УДК 511.2
ББК 22.13
С 34

Сизый С. В. **Лекции по теории чисел:** Учеб. пособие для студентов вузов. — 2-е изд., испр. — М.: ФИЗМАТЛИТ, 2008. — 192 с. — ISBN 978-5-9221-0741-9.

Настоящее учебное пособие представляет собой переработанный конспект лекций по курсу «Теория чисел» для студентов третьего курса механико-математического факультета Уральского государственного университета. В пособии представлены следующие разделы теории чисел: теория делимости целых чисел, цепные дроби, мультипликативные функции, теория сравнений, трансцендентные числа. Большинство разделов снабжено задачами для самостоятельного решения.

Рекомендовано к изданию Научно-методическим советом по математике и механике УМО университетов России в качестве учебного пособия для математических специальностей и направлений подготовки в университетах.

Табл. 5. Ил. 8. Библиогр. 22 назв.

Рецензенты:

Доцент кафедры алгебры и дискретной математики
Уральского государственного университета
Н. Ф. Сесекин

Доцент кафедры высшей математики
Уральского государственного технического университета
С. И. Тарлинский

ISBN 978-5-9221-0741-9

ОГЛАВЛЕНИЕ

Предисловие

Так уж было угодно судьбе, что эта книжка создавалась автором в довольно сложный период жизни России — борьба за демократию, международный терроризм, становление новой экономики, глубокие личные переживания. Автор искренне благодарит своих старших учителей и товарищей — профессора Л. Н. Шеврина и профессора В. А. Баранского за всестороннюю моральную поддержку и вдохновляющие беседы.

Автор искренне признателен Л. Н. Шеврину за эстетический, стилистический и композиционный анализ книжки. Последующие творческие обсуждения значительно улучшили ее текст.

Огромное спасибо Н. Ф. Сесекину, взявшему на себя труд первого прочтения и рецензирования рукописи.

Отдельное спасибо С. И. Тарлинскому, любезно прочитавшему первоначальный вариант издания и первому отважившемуся применить его в школьном преподавании (для учеников физико-математического класса специализированного лицея при Уральском госуниверситете).

Автор благодарит своих друзей Д. Н. Бушкова, В. Б. Савинова и Л. Ф. Спевака за обсуждение стиля и моральную поддержку.

Кроме того, все вышесказанное не означает, что автор хочет разделить с кем-то ответственность за ошибки, недочеты и довольно фривольный стиль этой книжки. Просто, автор желает выразить благодарность многим и многим людям, которые так или иначе приняли участие в ее создании. Спасибо всем!

Введение

Всякое искусство совершенно бесполезно.
О. Уайльд

Теория чисел — раздел математики, занимающийся изучением чисел непосредственно как таковых, их свойств и поведения в различных ситуациях. Упаси, Боже, меня давать здесь точное определение понятия «Теория чисел», так как, во-первых, я его не знаю, а во-вторых, даже если вы поместите в одну ε-окрестность двух ученых-профессионалов, работающих по их мнению в теории чисел, то они могут подраться между собой, так и не придя к единому мнению, из чего же состоит «Теория чисел». Я надеюсь, что читатели тоже будут иметь свое мнение по этому вопросу после окончания процесса понимания хотя бы одного учебника или (скромно так) этой книжки по теории чисел.

В головах многих математиков, как профессионалов, так и любителей, паразитирует мнение, что теория чисел — это наиболее абстрактная и отдаленная от практических применений математическая теория, пусть красивая и стройная сама по себе (эдакая «вещь в себе», по Канту), но совершенно бесполезная с точки зрения народного хозяйства.

Более того, некоторые теоретики-числовики даже гордятся такой точкой зрения, считая себя богемными представителями «чистого искусства», которое неприменимо, например, для создания атомной бомбы или чего-нибудь еще в этом роде. Они задирают нос, освобождают себя от моральных страданий Оппенгеймера и Эйнштейна, они творят красоту и только красоту, выше которой идет мудрость уже божественная, океан слепящего, непостижимого света.

Бедолаги! Их богемность разбивается уже фразой Пифагора: «Все есть число!», — и изучая числа, они неизбежно изучают окружающий нас мир и себя в том числе (каламбур). Но кроме этого философского замечания о практической применимости «чистой» теории чисел, я расскажу вам одну правдивую историю. Эта история убедит любого эстета от математики в том, что теория чисел — не просто красивейшая и стройнейшая область чистой науки, но и серьезная народохозяйственная структура.

В начале семидесятых годов XX в. американское космическое агентство NASA, получив от Конгресса США несколько миллиардов долларов, решило осуществить запуск исследовательского спутника на Юпитер. Спутник склепали, напичкали дорогостоящей аппаратурой, назвали «Пионер» (лектору в этом месте рекомендуется характерный жест правой рукой наискосок об лоб), и запустили вверх. Для успешного управления дальнейшим полетом уворочennого агрегата, ежику понятно, необходимо было постоянно перерасчитывать его траекторию, корректируя ее от случайных возмущений и целя в Юпитер, который, между прочим, хоть и большой, но летает от нас на расстоянии более 100 миллионов километров, поэтому попасть в него ужасно трудно.

Знатоки знают, что для расчета подобных траекторий нужно решать систему дифференциальных уравнений, которую не то что решать, а даже и писать-то не хочется, настолько она сложна и огромна. Но Пионер-то уже летит, а Конгресс внимательно следит за расходом средств налогоплательщиков, поэтому специалисты NASA вынуждены считать эти многомерные интегралы, причем в режиме реального времени. «В режиме реального времени» — это означает, что интеграл надо успеть посчитать до того, как спутник улетит вместо Юпитера в деревню Пропадайлово.

Знатоки опять знают, что единственный известный сегодня быстрый способ вычисления таких интегралов с использованием компьютера — это метод Монте-Карло (это такой город, а не фамилии авторов метода). Далее буду краток. Монте-Карлу нужно многократное случайное бросание точки в многомерную область. Электронная машина не умеет генерировать случайные числа, так как она работает по программе, написанной заранее на языке FORTRAN (в середине XX в. был такой). FORTRAN разработали специально для запуска пионеров и вставили в него датчик («датчик» — от слова «выдавать») случайных чисел $\mathrm{RND}(n)$, который, работая по некоторой наспех созданной схеме, выдавал последовательность «квазислучайных» чисел из отрезка $[0;1]$, равномерно на нем распределенную. Все было здорово.

Беда началась тогда, когда эти «квазислучайные» числа начали объединять в пары, тройки и т. д., чтобы получить координаты «случайной» точки многомерной области. $\mathrm{RND}(n)$ оказался составленным настолько неудачно, что 60% «случайных» точек из единичного квадрата на плоскости (всего-то двумерная область!) попадали в его нижнюю половину, а это даже в боксе не одобряют! Монте-Карло не сработал, спутник промазал мимо Юпитера

всего на каких-то 20 миллионов километров, и несколько миллиардов долларов вылетели в трубу.

Мораль: если теоретик-числовик на несколько минут спускается со своих заоблачных высот на бренную землю, чтобы сообщить процедуру получения случайных чисел с помощью эффектной цепочки делений и взятия остатков, выгоните его сразу — дешевле будет. Народохозяйственное применение теории чисел здесь очевидно: она должна дать такой способ получения случайных чисел, чтобы мы могли спокойно и спутники запускать, и землю пахать, и напильники коллекционировать. Вывод: изучайте теорию чисел, восторгайтесь ее красотами, любуйтесь ею, как произведением искусства, но помните, что вопреки эпиграфу к этому введению из «Портрета Дориана Грея», всякое искусство где-нибудь и когда-нибудь приносит пользу. Читателей же, заинтересовавшихся машинным получением случайных чисел, отсылаю к великолепной книжке Д. Кнута «Искусство программирования для ЭВМ», т. 2 «Получисленные алгоритмы», гл. 3 «Случайные числа». Увлекательное чтиво!

Ну как, дорогие читатели, убедил ли я вас в практической значимости теории чисел? Только не говорите, что нет, иначе мне придется рассказать еще сотню подобных историй, а это не входит ни в мои планы, ни в планы традиционных университетских курсов по теории чисел. Я хочу закончить на этом многословную общую болтовню о предмете, которому с любовью посвящаю эту скромную книжку, однако, по традиции, во введениях всего мира делают несколько предварительных замечаний и информируют читателя об устройстве дальнейшего текста, а, стало быть, и курса теории чисел. Сим и займемся.

Текст настоящей книжки незатейливо разбивается на параграфы, каждый из которых освещает некоторую тему достаточно полно с точки зрения автора (и, возможно, только автора). Каждый параграф, в свою очередь, разбивается на небольшие пункты. Студенты! Ожидаемый мною устный ответ на экзаменационный вопрос — это либо отдельный пункт (если он не очень большой), либо теорема с доказательством (любому студенту это должно быть понятно). Упорядоченность материала внутри каждого параграфа линейная, поэтому книжку рекомендуется читать подряд, а не так, как делал один мой однокурсник, читая сначала четные пункты, потом — нечетные. Однако, если у вас механически-идеальная память, вы можете изучать теорию чисел и этим способом.

В конце большинства пунктов приведено несколько задач для самостоятельного решения и каждый раз ваше внимание к их местонахождению привлекается картинкой, наподобие  .

Не гнушайтесь прорешать предлагаемые задачи, ибо человек начинает уютно себя чувствовать в изучаемом теоретическом материале только после решения нескольких задач.

Обозначения в книжке везде абсолютно стандартны и приводить их полный список нет надобности. Автодорожный знак  отмечает те места в тексте, на которых автору хочется заострить внимание читателя. Каждое специфическое обозначение всюду разъясняется в момент его появления, символ ⇳ нигде далее не встречается, а значок ♦ в тексте обычно обозначает конец доказательства и ассоциируется у автора с эффектным финальным шлепком бубнового туза по столу.

От всего сердца желаю вам крепкого здоровья, хорошего настроения и успехов в изучении прекрасного раздела математики — теории чисел. Удачи!

§ 1. ОСНОВНЫЕ ПОНЯТИЯ И ТЕОРЕМЫ

1. Деление с остатком

Целые числа — суть $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$. В этой книжке будет употребляться довольно стандартное обозначение этого множества — жирная буква $\mathbf{Z}$. Известно, что относительно обычных операций сложения и умножения множество целых чисел является кольцом, а для более страстных почитателей алгебры можно сказать и точнее: $\mathbf{Z}$ является моногенным ассоциативно-коммутативным кольцом с единицей. [1)]

«Прекрасная половина» $\{1, 2, 3, 4, \dots\}$ множества целых чисел зовется множеством натуральных чисел и стандартно обозначается жирной буквой $\mathbf{N}$.

Определение. Пусть $a, b \in \mathbf{Z}$. Число a *делится на число* b, если найдется такое число $q \in \mathbf{Z}$, что $a = qb$. Синонимы: a кратно b; b — делитель a. Запись: $a \vdots b$ или $b \mid a$.

Легко заметить, что отношение делимости $b \mid a$ есть бинарное отношение на множестве $\mathbf{Z}$, а если ограничиться рассмотрением только натуральных чисел, то несложно установить, что на множестве $\mathbf{N}$ это бинарное отношение является рефлексивным, антисимметричным и транзитивным, т. е. отношением частичного

[1)] Этот привычный со школьной скамьи объект на самом деле является очень сложным, но я не буду сейчас объяснять, в чем состоит сложность арифметики целых чисел, ибо такое объяснение может увести нас слишком далеко от названия этого пункта. Математику-профессионалу в этом месте могут прийти в голову и знаменитая теорема Гёделя о неполноте формальной арифметики, и выдающийся результат Матиясевича об алгоритмической неразрешимости систем диофантовых уравнений, и великое множество элементарно формулируемых, но до сих пор нерешенных теоретико-числовых проблем, и т. д., и т. п. Однако давайте пока воспримем $\mathbf{Z}$ просто как объект, преподнесенный нам в подарок природой-матушкой и займемся его изучением.

порядка. Легко проверяется также следующее свойство:

пусть $a_1 + a_2 + \ldots + a_n = c_1 + c_2 + \ldots + c_k$ — равенство сумм целых чисел. Если все слагаемые в этом равенстве, кроме одного, кратны b, то и оставшееся слагаемое обязано быть кратным b.

Перечисленные свойства отношения делимости позволят нам доказать основную теорему первого пункта.

Теорема. *Для данного целого отличного от нуля числа b всякое целое число a единственным образом представимо в виде $a = bq + r$, где $0 \leqslant r < |b|$.*

Доказательство. Ясно, что одно представление числа a равенством $a = bq + r$ мы получим, если возьмем bq равным наибольшему кратному числа b, не превосходящему a (см. рис. 1).

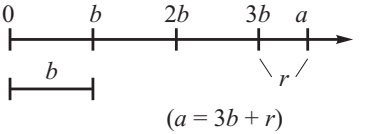


Рис. 1

Тогда, очевидно, $0 \leqslant r < |b|$. Докажем единственность такого представления. Пусть $a = bq + r$ и $a = bq_1 + r_1$ — два таких представления. Значит, $0 = a - a = b(q - q_1) + (r - r_1)$. Здесь 0 делится на b; $b(q - q_1)$ делится на b, следовательно, $(r - r_1)$ обязано делиться на b. Так как $0 \leqslant r < b$ и $0 \leqslant r_1 < b$, то $r - r_1 < b$ и $r - r_1$ делится на b, значит, $r - r_1$ равно нулю, а, значит, и $q - q_1$ равно нулю, т. е. два таких представления совпадают. ♦

Сразу после доказательства теоремы, пока не забылись использовавшиеся в нем обозначения, дадим

Определение. Число q называется *неполным частным*, а число r — *остатком* от деления a на b.

Признаюсь, что идея рис. 1, поясняющего доказательство теоремы, принадлежит не мне, а древним грекам. Именно древние греки, почему-то очень любили многократно укладывать один отрезок в другой, а оставшуюся часть большего отрезка, естественно, называли «остатком».

Заметим, дорогие читатели, что остаток — всегда есть число неотрицательное, а вот неполное частное может быть каким угодно целым числом. Поэтому на вопрос: «Сколько будет

минус пять поделить на три с остатком?», каждый должен бойко отвечать: «Минус два, в остатке — один!». Но за добрый десяток лет опыта приема устных вступительных экзаменов в университет, судьба еще не послала мне абитуриента, правильно ответившего на этот вопрос. А ведь это дети, специально готовившие себя поступать именно на математико-механический факультет. «Печально я гляжу на наше поколение...»

Задачки

1. Разделите с остатком: а) 161 на 17; б) −161 на 17; в) 161 на −17; г) −161 на −17.

2. Разделите с остатком: а) 17 на 161; б) −17 на 161; в) 17 на −161; г) −17 на −161.

3. Проверьте, что множество $\mathbf{N}\backslash\{1\} = \{2, 3, 4, \dots\}$ с отношением делимости есть частично упорядоченное множество. Найдите его минимальные элементы.

4. Справедливый ковбой зашел в бар и попросил у бармена стакан виски за 3 доллара, пачку Marlboro за доллар и 11 центов, шесть пачек патронов для своего кольта и дюжину коробков спичек. Услышав итоговую сумму — 28 долларов и 25 центов, ковбой пристрелил бармена. За что?

2. Наибольший общий делитель

Не затягивая развития событий, начнем сразу с определения.

Определение. Число $d \in \mathbf{Z}$, делящее одновременно числа $a, b, c, \dots, k \in \mathbf{Z}$, называется *общим делителем* этих чисел. Наибольшее d с таким свойством называется *наибольшим общим делителем*. Обозначение: $d = (a, b, c, \dots, k)$.

Перечислим, кое-где доказывая, основные свойства наибольшего общего делителя. Первое свойство покажет нам, как устроен наибольший общий делитель двух целых чисел.

***Свойство* 1**. *Если* $(a, b) = d$, *то найдутся такие целые числа* u *и* v, *что* $d = au + bv$.

Доказательство. Рассмотрим множество $\mathbf{P} = \{au + bv \mid u, v \in \mathbf{Z}\}$. Очевидно, что $\mathbf{P} \subseteq \mathbf{Z}$, а знатоки алгебры могут проверить, что $\mathbf{P}$ — идеал в $\mathbf{Z}$. Очевидно, что $a, b, 0 \in \mathbf{P}$. Пусть $x, y \in \mathbf{P}$ и $y \neq 0$. Тогда остаток от деления x на y принадлежит $\mathbf{P}$.

