квант» №4/2007

Редактор *А.Ю.Котова*

Обложка *А.Е.Пацхверия*

Макет и компьютерная верстка *Е.В.Морозова*

Компьютерная группа *Е.А.Митченко, Л.В.Калиничева*

ИБ № 87

Формат 84×108 1/32. Бум. офсетная. Гарнитура кудряшевская.

Печать офсетная. Объем 5 печ.л. Тираж 3000 экз.

Заказ № 330.

119296 Москва, Ленинский пр., 64-А, «Квант»

Тел.: (495)930-56-48, e-mail: admin@kvant.info

Отпечатано в ОАО Ордена Трудового Красного Знамени
«Чеховский полиграфический комбинат»

142300 г.Чехов Московской области.

Сайт: www.chpk.ru. E-mail: marketing@chpk.ru

Факс: 8(49672)6-25-36, факс. 8(499)270-73-00

Отдел продаж услуг многоканальный 8(499) 270-73-59

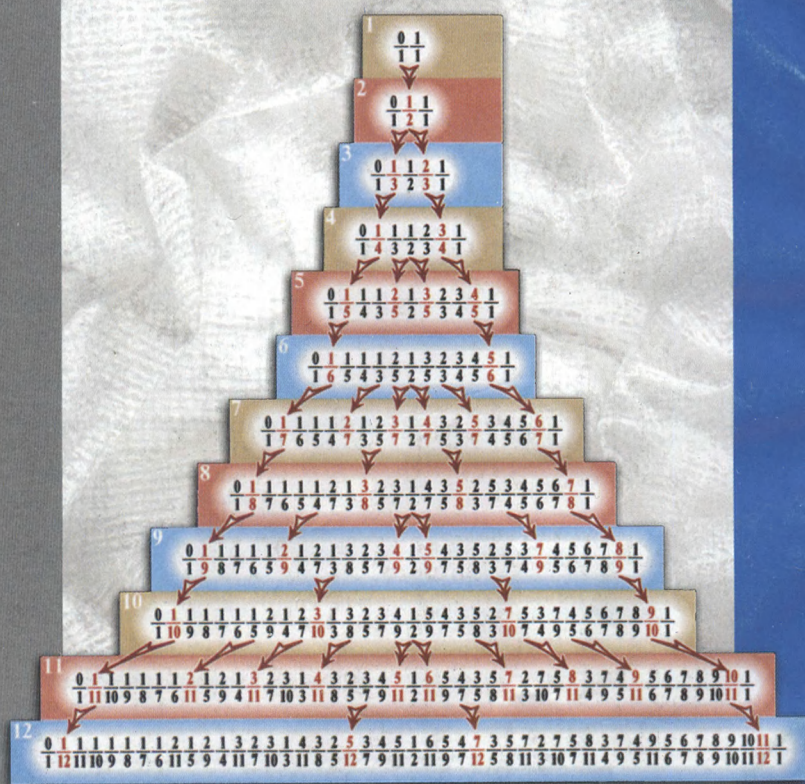
40=

Индекс 70465



Библиотечка КВАНТ

АРИФМЕТИКА



ВЫПУСК

102