Действительно:

$$x = yq + r, \quad 0 \leqslant r < y,$$
$$r = x - yq = au_1 + bv_1 - au_2 + bv_2)q =$$
$$= a(u_1 - u_2q) + b(v_1 - v_2q) \in \mathbf{P}.$$

Пусть $d \in \mathbf{P}$ — наименьшее положительное число из $\mathbf{P}$ (призадумайтесь, почему такое имеется!). Тогда a делится на d. В самом деле, $a = dq + r_1$, $0 \leqslant r_1 < d$, $a \in \mathbf{P}$, $d \in \mathbf{P}$, значит $r_1 \in \mathbf{P}$, следовательно, $r_1 = 0$. Аналогичными рассуждениями получается, что b делится на d, значит d — общий делитель a и b.

Далее, раз $d \in P$, то $d = au_0 + bv_0$. Если теперь d_1 — общий делитель a и b, то $d_1 \,|\, (au_0 + bv_0)$, т. е. $d_1 \,|\, d$. Значит, $d \geqslant d_1$ и d — наибольший общий делитель. ♦

***Свойство* 2.** *Для любых целых чисел a и k, очевидно, справедливо*: $(a, ka) = a$; $(1, a) = 1$.

***Свойство* 3.** *Если $a = bq + c$, то совокупность общих делителей a и b совпадает с совокупностью общих делителей b и c, в частности*, $(a, b) = (b, c)$.

Доказательство. Пусть $d \,|\, a$, $d \,|\, b$, тогда $d \,|\, c$. Пусть $d \,|\, c$, $d \,|\, b$, тогда $d \,|\, a$. ♦

Конечно, я привел здесь это «крутое» доказательство не потому, что читатели не смогли бы его придумать самостоятельно, а потому, что мне хочется, опять-таки, проиллюстрировать это доказательство на древнегреческий лад. Посмотрите на рис. 2:

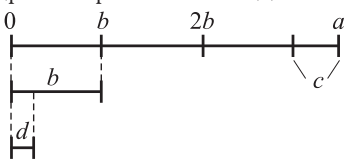


Рис. 2

Если d целое число раз укладывается в a и в b, то, очевидно, что d обязано целое число раз уложиться и в c. Наглядная иллюстрация! Спасибо грекам.

***Свойство* 4.** *Пусть a, b и m — произвольные целые числа. Тогда $(am, bm) = m(a, b)$.*

Доказательство. Если d — наибольший общий делитель чисел a и b, то $dm \,|\, am$ и $dm \,|\, bm$, т. е. dm — делитель am и bm. Покажем, что dm — наибольший общий делитель этих чисел. Поскольку d — наибольший общий делитель чисел a и b, то,

согласно свойству 1, для некоторых целых чисел u и v выполнено равенство $d = au + bv$. Умножив это равенство на m, получим равенство

$$dm = amu + bmv.$$

Видно, что если некоторое число s делит одновременно am и bm, то s обязано делить и dm, т. е. $s \leqslant dm$, следовательно, dm — наибольший общий делитель. ♦

***Свойство* 5.** *Пусть s — делитель a и b. Тогда*

$$\left(\frac{a}{s}, \frac{b}{s}\right) = \frac{(a,b)}{s}.$$

Доказательство. $(a,b) = \left(\frac{a}{s}s, \frac{b}{s}s\right) = s\left(\frac{a}{s}, \frac{b}{s}\right)$. ♦

***Свойство* 6.** *Очевидно теперь, что* $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$.

***Свойство* 7.** *Если* $(a,b) = 1$, *то* $(ac,b) = (c,b)$.

Доказательство. Пусть $(c,b) = d$. Имеем $d \,|\, b$, $d \,|\, c$, следовательно, $d \,|\, ac$, т. е. d — делитель ac и b. Пусть теперь $(ac,b) = s$. Имеем $s \,|\, b$, $s \,|\, ac$, s — делитель b, т. е. либо $s = 1$, либо s не делит a. Это означает, что $s \,|\, c$, значит, $s \,|\, d$. Итак, d и s делятся друг на друга, т. е. $d = s$. ♦

Что еще сказать в этом пункте? Да, пожалуй, больше и нечего.

Задачки

1. Докажите, что если $d = (a_1, a_2, \ldots, a_n)$ — наибольший общий делитель чисел $a_1, a_2, \ldots, a_n$, то найдутся такие целые числа $v_1, v_2, \ldots, v_n$, что

$$d = v_1a_1 + v_2a_2 + \ldots + v_na_n.$$

2. Вася любит Машу. Маша тоже любит Васю, но согласна выйти за него замуж только если наибольшие общие делители у пар чисел $(2^3 \cdot 5 \cdot 13 \cdot 45,\ 5^2 \cdot 11^6 \cdot 21)$ и $(6 \cdot 35 \cdot 10,\ 17^4 \cdot 15 \cdot 55)$ совпадают. Есть ли у Васи шанс?

3. Взаимно простые числа

Определение. Целые числа a и b *называются взаимно простыми*, если $(a,b) = 1$.

Вспоминая свойство 1 из предыдущего пункта, легко заметить, что два числа a и b являются взаимно простыми тогда и только тогда, когда найдутся целые числа u и v такие, что $au + bv = 1$.

Казалось бы, что особенного можно сказать о взаимно простых числах? Ну, нет у них общих делителей, отличных от 1 и -1, и все тут. Однако, зададимся вопросом: «Как часто встречаются пары взаимно простых чисел?», и постараемся ответить на него с довольно неожиданной точки зрения — в терминах теории вероятностей.

Пусть $X = \{x_n \,|\, n = 1, 2, \ldots\}$ — произвольная строго возрастающая последовательность натуральных чисел (или, если угодно, X — произвольное подмножество натуральных чисел, упорядоченное естественным образом). Обозначим через $\xi(N; X)$ число членов последовательности X, не превосходящих N.

Определение. Число

$$\rho = \overline{\lim_{N\to\infty}} \frac{\xi(N; X)}{N}$$

называется (верхней асимптотической) *плотностью последовательности* $X = \{x_n \,|\, n = 1, 2, \ldots\}$ в множестве $\mathbf{N}$.

Пример 1. Пусть $x_n = 2n$, где n пробегает $\mathbf{N}$, — последовательность всех четных чисел. Очевидно, что

$$\overline{\lim_{N\to\infty}} \frac{\xi(N; \{x_n\})}{N} = \frac{1}{2}.$$

Между прочим, это хорошо согласуется с нашими интуитивными представлениями о том, что четных чисел — половина.

Пример 2. Пусть $x_n = 2^n$, где n пробегает $\mathbf{N}$, — геометрическая прогрессия. Интуитивно ясно, что таких чисел в натуральном ряду мало, ибо чем «дальше в лес» по натуральному ряду, тем реже встречается степень двойки. Понятие плотности подтверждает это ощущение: $\xi(2^k; \{x_n\}) = k$, и, легко проверить, что

$$\overline{\lim_{N\to\infty}} \frac{\xi\,(N; \{x_n\})}{N} = \lim_{k\to\infty} \frac{k}{2^k} = 0.$$

Резонно считать, что плотность — это вероятность наугад вытащить из натурального ряда число, принадлежащее заданной последовательности. (Согласитесь, что вы всегда так и думали. Вероятность достать четное число есть $1/2$, а вероятность напороться на степень двойки, особенно среди больших чисел, вообще говоря, ничтожно мала).

Аналогично определению плотности последовательности можно дать определение плотности множества пар натуральных чисел. Пусть имеется произвольное множество X упорядоченных

пар натуральных чисел. Обозначим через $\xi(N;X)$ число пар из множества X, каждая компонента которых не превосходит N. Полезно представить себе пары чисел из множества X как координаты точек на координатной плоскости, тогда $\xi(N;X)$ есть просто число точек множества X, попавших в квадрат $\{(x,y)\,|\,0<x\leqslant N;0<y\leqslant N\}$.

Определение. Число

$$\rho=\varlimsup_{N\to\infty}\frac{\xi(N;X)}{N^2}$$

называется (верхней асимптотической) *плотностью множества пар* X в множестве $\mathbf{N}^2$.

Пример 3. Пусть X — множество всех пар натуральных чисел, у которых первая компонента строго больше второй. Множеству X соответствуют точки первой четверти координатной плоскости, лежащие под биссектрисой $y=x$. Плотность такого множества легко подсчитать:

$$\rho=\varlimsup_{N\to\infty}\frac{\xi(N;X)}{N^2}=\lim_{N\to\infty}\frac{N(N-1)/2}{N^2}=\frac{1}{2},$$

что, опять-таки, согласуется с нашим интуитивным представлением о том, что упорядоченных пар, у которых первая компонента превосходит вторую, примерно половина от общего количества всех пар натуральных чисел.

Пусть X — множество всех упорядоченных пар (u,v) натуральных чисел таких, что $(u,v)=1$, т. е. множество всех пар взаимно простых чисел. (В этом месте я подумал о неудачности стандартного обозначения (u,v) для наибольшего общего делителя, но, раз уж я влип в эту коллизию, то всякий раз в дальнейшем придется уповать на контекст, призванный вносить ясность в смысл обозначения.) Ответ на вопрос о частоте появления пары взаимно простых чисел дает удивительная теорема, открытая в 1881 г. итальянцем Э. Чезаро.

Теорема (Чезаро). *Вероятность выбрать из* $\mathbf{N}$ *пару взаимно простых чисел равна* $\dfrac{6}{\pi^2}$, *точнее*, $\varlimsup\limits_{N\to\infty}\dfrac{\xi(N;X)}{N^2}=\dfrac{6}{\pi^2}$.

Таким образом, плотность взаимно простых чисел в множестве $\mathbf{N}^2$, оказывается, существует и равна $\dfrac{6}{\pi^2}\approx 0{,}607\ldots$. Примерно в 60 % случаев вы вытащите из натурального ряда пару взаимно простых. И еще удивительно — в теореме Чезаро возникло число π, загадочное и вездесущее! Вот уж никак не ожидали мы встретить его посередь царства целых чисел!

Доказательство. Строгое доказательство теоремы Чезаро довольно сложно и громоздко. Но, как говорится, человека (а, в особенности, женщину) убеждает не строгая логика, а эмоция и правильно подобранные наводящие соображения. Вот и сейчас я схитрю и вместо строгого доказательства приведу некоторые эвристические рассуждения, призванные убедить читателя, почему эта теорема вообще должна быть правдоподобна.

Забудем, что существование вероятности (верхнего предела), строго говоря, нужно кропотливо доказывать. Предположим сразу, что существует вероятность p того, что случайно выбранные натуральные числа a и b взаимно просты.

Пусть $d \in \mathbf{N}$. Через $\mathsf{P}\{\mathbf{S}\}$ обозначим, как обычно, вероятность события $\mathbf{S}$. Рассуждаем:

$$\mathsf{P}\{(a,b)=d\} = \mathsf{P}\{d \mid a\}\cdot\mathsf{P}\{d \mid b\}\cdot\mathsf{P}\left\{\left(\frac{a}{d},\frac{b}{d}\right)=1\right\} = \frac{1}{d}\cdot\frac{1}{d}\cdot p = \frac{p}{d^2}.$$

Просуммировав теперь эти вероятности по всем возможным значениям d, мы должны получить единицу:

$$1 = \sum_{d\in\mathrm{N}} P\{(a,b)=d\} = \sum_{d=1}^{\infty}\frac{p}{d^2},$$

а сумма ряда $\sum\limits_{d=1}^{\infty}\dfrac{1}{d^2}$ известна и равна $\dfrac{\pi^2}{6}$ (см., напр., задачник Б. П. Демидовича по математическому анализу, раздел «Ряды Фурье»). Итак, $1 = \dfrac{\pi^2}{6}\cdot p$, следовательно, $p = \dfrac{6}{\pi^2}$. ♦

Лихо, правда?!

Задачки

1. Докажите, что из пяти последовательных целых чисел всегда можно выбрать одно, взаимно простое со всеми остальными.

2. Докажите, что из 16 последовательных целых чисел всегда можно выбрать одно, взаимно простое со всеми остальными.

3. Докажите, что каждые два числа последовательности $2+1, 2^2+1, 2^4+1, 2^8+1, \ldots, 2^{2^n}+1, \ldots$ являются взаимно простыми. [1])

4. (№ 2961 из задачника Демидовича). Разложить функцию $f(x) = x^2$ в ряд Фурье:

[1]) Между прочим, из утверждения этой задачи сразу следует бесконечность множества простых чисел. Действительно, если бы простых чисел было бы лишь конечное число, то не могло бы существовать бесконечно много чисел, попарно взаимно простых.

а) по косинусам кратных дуг в интервале $(-\pi, \pi)$;
б) по синусам кратных дуг в интервале $(0, \pi)$;
в) в интервале $(0, 2\pi)$.
Пользуясь этими разложениями, найти суммы рядов:

$$\sum_{n=1}^{\infty} \frac{1}{n^2}; \quad \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n^2}; \quad \sum_{n=1}^{\infty} \frac{1}{(2n-1)^2}.$$

5. Найдите плотность последовательностей:
а) $x_n = 5n + 2$;
б) $x_n = n^2$;
в) $x_n = n + 1000$.

6. Найдите плотность множества всех простых чисел. [1)]

7. Проверьте, что функция $\rho(X)$, ставящая в соответствие каждому множеству X натуральных чисел его плотность, удовлетворяет стандартным аксиомам вероятности:
1). $\rho(X) \geqslant 0$ для всех X (неотрицательность);
2). $\rho(\mathbf{N}) = 1$ (нормированность);
3). $\rho(\bigcup\limits_{n=1}^{\infty} X_n) = \sum\limits_{n=1}^{\infty} \rho(X_n)$ для попарно непересекающихся множеств X_n (счетная аддитивность).

8. Найдите плотность множества пар вида:
а) $(3n + 1, 4k + 3)$,
б) $(2^n, 4k + 3)$,
в) $(2^n, 3^k)$;
где n и k независимо пробегают $\mathbf{N}$.

9. Проверьте, что функция $\rho(X)$, ставящая в соответствие каждому множеству X упорядоченных пар натуральных чисел его плотность, удовлетворяет стандартным аксиомам вероятности.

10. Докажите, что если плотность последовательности строго больше нуля, то для любого натурального k в этой последовательности найдутся k членов, образующих k-членную арифметическую прогрессию. [2)]

[1)] Если эта задача вызывает затруднения, отложите ее в сторону, а после прочтения п. 15 вернитесь к ее решению. Правильный ответ — ноль.

[2)] Эта задачка — чистое издевательство, однако размышления над ней принесут вам немало пользы. Утверждение этой задачи в математическом мире известно как теорема Семиреди, а наиболее короткое ее доказательство, использующее эргодическую теорию, содержит около 60 с. Теорема Семереди устанавливает, в некотором смысле, характеристическое свойство арифметических прогрессий: всякая бесконечная арифметическая прогрессия имеет ненулевую плотность и всякая последовательность ненулевой плотности содержит сколь угодно длинную арифметическую прогрессию. Прекрасный рассказ об этой теореме и ее элементарное доказательство для $k = 3$ можно найти в книжке *Р. Грэхема* «Начала теории Рамсея». — М.: Мир, 1984.

4. Алгоритм Евклида

Слово «алгоритм» является русской транскрипцией латинизированного имени выдающегося арабского математика ал-Хорезми Абу Абдуллы Мухаммеда ибн ал-Маджуси (787–ок. 850) и означает в современном смысле некоторые правила, список инструкций или команд, выполняя которые, некто достигнет требуемого результата. В этом пункте я расскажу алгоритм, позволяющий по заданным натуральным числам a и b находить их наибольший общий делитель. Считается, что этот алгоритм придумал самый влиятельный математик всех времен и народов — Евклид, он изложил его в IX книге своих знаменитых «Начал».

Отступление «Панегирик Евклиду»

Не могу удержаться от небольшого исторического отступления про Евклида. О его жизни мы не имеем никаких достоверных сведений, может быть, даже, он не был реальной исторической личностью, а являлся коллективным псевдонимом некоей группы Александрийских математиков, типа Николя Бурбаки. Если он жил, то он жил во времена Птолемея Первого (306–283 до н. э.), которому, согласно преданию, он надерзил словами «К геометрии нет царской дороги». Но Птолемеи сознательно культивировали науку и культуру в Александрии, поэтому все эти закидоны своих ученых пропускали мимо ушей.

Наиболее знаменитое и выдающееся произведение Евклида — тринадцать книг его «Начал», но есть еще и другие мелкие опусы. Мы не знаем, какая часть этих трудов принадлежит самому Евклиду и какую часть составляют компиляции, но в этих трудах проявляется поразительная проницательность и дальновидность. Это — первые математические труды, которые дошли до нас от древних греков полностью. В истории Западного мира «Начала», после Библии, — наибольшее число раз изданная и более всего изучавшаяся книга. Большая часть нашей школьной геометрии заимствована буквально из первых шести книг «Начал», традиция Евклида до сих пор тяготеет над нашим элементарным обучением. Для профессионального математика эти книги все еще обладают неотразимым очарованием, а их логическое дедуктивное построение повлияло на сам способ научного мышления больше, чем какое бы то ни было другое произведение. Слава Птолемеям! Честь и хвала Евклиду! Идут пионеры — Салют «Началам»!

Панегирик окончен.

Пусть даны два числа a и b; $a \geqslant 0$, $b \geqslant 0$, считаем, что $a > b$. Символом $:=$ в записи алгоритма обозначаем присваивание. Алгоритм:

1. **Ввести** a и b.
2. **Если** $b = 0$, то **Ответ:** a. **Конец.**

3. **Заменить** $r :=$ «остаток от деления a на b», $a := b$, $b := r$.
4. **Идти** на 2.

Как и почему исполнение этого коротенького набора инструкций приводит к нахождению наибольшего общего делителя мы выясним чуть позже, сейчас же хочется сказать несколько слов про сам алгоритм. Внимательное разглядывание и пошаговое выполнение алгоритма Евклида убеждают в его, выражаясь словами иконописца Феофана Грека, «простоте без пестроты». Я очень сожалею, что в тексте невозможно проиллюстрировать работу алгоритма на греческий лад — греки стирали отрезки, нарисованные на песке. У лектора в аудитории в руках мел и тряпка, он может показать этот живой процесс на доске, а вам, дорогие читатели, придется довольствоваться застывшим рис. 3.

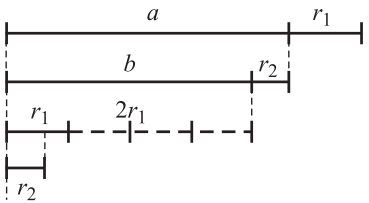


Рис. 3

В современной буквенной записи, кочующей из одного учебника в другой, алгоритм Евклида выглядит так: $a > b$; $a, b \in \mathbf{Z}$.

$$
\begin{aligned}
a &= bq_1 + r_1 && 0 \leqslant r_1 < b \\
b &= r_1 q_2 + r_2 && 0 \leqslant r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3 && 0 \leqslant r_3 < r_2 \\
r_2 &= r_3 q_4 + r_4 && 0 \leqslant r_4 < r_3 \\
&\vdots \\
r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1} && 0 \leqslant r_{n-1} < r_{n-2} \\
r_{n-2} &= r_{n-1} q_n + r_n && 0 \leqslant r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1} && r_{n+1} = 0
\end{aligned}
$$

Экзаменатор, настойчиво внушающий студенту мысль об ошибочности решения студента явиться на экзамен с невыученным алгоритмом Евклида.

Имеем $b > r_1 > r_2 > \ldots > r_n > 0$, следовательно, процесс оборвется **максимум через** b **шагов**. Очень интересный и практически важный народохозяйственный вопрос о том, когда алгоритм Евклида работает особенно долго, а когда справляется с работой молниеносно, мы рассмотрим в этой книжке чуть позже. Давайте

сейчас покажем, что $r_n = (a, b)$. Просмотрим последовательно равенства сверху вниз: всякий делитель a и b делит $r_1, r_2, \ldots, r_n$. Если же просматривать эту цепочку равенств от последнего к первому, то видно, что $r_n \mid r_{n-1}$, $r_n \mid r_{n-2}$, и т. д., т. е. r_n делит a и b. Поэтому r_n — наибольший общий делитель чисел a и b.

Как и всякая добротно выполненная работа, алгоритм Евклида дает гораздо больше, чем от него первоначально ожидалось получить. Из его разглядывания ясно, например, что совокупность делителей a и b совпадает с совокупностью делителей (a, b). Еще он дает практический способ нахождения чисел u и v из $\mathbf{Z}$ (или, если угодно, из теоремы п. 2) таких, что $r_n = au + bv = (a, b)$.

Действительно, из цепочки равенств имеем:

$$r_n = r_{n-2} - r_{n-1}q_n = r_{n-2} - (r_{n-3} - r_{n-2}q_{n-1})q_n = \ldots$$

(идем по цепочке равенств снизу вверх, выражая из каждого следующего равенства остаток и подставляя его в получившееся уже к этому моменту выражение)

$$\ldots = au + bv = (a, b).$$

Пример. Пусть $a = 525$, $b = 231$. Отдадим эти числа на растерзание алгоритму Евклида: (ниже приводится запись деления уголком, и каждый раз то, что было в уголке, т. е. делитель, приписывается к остатку от деления с левой стороны, а остаток, как новый делитель, берется в уголок)

$$\begin{array}{r|l}
525 & 231 \\
\cline{2-2}
462 & 2 \\
\cline{1-1}
231 & 63 \\
\cline{2-2}
189 & 3 \\
\cline{1-1}
63 & 42 \\
\cline{2-2}
42 & 1 \\
\cline{1-1}
42 & 21 \\
\cline{2-2}
42 & 2 \\
\cline{1-1}
0 &
\end{array}$$

Запись того же самого в виде цепочки равенств:

$$525 = 231 \cdot 2 + 63$$

$$231 = 63 \cdot 3 + 42$$

$$63 = 42 \cdot 1 + 21$$

$$42 = 21 \cdot 2$$

Таким образом, $(525, 231) = 21$. Линейное представление наибольшего общего делителя:

$$21 = 63 - 42 \cdot 1 = 63 - (231 - 63 \cdot 3) \cdot 1 =$$
$$= 525 - 231 \cdot 2 - (231 - (525 - 231 \cdot 2) \cdot 3) = 525 \cdot 4 - 231 \cdot 9,$$

и наши пресловутые u и v из $\mathbf{Z}$ равны, соответственно, 4 и –9.

Пункт 4 закончен.

Задачки

1. Предлагаю читателям самим придумать два разных трехзначных числа a и b и найти их наибольший общий делитель d и его представление в виде

$$d = au + bv, \quad u, v \in \mathbf{Z}.$$

Усложните задачу, заменив трехзначные числа четырехзначными, или даже пятизначными.

2. Найдите $d = (317811, 196418)$ и его представление в виде

$$d = 317811u + 196418v. \text{ [1)]}$$

3. Найдите $d =$ (81719, 52003, 33649, 30107).

5. Линейные диофантовы уравнения с двумя неизвестными

Обычно произвольное уравнение (но, как правило, все-таки с целыми коэффициентами) получает титул «диофантово», если хотят подчеркнуть, что его требуется решить в целых числах, т. е. найти все его решения, являющиеся целыми. Имя Диофанта — выдающегося александрийского математика — появляется здесь не случайно. Диофант интересовался решением уравнений в целых числах еще в третьем веке нашей эры и, надо сказать, делал это весьма успешно.

Отступление про Диофанта и его исторический след

Третий и последний период античного общества — период господства Рима. Рим завоевал Сиракузы в 212 г., Карфаген — в 146 г.,

[1)] Числа 196418 и 3167811 являются, соответственно, 27-м и 28-м членами последовательности Фибоначчи, с которой мы еще встретимся в этой книжке при анализе алгоритма Евклида. Для обработки алгоритмом Евклида этих двух чисел придется выполнить 26 делений с остатком, что, конечно, многовато для ручной работы, но я все-таки рекомендую вам ее проделать, дабы посмотреть, какие получаются остатки и почему они получаются именно такими.

Грецию — в 146 г., Месопотамию — в 46 г., Египет — в 30 г. до нашей эры. Огромные территории оказались на положении колоний, но римляне не трогали их культуры и экономического устройства, пока те исправно платили налоги и поборы. Установленный римлянами на столетия мир, в отличие от всех последующих великих миров и рейхов, принес всей завоеванной территории самый длинный период безвоенного существования, торговли и культурного обмена.

Александрия оказалась центром античной математики. Велись оригинальные исследования, хотя компилирование, пересказ и комментирование становились и стали основным видом научной деятельности. Александрийские ученые, если угодно, приводили науку в порядок, собирая разрозненные результаты в единое целое, и многие труды античных математиков и астрономов дошли до нас только благодаря их деятельности. Греческая наука с ее неуклюжим геометрическим способом выражения при систематическом отказе от алгебраических обозначений угасала, алгебру и вычисления (прикладную математику) александрийцы почерпнули с востока, из Вавилона, из Египта.

Основной труд Диофанта (ок. 250 г.) — «Арифметика». Уцелели только шесть книг оригинала, общее их число — предмет догадок. Мы не знаем, кем был Диофант, — возможно, что он был эллинизированный вавилонянин. Его книга — один из наиболее увлекательных трактатов, сохранившихся от греко-римской древности. В ней впервые встречается систематическое использование алгебраических символов, есть особые знаки для обозначения неизвестного, минуса, обратной величины, возведения в степень. Папирус № 620 Мичиганского университета, купленный в 1921 г., принадлежит эпохе Диофанта и наглядно это подтверждает. Среди уравнений, решаемых Диофантом, мы обнаруживаем такие, как $x^2 - 26y^2 = 1$ и $x^2 - 30y^2 = 1$, теперь известные нам как частные случаи «уравнения Пелля», причем Диофант интересуется их решениями именно в целых числах.

Книга Диофанта неожиданно оказала еще и огромное косвенное влияние на развитие математической науки последних трех столетий. Дело в том, что юрист из Тулузы Пьер Ферма (1601–1665), изучая «Арифметику» Диофанта, сделал на полях этой книги знаменитую пометку: «Я нашел воистину удивительное доказательство того, что уравнение $x^n + y^n = z^n$ при $n > 2$, не имеет решений в целых числах, однако поля этой книги слишком малы, чтобы здесь его уместить». Это одно из самых бесполезных математических утверждений получило название «Великой теоремы Ферма» и, почему-то, вызвало настоящий ажиотаж среди математиков и любителей (особенно после назначения в 1908 г. за его доказательство премии в 100 000 немецких марок). Попытки добить эту бесполезную теорему породили целые разделы современной алгебры, алгебраической теории чисел, теории функций комплексного переменного и алгебраической геометрии, практическая польза от которых уже не подлежит никакому сомнению. Сама теорема, кажется, благополучно доказана в 1995 г.; Пьер Ферма, конечно, погорячился на полях «Арифметики», ибо он физически не мог придумать подобного доказательства, требующего колоссальной совокуп-

ности математических знаний. Элементарного доказательства великой теоремы Ферма пока никто из жителей нашей планеты найти не смог, хотя над его поиском бились лучшие умы последних трех столетий.

Пусть требуется решить линейное диофантово уравнение:

$$ax + by = c, \quad \text{где } a, b, c \in \mathbf{Z}; \ a \text{ и } b \text{ — не нули.}$$

Попробуем порассуждать, глядя на это уравнение.

Пусть $(a, b) = d$. Тогда $a = a_1 d$; $b = b_1 d$ и уравнение выглядит так:

$$a_1 d \cdot x + b_1 d \cdot y = c, \quad \text{т. е. } d \cdot (a_1 x + b_1 y) = c.$$

Теперь ясно, что у такого уравнения имеется решение (пара целых чисел x и y) только тогда, когда $d \mid c$. Поскольку очень хочется решать это уравнение дальше, то пусть $d \mid c$. Поделим обе части уравнения на d, успокоимся, и всюду далее будем считать, что $(a, b) = 1$. Так можно.

Рассмотрим несколько случаев.

Случай 1. Пусть $c = 0$, уравнение имеет вид $ax + by = 0$ — «однородное линейное диофантово уравнение». Немножко потрудившись, находим, что $x = -\dfrac{b}{a}y$. Так как x должен быть целым числом, то $y = at$, где t — произвольное целое число (параметр). Значит $x = -bt$ и решениями однородного диофантова уравнения $ax + by = 0$ являются все пары вида $\{-bt, at\}$, где $t = 0; \pm 1; \pm 2; \ldots$. Множество всех таких пар называется общим решением линейного однородного диофантова уравнения, любая же конкретная пара из этого множества называется частным решением.

Дорогие читатели, не правда ли, что все названия уже до боли знакомы? «Однородное уравнение», «общее решение» — все это мы уже слышали и в курсе линейной алгебры и в лекциях по дифференциальным уравнениям. При разборе следующего случая эта аналогия буквально выпирает на первый план, что, конечно, не случайно, но исследование единства великого государства линейности на материке математики выходит за рамки этой скромной книжки.

Случай 2. Пусть теперь $c \neq 0$. Этот случай закрывается следующей теоремой.

Теорема. *Пусть* $(a,b)=1$, $\{x_0,y_0\}$ — *частное решение диофантова уравнения* $ax+by=c$. *Тогда его общее решение задается формулами*

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

Таким образом, и в теории линейных диофантовых уравнений общее решение неоднородного уравнения есть сумма общего решения соответствующего однородного уравнения и некоторого (любого) частного решения неоднородного уравнения. Вот оно — проявление единства линейного мира!

Доказательство. То, что правые части указанных в формулировке теоремы равенств действительно являются решениями, проверяется их непосредственной подстановкой в исходное уравнение. Покажем, что любое решение уравнения $ax+by=c$ имеет именно такой вид, какой указан в формулировке теоремы. Пусть $\{x^*,y^*\}$ — какое-нибудь решение уравнения $ax+by=c$. Тогда $ax^*+by^*=c$, но ведь и $ax_0+by_0=c$. Следуя многолетней традиции доказательства подобных теорем, вычтем из первого равенства второе и получим

$$a(x^*-x_0)+b(y^*-y_0)=0$$

— однородное уравнение. Далее, глядя на случай 1, рассмотрение которого завершилось несколькими строками выше, пишем сразу общее решение: $x^*-x_0=-bt$, $y^*-y_0=at$, откуда моментально, используя навыки средней школы, получаем

$$x^*=x_0-bt,\quad y^*=y_0+at. \qquad \blacklozenge$$

«Все это, конечно, интересно», — скажет читатель, — «Но как же искать то самое частное решение $\{x_0,y_0\}$, ради которого и затеяна вся возня этого пункта и которое, как теперь выясняется, нам так нужно?». Ответ прост. Мы договорились, что $(a,b)=1$. Это означает, что найдутся такие u и v из $\mathbf{Z}$, что $au+bv=1$ (если вы это забыли, вернитесь в п. 4), причем эти u и v мы легко умеем находить с помощью алгоритма Евклида. Умножим теперь равенство $au+bv=1$ на c и получим $a(uc)+b(vc)=c$, т. е. $x_0=uc$, $y_0=vc$. Вот и все!

Пример. Вы — хроноп, придуманный Хулио Кортасаром в книжке «Из жизни хронопов и фамов». Вам нужно расплатиться в магазине за синюю пожарную кишку, ибо красная в хо-

зяйстве уже давно есть. У вас в кармане монеты достоинством только в 7 и 12 копеек, а вам надо уплатить 43 копейки. Как это сделать? Решаем уравнение

$$7x + 12y = 43.$$

Включаем алгоритм Евклида:

$$\begin{aligned} 12 &= 7 \cdot 1 + 5, \\ 7 &= 5 \cdot 1 + 2, \\ 5 &= 2 \cdot 2 + 1, \\ 2 &= 1 \cdot 2. \end{aligned}$$

Значит, наибольший общий делитель чисел 7 и 12 равен 1, а его линейное выражение таково:

$$1 = 5 - 2 \cdot 2 = 5 - (7 - 5) \cdot 2 = (12 - 7) - (7 - (12 - 7) \cdot 2) = \\ = 12 \cdot 3 + 7 \cdot (-5),$$

т. е. $u = -5$, $v = 3$. Частное решение:

$$x_0 = uc = (-5) \cdot 43 = -215,$$
$$y_0 = vc = 3 \cdot 43 = 129.$$

Итак, вы должны отобрать у кассира 215 семикопеечных монет и дать ему 129 двенадцатикопеечных. Однако процедуру можно упростить, если записать общее решение неоднородного диофантова уравнения:

$$\begin{cases} x = -215 - 12t, \\ y = 129 + 7t, \end{cases}$$

и, легко видеть, что при $t = -18$, получаются вполне разумные $x = 1$, $y = 3$, поэтому дубасить кассира необязательно.

Задачки

1. Решите диофантовы уравнения:
а) $2x + 7y = 20$; б) $6x - 27y = 21$; в) $11x + 99y = 41$.

2. Для каждого целого z решите в целых числах уравнение

$$2x + 3y = 5z.$$

3. Решите уравнение $3\sin 7x + \cos 20x = 4$, а потом предложите решить его знакомому школьнику. Кто быстрее?

4. Сколькими различными способами можно расплатиться за вкуснейшую девяностосемикопеечную жевательную резинку лишь пятаками да копейками?

6. Простые числа и «основная» теорема арифметики

Определение. Число $p \in \mathbf{N}$, $p \neq 1$, называется *простым*, если p имеет в точности два положительных делителя: 1 и p. Остальные натуральные числа (кроме 1) принято называть составными. Число 1 — на особом положении, по договору, оно ни простое, ни составное.

Как это часто бывает в математике, да и в других науках, прилагательным «простой» называется объект только первоначально казавшийся простым. Простые числа, как выяснилось в процессе накопления научных знаний, появляются в различных областях математики и являются одним из самых загадочных и тяжелых для изучения монстров. Любопытного читателя, любителя ужастиков и лихо закрученных сюжетов, я отсылаю здесь к изумительному рассказу математика из Боннского университета Дон Цагира «Первые пятьдесят миллионов простых чисел», опубликованному в книжке «Живые числа», — М.: Мир, 1985 г.

Отметим некоторые несложные наблюдения, связанные с простыми числами.

Наблюдение 1. Наименьший делитель любого числа $a \in \in \mathbf{N}$, отличный от 1, есть число простое.

Доказательство. Пусть $c \mid a$, $c \neq 1$ и c — наименьшее с этим свойством. Если существует c_1 такое, что $c_1 \mid c$, то $c_1 \leqslant c$ и $c_1 \mid a$, следовательно, $c_1 = c$ или $c_1 = 1$. ♦

Наблюдение 2. Наименьший отличный от 1 делитель составного числа $a \in \mathbf{N}$ не превосходит $\sqrt{a}$.

Доказательство. $c \mid a$, $c \neq 1$, c — наименьший, следовательно $a = ca_1$, $a_1 \mid a$, $a_1 \geqslant c$, значит, $aa_1 \geqslant c^2 a_1$, $a \geqslant c^2$ и $c \leqslant \sqrt{a}$. ♦

Следующее наблюдение, отдавая дань уважения его автору — Евклиду, назовем теоремой.

Теорема (Евклид). *Простых чисел бесконечно много.*

Доказательство. От противного. Пусть $p_1, p_2, \ldots, p_n$ — все простые, какие только есть. Рассмотрим число $a = p_1 p_2 \cdot \ldots \cdot p_n + 1$. Его наименьший отличный от 1 делитель c, будучи простым, не может совпадать ни с одним из $p_1, p_2, \ldots, p_n$, так как иначе $c \mid 1$. Не перестаю удивляться изобретательности ума людей тысячелетней древности! ♦

Для составления таблицы простых чисел древний грек Эратосфен придумал процедуру, которая получила название «решето

Эратосфена»:

$$\underline{2}, \underline{3}, \cancel{4}, \underline{5}, \cancel{6}, \underline{7}, \cancel{8}, \cancel{9}, \cancel{10}, \underline{11}, \cancel{12}, \underline{13}, \cancel{14}, \cancel{15}, \cancel{16}, \underline{17}, \ldots$$

Идем по натуральному ряду слева направо. Подчеркиваем первое неподчеркнутое и невычеркнутое число, а из дальнейшего ряда вычеркиваем кратные только что подчеркнутому. И так много раз. Легко понять, что подчеркнутые числа — простые. Если вспомнить наблюдение 2, то становится понятно, что когда вычеркнуты все кратные простым, меньшим p, то оставшиеся невычеркнутые, меньшие p^2, — простые. Это значит, что составление таблицы всех простых чисел, меньших N, закончено сразу, как только вычеркнуты все кратные простым, меньшим $\sqrt{N}$.

Для чисел, растущих закономерно, например для квадратов или степеней двойки, было бы, конечно, нелепо разыскивать экземпляр, превосходящий все известные. Для простых же чисел, напротив, прилагаются громадные усилия, чтобы именно это и сделать. Чудаки люди! Например, в 1876 г. француз Люка доказал, что число $(2^{127}-1)$ — простое, и 75 лет оно оставалось наибольшим из известных простых чисел, что не покажется удивительным, если на него взглянуть:

$$2^{127}-1 = 170141183460469231731687303715884105727.$$

В настоящее время составлены таблицы всех простых чисел, не превосходящих 50 миллионов, далее известны только отдельные их представители. Читателей всегда привлекает гигантизм, поэтому укажу здесь два самых больших известных на сегодняшний момент простых числа: $2^{44497}-1$ и $2^{86243}-1$. Последнее число записано пока в книгу рекордов Гиннеса, в нем 25962 десятичных знака. Найдено оно было, конечно, в рекламных целях — демонстрация фирмой IBM возможностей очередного суперкомпьютера, которому для проверки этого числа на простоту с помощью специальных изощренных тестов (пригодных только для чисел вида 2^n-1) потребовалась неделя работы и куча денег.

Самой важной и общеизвестной в этом пункте является следующая теорема (искушенные алгебраисты скажут, что она утверждает факториальность кольца $\mathbf{Z}$, а я воздержусь от каких-либо комментариев в адрес этой теоремы, ибо про столь важную персону математического мира надо либо долго говорить, либо почтенно молчать). Эта теорема носит название «Основной теоремы арифметики».

Теорема. *Всякое целое число, отличное от* -1, 0 *и* 1, *единственным образом* (*с точностью до порядка сомножителей*) *разложимо в произведение простых чисел.*

Доказательство. Будем доказывать утверждение теоремы только для натуральных чисел, ибо знак минус перед числом умеют ставить все умеющие ставить знак минус.

Пусть $a > 1$, p_1 — его наименьший простой делитель. Значит, $a = p_1 a_1$. Если, далее, $a_1 > 1$, то пусть p_2 — его наименьший простой делитель и $a_1 = p_2 a_2$, т. е. $a = p_1 p_2 a_2$, и так далее, пока a_n не станет равным единице. Это обязательно произойдет, так как $a > a_1 > a_2 \ldots$, а натуральные числа с естественным порядком удовлетворяют условию обрыва убывающих цепей. Имеем, таким образом, $a = p_1 p_2 \ldots p_n$, и возможность разложения доказана.

Покажем единственность. Пусть $a = q_1 q_2 \cdot \ldots \cdot q_n$ — другое разложение, т. е. $p_1 p_2 \cdot \ldots \cdot p_n = q_1 q_2 \cdot \ldots \cdot q_s$. В последнем равенстве правая часть делится на q_1, следовательно, левая часть делится на q_1. Покажем, что если произведение $p_1 p_2 \cdot \ldots \cdot p_n$ делится на q_1, то один из сомножителей p_k обязан делиться на q_1.

Действительно, если $q_1 \,|\, p_1$, то все доказано. Пусть q_1 не делит p_1. Так как q_1 — простое число, то $(q_1, p_1) = 1$. Значит, найдутся такие $u, v \in \mathbf{Z}$, что $up_1 + vq_1 = 1$. Умножим последнее равенство на $p_2 \cdot \ldots \cdot p_n$, получим

$$p_2 \cdot \ldots \cdot p_n = p_1(p_2 \cdot \ldots \cdot p_n)u + q_1(p_2 \cdot \ldots \cdot p_n)v.$$

Оба слагаемых справа делятся на q_1, следовательно, $p_2 \cdot \ldots \cdot p_n$ делится на q_1. Далее рассуждайте по индукции сами.

Теперь пусть, например, $q_1 \,|\, p_1$. Значит, $q_1 = p_1$, так как p_1 — простое. Из равенства $p_1 p_2 \cdot \ldots \cdot p_n = q_1 q_2 \cdot \ldots \cdot q_s$ банальным сокращением моментально получим равенство $p_2 \cdot \ldots \cdot p_n = q_2 \cdot \ldots \cdot q_s$. Снова рассуждая по индукции, видим, что $n = s$, и каждый сомножитель левой части равенства $p_1 p_2 \cdot \ldots \cdot p_n = q_1 q_2 \cdot \ldots \cdot q_n$ обязательно присутствует в правой, и наоборот. ♦

Сразу отмечу без доказательства два достаточно очевидных следствия из этой теоремы.

Следствие 1. *Всякое рациональное число однозначно представимо в виде* $p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, *где* $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbf{Z}$. ♦

Следствие 2. *Если* $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$, $b = p_1^{\beta_1} p_2^{\beta_2} \cdot \ldots \cdot p_n^{\beta_n}$ — *целые числа, то наибольший общий делитель* a *и* b *равен* $p_1^{\gamma_1} p_2^{\gamma_2} \cdot \ldots \cdot p_n^{\gamma_n}$, *а наименьшее общее кратное* a *и* b *равно* $p_1^{\delta_1} p_2^{\delta_2} \cdot \ldots \cdot p_n^{\delta_n}$, *где* $\gamma_i = \min\{\alpha_i, \beta_i\}$, а $\delta_i = \max\{\alpha_i, \beta_i\}$. ♦

Можно очень долго анализировать, какие такие глубинные причины вызывают к жизни «основную теорему» арифметики, однако такой анализ, боюсь, уведет нас слишком далеко за пределы основных понятий арифметики. Отмечу только, что для справедливости обсуждаемой теоремы просто необходима аддитивная структура кольца целых чисел. Поясню необходимость наличия сложения плохим примером.

Плохой пример. Пусть $\mathbf{S} = \{4k+1 \mid k \in \mathbf{Z}\}$ — множество вот таких целых чисел. Легко проверить, что $\mathbf{S}$ замкнуто относительно умножения:

$$(4k_1+1)\cdot(4k_2+1) = 16k_1k_2 + 4k_2 + 4k_1 + 1 = \\ = 4\cdot(4k_1k_2 + k_1 + k_2) + 1 \in \mathbf{S},$$

однако это множество не замкнуто относительно сложения. «Квазипростые» числа из $\mathbf{S}$ — суть далее неразложимые в произведение чисел из $\mathbf{S}$: $5, 9, 13, 17, 21, 49, \ldots$. Индуктивным рассуждением, подобным рассуждению в первой части доказательства основной теоремы арифметики, легко убедиться, что всякое число из $\mathbf{S}$ разложимо в произведение «квазипростых». Однако единственность такого разложения отсутствует: $441 = 21\cdot 21 = 9\cdot 49$, при этом 9 не делит 21, и 49 не делит 21. Вот какой плохой пример.

Задачки

1. Докажите, что среди членов каждой из арифметических прогрессий:
а) 3, 7, 11, 15, 19,...; б) 5, 11, 17, 23, 29,...
в) 11, 21, 31, 41, 51,...имеется бесконечно много простых чисел. [1)]

2. Опоссум Порфирий в зоопарке раскладывает на простые множители число 81 057 226 635 000. Помогите ему, не то он обидится.

[1)] Оказывается, справедлив такой общий факт: Если первый член и разность арифметической прогрессии взаимно просты, то среди ее членов содержится бесконечно много простых чисел. Более того, ряд, составленный из обратных величин к этим простым числам, расходится. Это классическое утверждение называется теоремой Дирихле и доказывается весьма сложно. В 1950 г. датский математик А. Сельберг придумал чрезвычайно сложное и хитроумное элементарное (не использующее аппарат высшей математики) доказательство теоремы Дирихле, однако жить лучше от этого не стало и даже сильно одаренному школьнику доказательство теоремы Дирихле вряд ли объяснишь.

3. Методом Эратосфена составьте таблицу простых чисел, меньших 100.

4. Простое число — это число, имеющее в точности два различных положительных делителя (единицу и себя). Найдите все натуральные числа, имеющие в точности
а) три различных положительных делителя;
б) четыре различных положительных делителя;
в) k штук различных положительных делителей ($k > 4$).

5. Докажите, что в натуральном ряде имеются сколь угодно длинные промежутки вида $\{n, n+1, n+2, \dots, n+k\}$, не содержащие простых чисел.

6. Докажите, что не существует такого многочлена

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$$

с целыми коэффициентами, что все числа

$$f(0), f(1), f(2), f(3), \dots$$

являются простыми. [1])

---

[1]) Абсолютно несложное доказательство этого факта впервые придумал Л. Эйлер. Он же напридумывал массу многочленов $f(x)$, значения которых при многих последовательных натуральных x являются простыми числами. Два примера:

а) $f(x) = x^2 + x + 41$, при $x = 0, 1, 2, \dots, 39$.

б) $f(x) = x^2 - 79x + 1601$, при $x = 0, 1, 2, \dots, 79$.

Если же рассматривать многочлены от нескольких переменных, то, как следует из результатов Ю. В. Матиясевича о диофантовости рекурсивных множеств (опубликовано в 1970 г.), существуют многочлены, множество положительных значений которых в точности является множеством всех простых чисел. Преследуя чисто спортивный интерес, укажу здесь один такой многочлен от 26 переменных:

$$\begin{aligned}
&F(a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z) = \\
&= \{k+2\}\Big\{1 - (wz+h+j-q)^2 - (2n+p+q+z-e)^2 - \\
&- (a^2y^2 - y^2 + 1 - x^2)^2 - \big(\{e^4 + 2e^3\}\{a+1\}^2 - o^2\big)^2 - \\
&- \big(16\{k+1\}^3\{k+2\}\{n+1\}^2 + 1 - f^2\big)^2 - \\
&- \big(\{(a+u^4-u^2a)^2 - 1\}\{n+4dy\}^2 + 1 - \{x+cu\}^2\big)^2 - (ai+k+1-l-i)^2 - \\
&- \big(\{gk+2g+k+1\}\{h+j\} + h - z\big)^2 - \big(16r^2y^4\{a^2-1\} + 1 - u^2\big)^2 - \\
&- \big(p - m + l\{a-n-1\} + b\{2an + 2a - n^2 - 2n - 2\}\big)^2 - \\
&- \big(z - pm + pla - p^2l + t\{2ap - p^2 - 1\}\big)^2 - \\
&- \big(q - x + y\{a-p-1\} + s\{2ap + 2a - p^2 - 2p - 2\}\big)^2 - \\
&- (a^2l^2 - l^2 + 1 - m^2)^2 - (n + l + v - y)^2\Big\}.
\end{aligned}$$

§ 2. ЦЕПНЫЕ ДРОБИ

В этом параграфе мы отходим от изучения только целых чисел и действующими лицами станут произвольные действительные (как рациональные, так и иррациональные) числа. Сей параграф посвящен очень остроумному математическому аппарату — цепным (или непрерывным) дробям. Почему-то о них не рассказывают в школах, техникумах и университетах в обязательном порядке, а зря. Кроме того, что изучение цепных дробей занимательно само по себе, их применения выходят далеко за рамки теории чисел: они помогают исследовать числовые последовательности, анализировать алгоритмы, решать дифференциальные уравнения и т. д. Не претендуя на полноту изложения теории цепных дробей в этом параграфе и отдавая дань уважения славному ученому — математику А. Я. Хинчину, я сразу упомяну здесь его классическую книжку «Цепные дроби», в которой любопытный читатель найдет еще много интересных фактов, кроме тех, которые будут изложены ниже.

7. Разложение чисел в цепные дроби

Определение. *Цепной* (или, *непрерывной*) дробью называется выражение вида:

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cfrac{1}{\ddots \cfrac{}{q_n + \cfrac{1}{\ddots}}}}}}$$

Договоримся называть числа $q_1, q_2, \ldots, q_n, \ldots$ — неполными частными и считаем, что $q_1 \in \mathbf{Z}$, а $q_2, \ldots, q_n, \ldots \in \mathbf{N}$. Числа

$$\delta_1 = q_1, \quad \delta_2 = q_1 + \frac{1}{q_2}, \quad \delta_3 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}} \quad \text{и т. д.}$$

называются *подходящими дробями* цепной дроби α.

Цепная дробь может быть как конечной (содержащей конечное число дробных линий и неполных частных), так и бесконечной вниз и вправо (на юго-восток). В первом случае она, очевидно, представляет некоторое рациональное число, во втором случае — пока непонятно, что она вообще из себя представляет, но ясно, что все ее подходящие дроби — рациональные числа.

Договоримся называть *значением* (или *величиной*) бесконечной цепной дроби предел бесконечной последовательности ее подходящих дробей: $\alpha = \lim\limits_{n\to\infty} \delta_n$ (пока без всякого доказательства существования этого предела).

Наша глобальная цель на следующую тройку пунктов — доказательство основной теоремы о цепных дробях.

Теорема. *Всякое действительное число может быть разложено в цепную дробь единственным образом, и всякая конечная или бесконечная цепная дробь имеет своим значением некоторое действительное число.*

После доказательства этой теоремы можно будет смело сказать, что цепные дроби — это еще одна форма записи действительных чисел. Однако доказательство этой теоремы растянется у нас надолго. В процессе доказательства удобно будет вводить и исследовать новые понятия, складывать их в вашу копилку знаний, изучать их свойства. Именно поэтому я не буду сейчас писать с новой строки сакраментальное слово «**доказательство**» и собирать под его шапкой все дальнейшее. Обойдемся без этого слова, помня, что пока весь последующий рассказ как раз и нацелен на доказательство основной теоремы о цепных дробях.

Пусть $\alpha \in \mathbf{R}$ — действительное число, заключенное между двумя последовательными целыми числами: $a \leqslant \alpha < a+1$. Число a будем называть *нижним целым* числа α (это просто целая часть α), а число $a+1$ — *верхним целым*. Обозначениями для нижнего и верхнего целого числа α пусть будут, соответственно, $\lfloor\alpha\rfloor$ и $\lceil\alpha\rceil$.

Возьмем произвольное не целое действительное число $\alpha \in \mathbf{R}$, $\alpha \notin \mathbf{Z}$, $q_1 = \lfloor\alpha\rfloor$. Тогда $\alpha = q_1 + \beta_1$, $0 < \beta_1 < 1$, следовательно,

$$\alpha_2 = \frac{1}{\beta_1} > 1, \quad \text{и} \quad \alpha = q_1 + \frac{1}{\alpha_2}.$$

Если, далее, α_2 — не целое, то снова:

$$q_2 = \lfloor\alpha\rfloor, \;\; \alpha_2 = q_2 + \beta_2 = q_2 + \frac{1}{\alpha_3}, \;\; \alpha_3 > 1, \;\; \text{и} \;\; \alpha = q_1 + \frac{1}{q_2 + \frac{1}{\alpha_3}}.$$

Продолжая этот процесс взятия нижних целых и переворачивания дробных частей, получим запись произвольного числа $\alpha \in \mathbf{R}$ в виде цепной дроби. Изложенный процесс есть просто «лобовой» способ разложения произвольного числа в цепную дробь или, если угодно, наводящие соображения к доказательству основной теоремы.

Пример 1. Разложим в цепную дробь число $\alpha = \sqrt{2}$.

Имеем $q_1 = \lfloor \sqrt{2} \rfloor = 1$, $\beta_1 = \sqrt{2} - 1$, т. е. $\alpha = 1 + (\sqrt{2} - 1)$. Далее,

$$\alpha_2 = \frac{1}{\beta_1} = \frac{1}{\sqrt{2} - 1} = \frac{\sqrt{2} + 1}{1} = \sqrt{2} + 1,$$
$$q_2 = \lfloor \sqrt{2} + 1 \rfloor = 2, \quad \beta_2 = \sqrt{2} - 1,$$

$\alpha = 1 + \dfrac{1}{2 + (\sqrt{2} - 1)}$. Так как $\beta_1 = \beta_2$, то нетрудно понять, что этот процесс зациклится и, если его не останавливать, то получится бесконечная цепная дробь:

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}}}.$$

Все неполные частные в ней, начиная со второго, равны двойке.

Очевидно, что если $\alpha \in \mathbf{R}$ — иррационально, то описанный выше процесс бесконечен, так как иначе, в случае остановки этого процесса, α оказалось бы равным конечной цепной дроби, т. е. рациональному числу. Значит, всякое иррациональное число если и можно представить, то только бесконечной цепной дробью. Забудем пока про иррациональные числа и окунемся в приятный мир рациональных.

Пусть $\alpha \in \mathbf{Q}$, $\alpha = \dfrac{a}{b}$; $a, b \in \mathbf{Z}$, $b > 0$. Оказывается, что при этих условиях указанный выше процесс разложения числа в цепную дробь всегда конечен и выполним с помощью достопочтенного и любимого нами алгоритма Евклида. Действительно,

отдадим алгоритму числа a и b и внимательно посмотрим, что получится:

$$
\begin{aligned}
a &= bq_1 + r_1, && \text{т. е. } \frac{a}{b} = q_1 + 1\Big/\frac{b}{r_1},\\
b &= r_1q_2 + r_2, && \text{т. е. } \frac{b}{r_1} = q_2 + 1\Big/\frac{r_1}{r_2},\\
r_1 &= r_2q_3 + r_3, && \text{т. е. } \frac{r_1}{r_2} = q_3 + 1\Big/\frac{r_2}{r_3},\\
&\vdots\\
r_{n-2} &= r_{n-1}q_n + r_n, && \text{т. е. } \frac{r_{n-2}}{r_{n-1}} = q_n + 1\Big/\frac{r_{n-1}}{r_n},\\
r_{n-1} &= r_nq_{n+1}, && \text{т. е. } \frac{r_{n-1}}{r_n} = q_{n+1}.
\end{aligned}
$$

Значит,

$$
\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cfrac{1}{\ddots\,\cfrac{}{q_n + \cfrac{1}{q_{n+1}}}}}}},
$$

где $q_1, q_2, \ldots, q_{n+1}$ — как раз те самые неполные частные из алгоритма Евклида (вот откуда название этих чисел в цепных дробях). Таким образом, в случае рационального числа $\frac{a}{b}$, процесс разложения в цепную дробь конечен и дробь содержит не более b этажей. Наиболее одаренные читатели в этом месте уже поняли, что основная теорема о цепных дробях для рациональных чисел оказалась почти доказана (не доказали только единственность разложения, но она в случае конечных цепных дробей почти очевидна — приравняйте две цепных дроби и, рассуждая по индукции, получите, что у равных дробей совпадают все неполные частные).

Согласитесь, что горизонтальные дробные линии в начертании цепной дроби сильно напоминают рис. 3 из п. 4 — отрезки, которые рисовали древние греки на песке, да и связь алгоритма

Евклида с цепными дробями — непосредственная и, можно сказать, даже трогательно-интимная.

Пример 2. Этот пример заимствован мною из книги И. М. Виноградова «Основы теории чисел», ведь придумать самому такое рациональное число практически невозможно. Итак: разложить $\frac{105}{38}$ в цепную дробь.

Включаем алгоритм Евклида:

$$\begin{aligned} 105 &= 38 \cdot \underline{2} + 29, \\ 38 &= 29 \cdot \underline{1} + 9, \\ 29 &= 9 \cdot \underline{3} + 2, \\ 9 &= 2 \cdot \underline{4} + 1, \\ 2 &= 1 \cdot \underline{2}. \end{aligned}$$

Неполные частные я специально подчеркнул потому, что теперь для написания ответа нужно аккуратно расположить их подряд на этажах цепной дроби перед знаками плюс:

$$\frac{105}{38} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{2}}}}.$$

Вот и все. Потренируйтесь еще, пожалуйста, самостоятельно раскладывать числа в цепную дробь, решая задачки к этому пункту, а я на этом п. 7 заканчиваю.

Задачки

1. Разложите в цепную дробь число α, если:
а) $\alpha = \frac{5391}{3976}$; б) $\alpha = \frac{10946}{6765}$; [1] в) $\alpha = \sqrt{3}$; г) $\alpha = \frac{1+\sqrt{3}}{2}$; д) $\alpha = \log_2 3$ (ограничьтесь нахождением пяти первых неполных частных).

2. Вычислите для каждой цепной дроби из предыдущей задачи первые пять штук подходящих дробей $\delta_1, \delta_2, \delta_3, \delta_4, \delta_5$. Нарисуйте каждый раз на числовой оси число α и его подходящие дроби.

[1] Это отношение двадцать первого числа Фибоначчи к двадцатому.

8. Вычисление подходящих дробей

В этом пункте мы будем внимательно наблюдать за поведением подходящих дробей $\delta_1 = q_1$, $\delta_2 = q_1 + \dfrac{1}{q_2}$, $\delta_3 = q_1 + \dfrac{1}{q_2 + \dfrac{1}{q_3}}, \ldots$ цепной дроби

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cfrac{1}{\ddots \cfrac{}{q_n + \cfrac{1}{\ddots}}}}}}$$

с целью научиться быстро их вычислять, не связываясь с преобразованием многоэтажных выражений.

Понятно, что подходящая дробь δ_s, $s > 1$, получается из дроби δ_{s-1} заменой в записи выражения δ_{s-1} буквы q_{s-1} выражением $q_{s-1} + \dfrac{1}{q_s}$. Мы уже знаем из п. 7, что если «многоэтажную» подходящую дробь упростить (посчитать), то получится некоторое рациональное число $\dfrac{P}{Q}$ — «одноэтажная» дробь. Договоримся всегда буквой P_s обозначать числитель подходящей дроби δ_s (числитель именно ее рационального значения, т. е. «одноэтажной» дроби), а буквой Q_s — знаменатель. Давайте научимся быстро считать эти числители и знаменатели.

Положим для удобства $P_0 = 1$, $Q_0 = 0$. (Это просто соглашение, не пугайтесь, на ноль делить никто не заставляет.) Имеем

$$\delta_0 = \frac{P_0}{Q_0} = \infty,$$

$$\delta_1 = \frac{q_1}{1} = \frac{P_1}{Q_1}, \quad \text{т. е. } P_1 = q_1, \ Q_1 = 1,$$

$$\delta_2 = \frac{q_1 + \frac{1}{q_2}}{1} = \frac{q_1 q_2 + 1}{1 \cdot q_2 + 0} = \frac{q_2 P_1 + P_0}{q_2 Q_1 + Q_0} = \frac{P_2}{Q_2},$$

$$\delta_3 = \frac{\left(q_2 + \dfrac{1}{q_3}\right) P_1 + P_0}{\left(q_2 + \dfrac{1}{q_3}\right) Q_1 + Q_0} = \frac{q_3 P_2 + P_1}{q_3 Q_2 + Q_1} = \frac{P_3}{Q_3} \ \text{ и т. д.}$$

Видно, что получаются рекуррентные соотношения:

$$P_s = q_s P_{s-1} + P_{s-2} \ - \text{числители},$$
$$Q_s = q_s Q_{s-1} + Q_{s-2} - \text{знаменатели}.$$

Просьба хорошенько запомнить эти соотношения вместе с начальными условиями $P_0 = 1$, $Q_0 = 0$, $P_1 = q_1$, $Q_1 = 1$, ибо их использование значительно ускоряет процесс вычисления подходящих дробей и доставляет много других радостей. Сами соотношения очень легко доказать, если воспользоваться принципом математической индукции и головным мозгом. Проделайте это, пожалуйста, самостоятельно.

Пример. Вспомним разложение в цепную дробь числа $\frac{105}{38}$ из предыдущего пункта и вычислим подходящие дроби. Имеем

$$\frac{105}{38} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{2}}}}.$$

Вычисления числителей и знаменателей подходящих дробей организуем в таблицу.

s	0	1	2	3	4	5
q_s	Пустая клетка	2	1	3	4	2
P_s	1	2	3	11	47	105
Q_s	0	1	1	4	17	38

Посмотрите внимательно. Вторая строчка этой таблицы — неполные частные — заполняется сразу после работы алгоритма Евклида, числа $P_0 = 1$, $Q_0 = 0$, $P_1 = q_1$, $Q_1 = 1$ проставляются в таблицу автоматически. Две последние строки заполняются слева направо с использованием рекуррентных соотношений. Например, число $11 = P_3$ в третьей строке возникло так: тройка, стоящая над ним, умножилась на тройку, стоящую перед ним, и к результату прибавилась стоящая впереди двойка, ибо $P_3 = q_3 P_2 + P_1 = 3 \cdot 3 + 2$. После того, как в таблице уже стоит число 11, следующая клетка в этой строке заполняется числом

$4 \cdot 11 + 3 = 47$, и т. д. Согласитесь, этот процесс гораздо быстрее и приятнее раскручивания многоэтажных дробей. Ответ:

$$\delta_0 = \infty; \quad \delta_1 = 2; \quad \delta_2 = 3; \quad \delta_3 = \frac{11}{4} = 2,75;$$
$$\delta_4 = \frac{47}{17} \approx 2,764\ldots; \quad \delta_5 = \frac{105}{38} \approx 2,76315\ldots$$

— на пятом шаге (считая с нуля) подходящие дроби подошли к самому числу, прыгая вокруг него. Я имею ввиду то, что дроби с четными номерами больше исходного числа, а дроби с нечетными номерами — меньше, и последовательность подходящих дробей очень быстро сходится к самому числу. Это, конечно, не случайно, но об этих свойствах как раз чуть ниже и в следующем пункте.

Я хотел было закончить здесь п. 8, но человек — существо ужасно любопытное. Если он идет мимо забора за которым что-то попискивает, то он обязательно заглянет в щелочку, чтобы узнать, что это там пищит. Вот и сейчас любопытство взяло верх, и мне страшно хочется посчитать подходящие дроби разложения $\sqrt{2}$ в цепную дробь из примера 1 предыдущего пункта. Не буду себя сдерживать и составлю таблицу:

s	0	1	2	3	4	5	6	7
q_s		2	1	2	2	2	2	2
P_s	1	1	3	7	17	41	99	239
Q_s	0	1	2	5	12	29	70	169

Уже на шестом шаге я получил дробь $\frac{99}{70} = 1,41428\ldots$, т. е. достиг точности, которую помнят только влюбленные в математику человеки — $\sqrt{2} \approx 1,4142$; понадобилось же мне для этого две минуты и шесть секунд устных вычислений. Вот какой мощный аппарат — цепные дроби!

Задачки

1. Составляя таблицу, вычислите десяток подходящих дробей следующих цепных дробей и запишите их значения в виде десятичной дроби:

а) $\Phi = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\ddots}}}}}}$

(все неполные частные равны единице);

б) $e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{\ddots}}}}}}$

(последовательность неполных частных такова: 2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, 1, 1, 14, 1, 1, 16, 1,…); [1]

в) $\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \cfrac{1}{1 + \cfrac{1}{\ddots}}}}}}$

(последовательность неполных частных такова: 3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, 2, 2, 1, 84, 2, 1, 1, 15, 3, 13,…); [2]

2. Решите уравнение: $x = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\ddots \cfrac{\ddots}{1 + \cfrac{1}{x}}}}}$,

где справа в цепной дроби стоит n дробных черточек.

[1] Разложение в цепную дробь основания натуральных логарифмов впервые получил Эйлер, подметивший и доказавший закономерность в последовательности неполных частных.

[2] Для последовательности неполных частных разложения в цепную дробь числа π в настоящее время неизвестно никакой закономерности и никаких ее свойств, кроме того, что эта последовательность заведомо не периодическая (см. п. 11).

9. Свойства подходящих дробей

Это сложный пункт, в нем будет мало слов крупным шрифтом. Взгляните еще раз на название пункта, и «поехали» (цитата из литературного наследия Ю. Гагарина, точнее, это литературное наследие здесь процитировано полностью).

Свойство 1. $P_sQ_{s-1} - Q_sP_{s-1} = (-1)^s$, $s > 0$.

Доказательство. Обозначим $h_s = P_sQ_{s-1} - Q_sP_{s-1}$, тогда

$$h_1 = P_1Q_0 - Q_1P_0 = q_1 \cdot 0 - 1 \cdot 1 = -1,$$
$$h_s = P_sQ_{s-1} - Q_sP_{s-1} = (q_sP_{s-1} + P_{s-2})Q_{s-1} -$$
$$- (q_sQ_{s-1} + Q_{s-2})P_{s-1} = P_{s-2}Q_{s-1} - Q_{s-2}P_{s-1} = -h_{s-1}.$$

Значит, $h_s = (-1)^s$. ♦

Свойство 2. $\delta_s - \delta_{s-1} = \dfrac{(-1)^s}{Q_sQ_{s-1}}$, $s > 1$.

Доказательство.

$$\delta_s - \delta_{s-1} = \frac{P_s}{Q_s} - \frac{P_{s-1}}{Q_{s-1}} = \frac{h_s}{Q_sQ_{s-1}} = \frac{(-1)^s}{Q_sQ_{s-1}}.$$

♦

Свойство 3. *Для любого $s > 0$, дробь $\dfrac{P_s}{Q_s}$ — несократима.*

Доказательство. Пусть наибольший общий делитель (P_s, Q_s) равен d и $d > 1$. Тогда d делит разность $P_sQ_{s-1} - Q_sP_{s-1}$, равную $(-1)^s$, что невозможно. ♦

Свойство 4. $Q_s \geqslant \dfrac{1}{\sqrt{5}}\left[\left(\dfrac{1+\sqrt{5}}{2}\right)^s - \left(\dfrac{1-\sqrt{5}}{2}\right)^s\right]$, $s \geqslant 0$, *и равенство достигается только при $q_1 = q_2 = \ldots = q_s = 1$.*

Доказательство. Нам уже известно, что $Q_0 = 0$, $Q_1 = 1$, $q_i \in \mathbf{N}$, $Q_s = q_sQ_{s-1} + Q_{s-2} \geqslant Q_{s-1} + Q_{s-2}$. Наиболее медленный рост знаменателей будет наблюдаться при $Q_s = Q_{s-1} + Q_{s-2}$, т. е. при $q_1 = q_2 = \ldots = q_s = 1$. Это рекуррентное соотношение вместе с начальными условиями $Q_0 = 0$, $Q_1 = 1$ задает последовательность Фибоначчи. Характеристическое уравнение для рекуррентного соотношения Фибоначчи:

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

его корни: $x_{1,2} = \dfrac{1 \pm \sqrt{5}}{2}$; общее решение:

$$Q_s = C_1 \left(\frac{1+\sqrt{5}}{2}\right)^s + C_2 \left(\frac{1-\sqrt{5}}{2}\right)^s.$$

Подстановка начальных условий в общее решение дает

$$\begin{cases} 0 = C_1 + C_2 \\ 1 = C_1 \left(\dfrac{1+\sqrt{5}}{2}\right) + C_2 \left(\dfrac{1-\sqrt{5}}{2}\right) \end{cases}, \text{ откуда } C_1 = -C_2 = \frac{1}{\sqrt{5}}.$$

Впрочем, формула s-го члена последовательности Фибоначчи достаточно общеизвестна, ее вывод можно посмотреть, например, в брошюрах А. И. Маркушевича «Возвратные последовательности» или Н. Н. Воробьева «Числа Фибоначчи» из серии «Популярные лекции по математике», регулярно выходившей для школьников в издательстве «Наука».

Итак, знаменатели подходящих дробей растут не медленнее последовательности Фибоначчи: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55,... ♦

Отступление про Фибоначчи

Фибоначчи — «Сын Боначчо» или Леонардо Пизанский (1180–1240), — известный средневековый математик, философ, купец и т. д. Путешествовал и торговал в странах востока, изучал науку востока. По возвращению в Европу он записал собранные сведения, добавил много собственных исследований и издал книги «Практика геометрии» и «Книга абака». Последовательность Фибоначчи возникает у самого Леонардо при решении следующей задачи: сколько пар кроликов может произойти от одной пары в течении года, если а) каждая пара каждый месяц порождает новую пару, которая со второго месяца становится производителем, и б) кролики не дохнут. Поразительным образом, демонстрируя единство мироздания, последовательность Фибоначчи появляется не только при изучении цепных дробей, но и во многих других разделах математики, физики, биологии, искусствоведения. Кроме порождения на свет этой замечательной последовательности и другого прочего, «Книга абака» была одним из решающих источников проникновения в Западную Европу десятичной системы счисления и арабской записи цифр. Честь и хвала безумцам, которые, порой в ущерб своему благосостоянию, сохраняют и развивают культуру целых поколений, безумцам, чья система ценностей не замкнута на шмотках, деньгах и развлечениях!

Свойство 5. *Для любой бесконечной цепной дроби последовательность $\delta_1, \delta_2, \delta_3, \ldots$ сходится.*

Доказательство. Рассмотрим подпоследовательности

$$\frac{P_0}{Q_0}, \frac{P_2}{Q_2}, \ldots, \frac{P_{2n}}{Q_{2n}}, \ldots \quad \text{— дроби с четными номерами}$$

и

$$\frac{P_1}{Q_1}, \frac{P_3}{Q_3}, \ldots, \frac{P_{2n+1}}{Q_{2n+1}}, \ldots \quad \text{— дроби с нечетными номерами.}$$

Имеем

$$\frac{P_{2n+2}}{Q_{2n+2}} - \frac{P_{2n}}{Q_{2n}} = \delta_{2n+2} - \delta_{2n+1} + \delta_{2n+1} - \delta_{2n} = \\ = \frac{1}{Q_{2n+2}Q_{2n+1}} + \frac{-1}{Q_{2n+1}Q_{2n}} < 0,$$

так как $Q_{2n+2}Q_{2n+1} > Q_{2n+1}Q_{2n}$. Значит, подпоследовательность дробей с четными номерами монотонно убывает. Аналогично, вторая подпоследовательность монотонно возрастает. Всякий член «четной» последовательности больше всякого члена «нечетной». Действительно, рассмотрим δ_{2n} и δ_{2m+1}. Возьмем четное k такое, что $k+1 > 2n$ и $k+1 > 2m+1$. Тогда

$$\delta_k - \delta_{k-1} = +\frac{1}{Q_k Q_{k-1}} > 0, \quad \text{т. е. } \delta_k > \delta_{k-1}.$$

Но ведь $\delta_k < \delta_{2n}$ в силу убывания последовательности «четных», а $\delta_{k-1} > \delta_{2m+1}$ в силу возрастания последовательности «нечетных». Значит, $\delta_{2n} > \delta_k > \delta_{k-1} > \delta_{2m+1}$, что и нужно. Получается, что обе последовательности монотонны и ограничены, следовательно, имеют пределы. Кроме того,

$$|\delta_s - \delta_{s-1}| = \frac{1}{Q_s Q_{s-1}} < \frac{1}{\Phi_s \Phi_{s-1}} \underset{s\to\infty}{\longrightarrow} 0,$$

где Φ_s — s-й член последовательности Фибоначчи, следовательно, пределы обеих подпоследовательностей совпадают.

Итак, всякая бесконечная цепная дробь имеет некоторое значение. ♦

Свойство 6. *Пусть $\alpha \in \mathbf{R}$ раскладывается в цепную дробь, например, с помощью процесса взятия целых частей и «пе-*

реворачивания» дробных (этот процесс предложен в п. 7 после формулировки основной теоремы о цепных дробях), *т. е.*

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots \cfrac{}{q_s + \cfrac{1}{\alpha_{s+1}}}}}}$$

— результат очередного этапа процесса разложения. Тогда α *лежит между* δ_{s-1} *и* δ_s, *причем ближе к* δ_s, *чем к* δ_{s-1}.

Доказательство. На $(s+1)$-м шаге разложения мы заменяем q_s на $q_s + \dfrac{1}{\alpha_{s+1}}$, поэтому имеем точное равенство:

$$\alpha = \frac{\alpha_{s+1}P_s + P_{s-1}}{\alpha_{s+1}Q_s + Q_{s-1}},$$

значит,

$$\alpha\alpha_{s+1}Q_s + \alpha Q_{s-1} - \alpha_{s+1}P_s - P_{s-1} = 0.$$

Преобразуем его:

$$\alpha_{s+1}Q_s\left(\alpha - \frac{P_s}{Q_s}\right) + Q_{s-1}\left(\alpha - \frac{P_{s-1}}{Q_{s-1}}\right) = 0.$$

Это равенство означает, что разности в скобках имеют разные знаки. Кроме того, $Q_s > Q_{s-1}$, $\alpha_{s+1} > 1$, значит,

$$\left|\alpha - \frac{P_s}{Q_s}\right| < \left|\alpha - \frac{P_{s-1}}{Q_{s-1}}\right|. \qquad \blacklozenge$$

Свойство 7. *Для любого* $\alpha \in \mathbf{R}$, *разложение в цепную дробь единственно.*

Доказательство. Пусть имеются два разложения одного и того же числа:

$$p_1 + \cfrac{1}{p_2 + \cfrac{1}{p_3 + \cfrac{1}{\ddots}}} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots}}}.$$

Если два числа совпадают, то у них совпадают целые части, т. е. $p_1 = q_1$, и совпадают обратные величины к дробным частям:

$$p_2 + \cfrac{1}{p_3 + \cfrac{1}{\ddots}} = q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots}}.$$

Далее точно так же, по индукции. ♦

Наблюдательный читатель уже наверняка заметил, что основная теорема о цепных дробях (сформулированная в п. 7), о необходимости доказательства которой так долго говорили, к этому моменту оказалась доказанной. Более того, из вышеизложенного следует, что всякая цепная дробь (конечная или бесконечная) сходится именно к тому числу, которое было в нее разложено.

Задачки

1. Найдите формулу n-го члена последовательности, задаваемой рекуррентно: $a_n = a_{n-1} + 2a_{n-2}$; $a_1 = 0$, $a_2 = 6$.

2. Продвинутый десятиклассник Петя решает на школьной олимпиаде такую задачу:

Доказать, что при любом $n = 0, 1, 2, \ldots$, число

$$a_n = \frac{11 + \sqrt{10}}{10 + \sqrt{10}} \left(\frac{1 + \sqrt{10}}{2} \right)^n + \frac{-1}{10 + \sqrt{10}} \left(\frac{1 - \sqrt{10}}{2} \right)^n$$

является целым. Поскольку Петя знает только бином Ньютона, у него получаются очень громоздкие вычисления, в которых он тонет. Помогите Пете, не используя бином Ньютона.

3. Вычислите α с точностью до десятого знака после запятой, если:
а) $\alpha = \sqrt{2}$;
б) $\alpha = \sqrt{5}$.
Разрешается использовать только ваше умение оценивать разность между соседними подходящими дробями и калькулятор, умеющий выполнять сложение, умножение, вычитание и деление.

4. Вычислив последнюю и предпоследнюю подходящие дроби числа $\dfrac{215}{157}$, решите диофантовы уравнения:
а) $215x - 157y = 1$;
б) $215x - 157y = 4$.

10. Континуанты. Анализ алгоритма Евклида

В этом пункте я расскажу о вещах совсем малоизвестных, хотя абсолютно доступных для понимания. Сначала напомню забывчивым читателям рекуррентные соотношения для числителей и знаменателей подходящих дробей:

$$\begin{aligned} P_s &= q_s P_{s-1} + P_{s-2} \quad &&\text{— числители,} \\ Q_s &= q_s Q_{s-1} + Q_{s-2} \quad &&\text{— знаменатели.} \end{aligned}$$

Начальные условия: $P_1 = q_1$, $P_0 = 1$, $Q_1 = 1$, $Q_0 = 0$.

Теперь, когда эти соотношения стоят как живые у нас перед глазами в удобном месте, давайте рассмотрим не их, а трехдиагональный определитель:

$$\begin{vmatrix} q_1 & 1 & 0 & 0 & \dots & 0 & 0 \\ -1 & q_2 & 1 & 0 & \dots & 0 & 0 \\ 0 & -1 & q_3 & 1 & \dots & 0 & 0 \\ . & \vdots & . & . & . & \vdots & . \\ 0 & 0 & 0 & 0 & \dots & q_{n-1} & 1 \\ 0 & 0 & 0 & 0 & \dots & -1 & q_n \end{vmatrix} = (q_1 q_2 \cdot \ldots \cdot q_n).$$

Определение. Определитель [1]), обозначенный несколькими строками выше через $(q_1 q_2 \cdot \ldots \cdot q_n)$, называется *континуантой n-го порядка*. Числа $q_1, q_2, \ldots, q_n$ в дальнейшем будут у нас неполными частными из алгоритма Евклида, поэтому подразумеваются целыми.

Разложим континуанту n-го порядка по последнему столбцу (читатели наверняка натренировались делать это еще на первом курсе, когда вычисляли подобные определители из задачника Проскурякова по алгебре). Получим

$$(q_1 q_2 \cdot \ldots \cdot q_n) = q_n (q_1 q_2 \cdot \ldots \cdot q_{n-1}) + (q_1 q_2 \cdot \ldots \cdot q_{n-2}).$$

Получившееся соотношение очень напоминает рекуррентные соотношения для числителей и знаменателей подходящих дробей. Это не случайно и две следующие леммы только подтверждают нашу зародившуюся догадку о явной связи континуант и цепных дробей.

[1]) При устном рассказе, во избежание ненужной аллитерации «определение определителя», — детерминант.

Лемма 1. *Континуанта* $(q_1q_2\cdot\ldots\cdot q_n)$ *равна сумме всевозможных произведений элементов* $q_1, q_2, \ldots, q_n$, *одно из которых содержит все эти элементы, а другие получаются из него выбрасыванием одной или нескольких пар сомножителей с соседними номерами* (*если выбросили все сомножители, то считаем, что осталась* 1).

Поясняющий пример:

$$(q_1q_2q_3q_4q_5q_6) = q_1q_2q_3q_4q_5q_6 + q_3q_4q_5q_6 + q_1q_4q_5q_6 + q_1q_2q_5q_6 +$$
$$+ q_1q_2q_3q_6 + q_1q_2q_3q_4 + q_5q_6 + q_3q_6 + q_1q_6 + q_3q_4 + q_1q_4 + q_1q_2 + 1.$$

Доказательство леммы. База индукции

$$(q_1) = q_1,$$
$$(q_1q_2) = \begin{vmatrix} q_1 & 1 \\ -1 & q_2 \end{vmatrix} = q_1q_2 + 1,$$

и утверждение леммы справедливо для континуант первого и второго порядков.

Шаг индукции. Пусть утверждение леммы верно для континуант $(n-2)$-го и $(n-1)$-го порядков. Тогда имеем

$$(q_1q_2\cdot\ldots\cdot q_n) = q_n(q_1q_2\cdot\ldots\cdot q_{n-1}) + (q_1q_2\cdot\ldots\cdot q_{n-2})$$

и просто внимательное разглядывание этого равенства в сочетании с мысленным прикидыванием, какие произведения получатся от умножения континуанты $(q_1q_2\cdot\ldots\cdot q_{n-1})$ на q_n, доказывает требуемое. ♦

Наблюдение. Количество слагаемых в континуанте n-го порядка есть сумма числа слагаемых в континуантах $(n-1)$-го и $(n-2)$-го порядков, т. е. континуанта $(q_1q_2\cdot\ldots\cdot q_n)$ содержит Φ_{n+1} слагаемых, где $\Phi_{n+1} - (n+1)$-е число Фибоначчи.

Лемма 2.

$$q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots \cfrac{\ddots}{+\cfrac{1}{q_n}}}}} = \frac{(q_1q_2\cdot\ldots\cdot q_n)}{(q_2q_3\cdot\ldots\cdot q_n)}.$$

Доказательство. База индукции:

$$q_1 + \frac{1}{q_2} = \frac{q_1 q_2 + 1}{q_2} = \frac{(q_1 q_2)}{(q_2)} \quad \text{— верно.}$$

Шаг индукции. Пусть верно, что

$$q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots \cfrac{\ddots}{+\cfrac{1}{q_{n-1}}}}}} = \frac{(q_1 q_2 \cdot \ldots \cdot q_{n-1})}{(q_2 q_3 \cdot \ldots \cdot q_{n-1})}.$$

Тогда следующая дробь получается из предыдущей подстановкой вместо q_{n-1} выражения $q_{n-1} + \dfrac{1}{q_n}$:

$$q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots \cfrac{\ddots}{+\cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}} = \frac{\left(q_1 q_2 \cdot \ldots \cdot \left(q_{n-1} + \dfrac{1}{q_n}\right)\right)}{\left(q_2 q_3 \cdot \ldots \cdot \left(q_{n-1} + \dfrac{1}{q_n}\right)\right)} =$$

$$= \frac{\left(q_{n-1} + \dfrac{1}{q_n}\right)(q_1 q_2 \cdot \ldots \cdot q_{n-2}) + (q_1 q_2 \cdot \ldots \cdot q_{n-3})}{\left(q_{n-1} + \dfrac{1}{q_n}\right)(q_2 q_3 \cdot \ldots \cdot q_{n-2}) + (q_2 q_3 \cdot \ldots \cdot q_{n-3})} =$$

$$= \frac{(q_1 q_2 \cdot \ldots \cdot q_{n-1}) + \dfrac{1}{q_n}(q_1 q_2 \cdot \ldots \cdot q_{n-2})}{(q_2 q_3 \cdot \ldots \cdot q_{n-1}) + \dfrac{1}{q_n}(q_2 q_3 \cdot \ldots \cdot q_{n-2})} = \frac{(q_1 q_2 \cdot \ldots \cdot q_n)}{(q_2 q_3 \cdot \ldots \cdot q_n)}. \qquad \blacklozenge$$

Утверждение леммы 2, устанавливающее прямую связь континуант с цепными дробями, впервые заметил Леонард Эйлер. Этот гениальный математик еще много что заметил, но, боюсь, полный рассказ о его математических достижениях не уместится в эту книжку даже самым мелким шрифтом. Мы отложим должное небольшое историческое отступление про Эйлера до п. 18, где будет рассказана теорема, носящая его имя.

Приступим теперь к исполнению второй части названия этого пункта — анализу алгоритма Евклида. Нас будет интересовать наихудший случай — когда алгоритм работает особенно долго? Спросим точнее: какие два наименьших числа надо засунуть в алгоритм Евклида, чтобы он работал в точности заданное число шагов? Ответ на этот вопрос дает

Теорема (Ламэ, 1845 г.). *Пусть $n \in \mathbf{N}$ и пусть $a > b > 0$ такие, что алгоритму Евклида для обработки a и b необходимо выполнить точно n шагов* (*делений с остатком*), *причем a — наименьшее с таким свойством. Тогда $a = \Phi_{n+2}$, $b = \Phi_{n+1}$, где Φ_k — k-е число Фибоначчи.*

Доказательство. Разложим $\dfrac{a}{b}$ в цепную дробь:

$$\frac{a}{b} = \frac{(q_1 q_2 \cdot \ldots \cdot q_n)}{(q_2 q_3 \cdot \ldots \cdot q_n)},$$

где $q_1, q_2, \ldots, q_n$ — неполные частные из алгоритма Евклида; по условию теоремы, их точно n штук. Согласно свойству 3 п. 9, континуанты $(q_1 q_2 \cdot \ldots \cdot q_n)$ и $(q_2 q_3 \cdot \ldots \cdot q_n)$ взаимно просты, значит, если $(a, b) = d$ — наибольший общий делитель, то

$$\begin{cases} a = (q_1 q_2 \cdot \ldots \cdot q_n) d \\ b = (q_2 q_3 \cdot \ldots \cdot q_n) d \end{cases} \qquad (\spadesuit)$$

Заметим, что по смыслу конечной цепной дроби, $q_n \geqslant 2$, а $q_1, q_2, \ldots, q_{n-1}$, $d \geqslant 1$.

Поскольку континуанта суть многочлен с неотрицательными коэффициентами от всех этих переменных, минимальное значение достигается при $q_1 = q_2 = \ldots = q_{n-1} = d = 1$, $q_n = 2$. Подставляя эти значения в ($\spadesuit$), получим $a = \Phi_{n+2}$, $b = \Phi_{n+1}$. ♦

Следствие. *Если натуральные числа a и b не превосходят $N \in \mathbf{N}$, то число шагов* (*операций деления с остатком*), *необходимых алгоритму Евклида для обработки a и b, не превышает*

$$\lceil \log_\Phi (\sqrt{5}\, N) \rceil - 2,$$

где $\lceil \alpha \rceil$ — верхнее целое α, $\Phi = \dfrac{1+\sqrt{5}}{2}$ — больший корень характеристического уравнения последовательности Фибоначчи (искусствоведы сказали бы: «золотое сечение»).

Доказательство. Максимальное число шагов n достигается при $a = \Phi_{n+2}$, $b = \Phi_{n+1}$, где n — наибольший номер такой, что

$\Phi_{n+2} < N$. Рассматривая формулу для n-го члена последовательности Фибоначчи (смотри, например, доказательство свойства 4 в п. 9), легко понять, что Φ_{n+2} — ближайшее целое к $\frac{1}{\sqrt{5}}\Phi^{n+2}$. Значит, $\frac{1}{\sqrt{5}}\Phi^{n+2} < N$, следовательно, $n+2 < \log_\Phi(\sqrt{5}\,N)$, откуда моментально

$$n < \lceil \log_\Phi(\sqrt{5}\,N) \rceil - 3$$

(именно «минус три», ведь рассматривается верхнее целое, т. е. кажется, утверждение следствия можно усилить). ♦

Для еще не купивших калькулятор сообщу, что $\log_\Phi(\sqrt{5}\,N) \approx \approx 4{,}785 \cdot \lg N + 1{,}672$, поэтому, например, с любой парой чисел, меньших миллиона, алгоритм Евклида разбирается не более, чем за $\lceil 4{,}785 \cdot 6 + 1{,}672 \rceil - 3 = 31 - 3 = 28$ шагов.

Ну вот, используя теорему Ламэ, мы провели некоторый анализ быстродействия алгоритма Евклида и узнали наихудший случай для него — два последовательных числа Фибоначчи. Таким образом, давно висевшая перед нами проблема об эффективности древнегреческого наследия решена полностью. На этом пункт и закончим.

Задачки

1. Вычислите континуанты:
а) (1, 2, 3, 4, 5);
б) (1, 1, 1, 1, 1, 1);
в) (1, –1, 1, –1, 1).

2. (№ 301 из задачника Проскурякова). Методом рекуррентных соотношений вычислить определитель

$$\begin{vmatrix} 7 & 5 & 0 & 0 & \cdots & 0 & 0 \\ 2 & 7 & 5 & 0 & \cdots & 0 & 0 \\ 0 & 2 & 7 & 5 & \cdots & 0 & 0 \\ 0 & 0 & 2 & 7 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 7 & 5 \\ 0 & 0 & 0 & 0 & \cdots & 2 & 7 \end{vmatrix}.$$

3. Потрудитесь и разложите на сумму произведений континуанту $(q_1q_2q_3q_4q_5q_6q_7)$. Сколько получилось слагаемых?

4. Найдите все перестановки σ множества $\{1, 2, \ldots, n\}$ такие, что $(q_1q_2 \cdot \ldots \cdot q_n) = (q_{\sigma(1)}q_{\sigma(2)} \cdot \ldots \cdot q_{\sigma(n)})$ для любых чисел $q_1, q_2, \ldots, q_n$.

5. Найдите произведение матриц

$$\begin{pmatrix} x_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x_2 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} x_n & 1 \\ 1 & 0 \end{pmatrix}.$$

6. Пусть α — иррациональное число и его разложение в цепную дробь суть:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots \cfrac{}{a_n + \cfrac{1}{\ddots}}}}}}.$$

Докажите, что тогда

$$\frac{1}{\alpha} = b_0 + \cfrac{1}{b_1 + \cfrac{1}{\ddots \cfrac{}{b_m + \cfrac{1}{a_5 + \cfrac{1}{a_6 + \cfrac{1}{a_7 + \cfrac{1}{\ddots}}}}}}}$$

для соответствующих целых $b_0, b_1, \ldots, b_m$. (Рассмотрите отдельно случаи $\alpha > 0$ и $\alpha < 0$.) Объясните, как выражаются все $b_0, b_1, \ldots, b_m$ через a_0, a_1, a_2, a_3, a_4.

7. Каково наибольшее число шагов, необходимых алгоритму Евклида для обработки двух чисел, меньших миллиарда?

11. Еще кое-что о цепных дробях (приближение чисел, периодичность, теорема Эрмита)

В этом пункте я хочу рассказать кое-что еще о свойствах цепных дробей, что не уложилось в схему рассказа предыдущих четырех пунктов. Прежде всего, это следующая замечательная теорема, показывающая, что среди всех рациональных дробей

с ограниченным по величине знаменателем, наилучшим образом приближает произвольное число именно его подходящая дробь.

Теорема. *Пусть α — произвольное число, $s > 1$, а если при этом $\alpha = \dfrac{a}{b}$ — несократима, то $s < n$, где n таково, что $Q_n = b$. Тогда неравенство $\left|\alpha - \dfrac{c}{d}\right| < |\alpha - \delta_s|$ возможно только если у несократимой дроби $\dfrac{c}{d}$ знаменатель больше Q_s.*

Доказательство. Мы знаем, что α всегда лежит между соседними подходящими дробями, поэтому всегда $\left|\dfrac{c}{d} - \delta_{s+1}\right| < |\delta_s - \delta_{s+1}|$. Это неравенство проиллюстрировано рис. 4, разглядывая который, нужно помнить, что $\left|\alpha - \dfrac{c}{d}\right| < |\alpha - \delta_s|$ (тогда иллюстрируемое неравенство становится очевидным, даже если $\dfrac{c}{d} < \delta_{s+1}$).

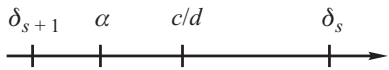


Рис. 1

Из проиллюстрированного неравенства следует, что

$$\left|\frac{c}{d} - \frac{P_{s+1}}{Q_{s+1}}\right| < \frac{1}{Q_s Q_{s+1}}$$

и, если $\dfrac{c}{d} \neq \delta_{s+1}$, то

$$\left|\frac{c}{d} - \frac{P_{s+1}}{Q_{s+1}}\right| = \left|\frac{cQ_{s+1} - P_{s+1}d}{dQ_{s+1}}\right| \geqslant \frac{1}{dQ_{s+1}}.$$

Следовательно, $\dfrac{1}{dQ_{s+1}} < \dfrac{1}{Q_s Q_{s+1}}$ и, значит, $d > Q_s$, что и требовалось. Если же $\dfrac{c}{d} = \delta_{s+1}$, то $d = Q_{s+1} > Q_s$. ♦

Итак, подходящая дробь — наилучшее приближение данного числа среди всех дробей, знаменатели которых не превосходят знаменатель подходящей дроби. Здесь мы вплотную подошли к вопросу о приближении произвольных чисел рациональными дробями. Оказывается, что это очень интересная теория, имеющая далеко идущие следствия. Остановимся, однако, здесь до лучших времен наступления § 5 «Трансцендентные числа», где мы снова столкнемся с приближением действительных чисел при

изучении их алгебраических свойств. Есть время разбрасывать камни, есть время их собирать.

Обратим теперь наше внимание на внешний вид цепных дробей. Внешний вид математического объекта может многое поведать о внутренних свойствах. Мы знаем, например, что любая периодическая десятичная дробь (периодичность — это «внешний вид») обязательно представляет собой некоторое рациональное число (рациональность — это «внутреннее свойство») и наоборот. Попытаемся взглянуть с подобной точки зрения на цепные дроби и зададимся вопросом — какие числа представимы в виде периодической цепной дроби?

Определение. Бесконечная цепная дробь

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cfrac{1}{\ddots \cfrac{}{q_n + \cfrac{1}{\ddots}}}}}}$$

называется *периодической*, если для последовательности $q_1, q_2, \ldots, q_n, \ldots$ ее неполных частных найдутся такие натуральные k_0 и h, что для любого $k \geqslant k_0$ выполнено $q_{k+h} = q_k$, т. е. последовательность неполных частных, начиная с некоторого места k_0 периодическая.

Определение. Иррациональное число, являющееся корнем некоторого квадратного уравнения с целыми коэффициентами, называется *квадратичной иррациональностью*.

Примеры квадратичных иррациональностей: $\sqrt{2}$, $9\sqrt{7} - 4$, $\dfrac{5+\sqrt{21}}{8}$, $\dfrac{1+\sqrt{15}}{6-2\sqrt{7}}$. Примеры не квадратичных иррациональностей: $\sqrt[5]{2}$, $\sqrt[3]{5} + 17$, числа π, e и многие другие (пояснения к подобным примерам не квадратичных иррациональностей будут даны в § 5 «Трансцендентные числа»).

Теорема (Лагранж). *Квадратичные иррациональности и только они представимы в виде бесконечной периодической цепной дроби.*

Доказательство. Пусть

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cfrac{1}{\ddots \cfrac{1}{q_n + \cfrac{1}{\ddots}}}}}}$$

— периодическая цепная дробь. Назовем число

$$r_n = q_n + \cfrac{1}{q_{n+1} + \cfrac{1}{q_{n+2} + \cfrac{1}{\ddots}}}$$

остатком цепной дроби α. Таким образом, остаток r_n цепной дроби α — это весь ее «хвост» вниз и вправо, начиная с n-го этажа. Ясно, что

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots \cfrac{1}{q_{n-1} + \cfrac{1}{r_n}}}}.$$

Остатки периодической цепной дроби, очевидно, удовлетворяют соотношению: $r_{k+h} = r_k$, где $k \geqslant k_0$, h — период последовательности неполных частных. Это означает (вспоминаем свойства подходящих дробей), что

$$\alpha = \frac{P_{k-1}r_k + P_{k-2}}{Q_{k-1}r_k + Q_{k-2}} = \frac{P_{k+h-1}r_{k+h} + P_{k+h-2}}{Q_{k+h-1}r_{k+h} + Q_{k+h-2}} = \\ = \frac{P_{k+h-1}r_k + P_{k+h-2}}{Q_{k+h-1}r_k + Q_{k+h-2}},$$

откуда

$$\frac{P_{k-1}r_k + P_{k-2}}{Q_{k-1}r_k + Q_{k-2}} = \frac{P_{k+h-1}r_k + P_{k+h-2}}{Q_{k+h-1}r_k + Q_{k+h-2}}$$

— квадратное уравнение с целыми коэффициентами для нахождения r_k. Значит, r_k — квадратичная иррациональность, следовательно, $\alpha = \dfrac{P_{k-1}r_k + P_{k-2}}{Q_{k-1}r_k + Q_{k-2}}$ — тоже квадратичная иррациональность.

Обратное утверждение теоремы доказывается чуть-чуть сложнее. Пусть α удовлетворяет квадратному уравнению с целыми коэффициентами:

$$a\alpha^2 + b\alpha + c = 0. \tag{1}$$

Разложим α в цепную дробь и подставим в уравнение (1) вместо α его выражение $\alpha = \dfrac{P_{n-1}r_n + P_{n-2}}{Q_{n-1}r_n + Q_{n-2}}$ через некоторый остаток r_n цепной дроби. После преобразований снова получается квадратное уравнение

$$A_n r_n^2 + B_n r_n + C_n = 0, \tag{2}$$

где

$$\begin{cases} A_n = aP_{n-1}^2 + bP_{n-1}Q_{n-1} + cQ_{n-1}^2, \\ B_n = 2aP_{n-1}P_{n-2} + b(P_{n-1}Q_{n-2} + P_{n-2}Q_{n-1}) + 2cQ_{n-1}Q_{n-2}, \\ C_n = aP_{n-2}^2 + bP_{n-2}Q_{n-2} + cQ_{n-2}^2 \end{cases}$$

— суть целые числа. Видно, что $C_n = A_{n-1}$. Кроме того, дискриминанты квадратных уравнений (1) и (2) совпадают при всех n:

$$B_n^2 - 4A_nC_n = (b^2 - 4ac)\underbrace{(P_{n-1}Q_{n-2} + P_{n-2}Q_{n-1})^2}_{(-1)^{2n}} = b^2 - 4ac.$$

Так как (по свойствам подходящих дробей)

$$\left|\alpha - \frac{P_{n-1}}{Q_{n-1}}\right| < \frac{1}{Q_{n-1}^2},$$

то $P_{n-1} = \alpha Q_{n-1} + \dfrac{\varepsilon_{n-1}}{Q_{n-1}}$, где ε_{n-1} — некоторое подходящее число такое, что $|\varepsilon_{n-1}| < 1$. Теперь, набравшись терпения, посчитаем коэффициент A_n в квадратном уравнении (2):

$$\begin{aligned} A_n &= aP_{n-1}^2 + bP_{n-1}Q_{n-1} + c\,Q_{n-1}^2 = \\ &= a\left(\alpha Q_{n-1} + \frac{\varepsilon_{n-1}}{Q_{n-1}}\right)^2 + b\left(\alpha Q_{n-1} + \frac{\varepsilon_{n-1}}{Q_{n-1}}\right)Q_{n-1} + cQ_{n-1}^2 = \end{aligned}$$

$$= \underbrace{(a\alpha^2 + b\alpha + c)}_{0} Q_{n-1}^2 + 2a\alpha\varepsilon_{n-1} + a\frac{\varepsilon_{n-1}^2}{Q_{n-1}^2} + b\varepsilon_{n-1} =$$

$$= 2a\alpha\varepsilon_{n-1} + a\frac{\varepsilon_{n-1}^2}{Q_{n-1}^2} + b\varepsilon_{n-1}.$$

Значит, для любого натурального n

$$|A_n| = \left|2a\alpha\varepsilon_{n-1} + a\frac{\varepsilon_{n-1}^2}{Q_{n-1}^2} + b\varepsilon_{n-1}\right| < 2\,|a\alpha| + |a| + |b|\,,$$

$$|C_n| = |A_{n-1}| < 2\,|a\alpha| + |a| + |b|\,.$$

Таким образом, целые коэффициенты A_n и C_n уравнения (2) ограничены по абсолютной величине и, следовательно, при изменении n могут принимать лишь конечное число различных значений. Так как дискриминанты уравнений (1) и (2) совпадают, то и коэффициент B_n может принимать лишь конечное число различных значений. Значит, при изменении n от 1 до ∞, мы повстречаем лишь конечное число различных уравнений вида (2), т. е. лишь конечное число различных остатков r_n. Это значит, что некоторые два остатка r_n и r_{n+h} с разными номерами обязательно совпадают, что и означает периодичность цепной дроби. ♦

Итак, квадратичные иррациональности и только они представляются периодическими цепными дробями. «Внешний вид» цепных дробей, представляющих иррациональности других типов, в настоящее время науке неизвестен (за очень редкими исключениями), и, по видимому, описание этого внешнего вида является очень сложным вопросом. Некоторые дополнительные замечания о внешнем виде цепных дробей содержатся в п. 25.

Я хочу закончить весь этот параграф о цепных дробях демонстрацией их применения в изящном и элегантном теоретико-числовом рассуждении, принадлежащем Ш. Эрмиту (1822–1901). Этот эффектный результат представляет собой типичный пример в достаточной степени бесполезного, с точки зрения народного хозяйства, математического утверждения.

Теорема. *Всякий делитель числа* $a^2 + 1$, *где* $a \in \mathbf{Z}$, *представим в виде суммы двух квадратов.*

Доказательство. Пусть $d \mid (a^2 + 1)$. Значит, d не делит a. Разложим a/d в цепную дробь. Знаменатели ее подходящих дробей

образуют возрастающую цепочку: $1 = Q_1 < Q_2 < \ldots < Q_n = d$. Значит, найдется такой номер $k \in \mathbf{N}$, что

$$Q_k \leqslant \sqrt{d} \leqslant Q_{k+1} \qquad (\spadesuit)$$

и хоть одно из этих неравенств — строгое. Далее, a/d лежит между соседними подходящими дробями, значит,

$$\left|\frac{a}{d} - \frac{P_k}{Q_k}\right| \leqslant \left|\frac{P_{k+1}}{Q_{k+1}} - \frac{P_k}{Q_k}\right| = \frac{1}{Q_k Q_{k+1}},$$

т. е. $\left|\dfrac{a}{d} - \dfrac{P_k}{Q_k}\right| = \dfrac{\varepsilon}{Q_k Q_{k+1}}$, где $\varepsilon \leqslant 1$. Приведем разность внутри модуля к общему знаменателю: $\left|\dfrac{aQ_k - dP_k}{dQ_k}\right| = \dfrac{\varepsilon}{Q_k Q_{k+1}}$. Имеем

$$|aQ_k - dP_k| = \frac{d}{Q_{k+1}}\varepsilon \leqslant \frac{d}{\sqrt{d}}\varepsilon = \sqrt{d}\,\varepsilon \leqslant \sqrt{d}$$

(здесь первое неравенство следует из (♠)), значит, $(aQ_k - dP_k)^2 \leqslant d$. Кроме того, из другого неравенства в (♠) следует $Q_k^2 \leqslant d$ и хоть одно из двух последних написанных неравенств строгое. Сложив их, получим строгое неравенство:

$$(aQ_k - dP_k)^2 + Q_k^2 < 2d,$$

т. е.

$$\bigl(a^2 + 1\bigr)Q_k^2 - 2adQ_kP_k + d^2P_k^2 < 2d.$$

Слева стоит сумма двух квадратов — целое положительное число (строго больше нуля) и каждое из трех слагаемых слева делится на d. Получается, что левая часть делится на d и строго меньше $2d$, т. е. левая часть есть само число d, и

$$(aQ_k - dP_k)^2 + Q_k^2 = d$$

— сумма двух квадратов. ♦

Финиш одиннадцатого пункта и всего второго параграфа.

Задачки

1. Найдите наилучшее рациональное приближение к числу $\dfrac{971}{773}$ со знаменателем, не превышающим 82, и оцените погрешность приближения.

2. Среди всех рациональных дробей со знаменателем, не превосходящим 72, найдите ближайшую к числу $2 + \sqrt{5}$. Оцените погрешность.

3. Вычислите значение периодической цепной дроби α и напишите квадратное уравнение с целыми коэффициентами, корнем которого она является, если

а)

$$\alpha = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}}}};$$

б)

$$\alpha = 7 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}}}}}}.$$

4. Представить число 761 в виде суммы двух квадратов. (Подсказка: $761 \cdot 2 = 39^2 + 1$.)

§ 3. ВАЖНЕЙШИЕ ФУНКЦИИ В ТЕОРИИ ЧИСЕЛ

Введение в математику переменных величин и функционального мышления во времена Ньютона коренным образом преобразило все естественные науки и расширило область их применения, изменив сам стиль исследовательской деятельности. Не избежала этой участи и теория чисел, в которой функциональный взгляд на многие числовые явления позволяет легко и быстро получать красивые и полезные утверждения. Знакомством с важнейшими функциями, занятыми в спектакле «Теория чисел» на главных ролях, с их работой, чаяниями и нуждами, мы займемся в этом параграфе.

Название этого параграфа и названия первых трех его пунктов взяты мной из классической книжки И. М. Виноградова «Основы теории чисел», ибо зачем придумывать самому уже давно и хорошо придуманное? Содержание же этих пунктов получилось гораздо обширнее, чем в вышеупомянутой книжке, поэтому работа предстоит тяжелая. Приступим.

12. Целая и дробная часть

Определение. Пусть $x \in \mathbf{R}$ — действительное число. *Целой частью* $[x]$ числа x называется его нижнее целое, т. е. наибольшее целое, не превосходящее x; *дробной частью* $\{x\}$ числа x называется число $\{x\} = x - [x]$.

Примеры. $[2,81] = 2$; $\{2,81\} = 0{,}81$; $[-0,2] = -1$; $\{-0,2\} = 0,8$.

Отметим, что эти две функции известны каждому со школьной скамьи; что целая часть — неубывающая функция; что дробная часть — периодическая с периодом 1 функция; что дробная часть всегда неотрицательна, но меньше единицы; что обе эти функции разрывны при целых значениях x, но непрерывны при этих x справа. Посмотрим на их дальнейшие применения, порой изящные и неочевидные.

Лемма 1. *Показатель, с которым простое число p входит в разложение $n!$, равен $\alpha = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$.*

Доказательство. Очевидно, ряд $\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$ обрывается на том месте k, на котором p^k превзойдет n. Имеем

$$n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot p \cdot \ldots \cdot p^2 \ldots \cdot p^3 \ldots \cdot (n-1) \cdot n.$$

Число сомножителей, кратных p, равно $\left[\frac{n}{p}\right]$. Среди них, кратных p^2 содержится $\left[\frac{n}{p^2}\right]$; кратных p^3 имеется $\left[\frac{n}{p^3}\right]$ и т. д. Сумма α и дает искомый результат, так как всякий сомножитель, кратный p^m, но не кратный p^{m+1}, сосчитан в ней точно m раз: как кратный p, как кратный p^2, как кратный p^3, ..., как кратный p^m. ♦

Пример. Показатель, с которым 5 входит в 643! равен

$$\left[\frac{643}{5}\right] + \left[\frac{643}{25}\right] + \left[\frac{643}{125}\right] + \left[\frac{643}{625}\right] = 128 + 25 + 5 + 1 = 159.$$

Определение. Точка координатной плоскости называется *целой*, если обе ее координаты — целые числа.

Лемма 2. *Пусть функция $f(x)$ непрерывна и неотрицательна на отрезке $[a, b]$. Тогда число целых точек в области $\mathbf{D} = \{a < x \leqslant b, 0 < y \leqslant f(x)\}$ равно $\sum\limits_{\substack{a<x\leqslant b \\ x\in \mathrm{Z}}} [f(x)]$.*

Доказательство. На вертикальной прямой с целой абсциссой x в области $\mathbf{D}$ лежит $[f(x)]$ целых точек. ♦

Еще одно забавное утверждение про целые точки относится к области комбинаторной геометрии.

Лемма 3. *Пусть M — многоугольник на координатной плоскости с вершинами в целых точках, контур M сам себя не пересекает и не касается, S — площадь этого многоугольника, $T = \left(\sum\limits_A \delta_A\right) - 1$, где суммирование ведется по всем целым точкам A, лежащим внутри и на границе этого многоугольника, причем $\delta_A = 1$, если точка A лежит внутри M, и $\delta_A = \frac{1}{2}$, если точка A лежит на границе M. Тогда $T = S$.*

Доказательство этой леммы я здесь приводить не буду, так как эта лемма, вообще говоря, не относится к теории чисел. Намечу только схему этого доказательства.

1) Для треугольника с вершинами в целых точках и без целых точек внутри утверждение очевидно.

2) Для выпуклого многоугольника: фиксируем одну из его вершин и соединяем ее прямыми с остальными вершинами — попадаем в случай треугольников.

3) Случай невыпуклого многоугольника рассматриваем как разность выпуклых многоугольников. ♦

Что это я все время о целых частях, да о целых частях? Приведу замечательное утверждение о дробных частях, принадлежащее Лежену Дирихле (1805–1859).

Теорема. *Для любого* $\alpha \in \mathbf{R}$ *число* 0 *является предельной точкой последовательности* $x_n = \{\alpha \cdot n\}$.

Доказательство. Возьмем любое натуральное t и покажем, что неравенство $\left|\alpha - \dfrac{p}{q}\right| < \dfrac{1}{qt}$ обязательно имеет решение в целых числах p и q, где $q \geqslant 1$. Пусть $0 = \{\alpha \cdot 0\}\, \{\alpha \cdot 1\}, \{\alpha \cdot 2\}, \ldots, \{\alpha \times \times (t-1)\}, \{\alpha \cdot t\}$ — $(t+1)$ штук чисел. Все они из отрезка $[0, 1]$. Разделим этот отрезок на t равных частей шагом $\dfrac{1}{t}$. По принципу Дирихле (именно для доказательства этой теоремы Дирихле и придумал свой знаменитый «принцип Дирихле» про t клеток и $(t+1)$ кролика, которым негде сидеть) в одной из частей отрезка лежат два числа: $\{\alpha \cdot k_1\}$ и $\{\alpha \cdot k_2\}$, где $k_2 > k_1$. Имеем

$$|\{\alpha k_1\} - \{\alpha k_2\}| = |\alpha(k_2 - k_1) - ([\alpha k_2] - [\alpha k_1])| < \frac{1}{t}.$$

Положим $k_2 - k_1 = q$, $[\alpha \cdot k_2] - [\alpha \cdot k_1] = p$, ясно, что $q \leqslant t$. Тогда будем иметь

$$|\alpha q - p| < \frac{1}{t}, \quad 0 < q \leqslant t$$

Это означает, что $\dfrac{p}{q}$ — решение неравенства $\left|\alpha - \dfrac{p}{q}\right| < \dfrac{1}{qt}$.

Устремим t к бесконечности. Получим, что αq отлично от целого числа p менее, чем на $\dfrac{1}{t}$, а $\dfrac{1}{t} \underset{t\to\infty}{\longrightarrow} 0$. Следовательно, либо 0, либо число 1 — предельная точка последовательности $x_n = \{\alpha \cdot n\}$. Если число 0 — предельная точка, то все доказано. Если же предельная точка — число 1, то тогда для любого $\varepsilon > 0$

найдется член x последовательности x_n такой, что $x > 1 - \varepsilon$. Пусть $x = 1 - \delta$. Тогда $2x = 2 - 2\delta$, а $\{2x\}$ (очевидно, что $\{2x\}$ — тоже член последовательности x_n) не дотягивает до 1 уже на 2δ; число $\{3x\}$ меньше 1 уже на 3δ, и т. д. Следовательно, можно подобрать такое натуральное k, что член $\{kx\}$ будет меньше единицы на $k\delta$ и попадет в ε-окрестность нуля. Это означает, что число 0 также является предельной точкой последовательности x_n, а именно это и требовалось. ♦

Очевидно, что если $\alpha = \dfrac{p}{q}$ — рациональное число, где $(p, q) = 1$, то последовательность $x_n = \{\alpha \cdot n\}$ является периодической с периодом q и ее членами являются только числа $0, \dfrac{1}{q}, \dfrac{2}{q}, \ldots, \dfrac{q-1}{q}$. Несколько модернизировав рассуждения из доказательства предыдущей теоремы, можно обосновать любопытное следствие, так же принадлежащее перу Дирихле.

Следствие. *Если число $\alpha \in \mathbf{R}$ иррационально, то члены последовательности $x_n = \{\alpha \cdot n\}$ всюду плотно заполняют отрезок $[0, 1]$.*

Попытайтесь доказать это следствие самостоятельно, а я на этом пункт 12 заканчиваю.

Задачки

1. Постройте графики функций:
а) $y = [x]$; б) $y = \{x\}$; в) $y = [x^2]$; г) $y = \{x^2\}$.
Особое внимание уделите плавности линий, проработке отдельных элементов композиции, грамотной прорисовке точек разрыва.

2. Аккуратно докажите следующие свойства целой части:
а) $[x + y] \geqslant [x] + [y]$; б) $\left[\dfrac{[x]}{n}\right] = \left[\dfrac{x}{n}\right]$, где $n \in \mathbf{N}$;
в) $\left[x + \dfrac{1}{2}\right] = [2x] - [x]$;
г) $[x] + \left[x + \dfrac{1}{n}\right] + \left[x + \dfrac{2}{n}\right] + \ldots + \left[x + \dfrac{n-1}{n}\right] = [nx]$, где $n \in \mathbf{N}$.

3. Разложите на простые множители число 100!

4. Решите уравнение: $x^3 - [x] = 3$.

5. Докажите, что при любых $a \neq 0$ и b уравнение
$$[x] + a\{x\} = b$$
имеет $[|a|]$ или $[|a|] + 1$ решений.

6. Для каждого натурального n определите, сколько решений имеет уравнение $x^2 - [x^2] = \{x\}^2$ на отрезке $[1; n]$.

7. Найдите предел: $\lim\limits_{n\to\infty} \{(2+\sqrt{3}\,)^n\}$.

8. Докажите, что для любого натурального n имеет место оценка: $\{n\sqrt{2}\,\} > \dfrac{1}{2n\sqrt{2}}$, однако для любого $\varepsilon > 0$ найдется натуральное n, удовлетворяющее неравенству

$$\{n\sqrt{2}\,\} < \frac{1+\varepsilon}{2n\sqrt{2}}.$$

9. Сколько целых точек лежит в области между осью абсцисс и параболой $y = -x^2 + 30$?

10. Найдите площадь многоугольника, который получится, если последовательно соединить отрезками точки $A(0,0)$, $B(2,7)$, $C(4,2)$, $D(8,8)$, $E(10,0)$, $F(5,-5)$, $A(0,0)$.

11. Докажите, что для любого иррационального числа $\alpha \in \mathbf{R}$ неравенство

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$$

имеет бесконечное множество решений $(p, q) \in \mathbf{Z} \times \mathbf{N}$ и, следовательно, знаменатели q всех решений неограничены. [1)]

13. Мультипликативные функции

В этом пункте речь пойдет об одном важном классе функций, которому в теории чисел посвящены целые монографии (см., напр., книжку *Г. Дэвенпорта* «Мультипликативная теория чисел»).

Определение. Функция $\theta : \mathbf{R} \to \mathbf{R}$ (или, более общо, $\theta : \mathbf{C} \to \mathbf{C}$) называется *мультипликативной*, если:

1) функция θ определена всюду на $\mathbf{N}$ и существует $a \in \mathbf{N}$ такой, что $\theta(a) \neq 0$;

2) для любых взаимно простых натуральных чисел a_1 и a_2 выполняется $\theta(a_1 \cdot a_2) = \theta(a_1) \cdot \theta(a_2)$.

[1)] В теории приближения действительных чисел рациональными числами утверждение этой задачи звучит так: всякое иррациональное число допускает степенной порядок приближения $1/q^2$. Это — один из основополагающих фактов упомянутой теории.

Пример 1. $\theta(a) = a^s$, где s — любое (хоть действительное, хоть комплексное) число. Проверка аксиом 1) и 2) из определения мультипликативной функции не составляет труда, а сам пример показывает, что мультипликативных функций по меньшей мере континуум, т. е. много.

Перечислим, кое-где доказывая, некоторые свойства мультипликативных функций. Пусть всюду ниже $\theta(a)$ — произвольная мультипликативная функция.

Свойство 1. $\theta(1) = 1$.

Доказательство. Пусть a — то самое натуральное число, для которого $\theta(a) \neq 0$. Тогда $\theta(a \cdot 1) = \theta(a) \cdot \theta(1) = \theta(a)$. ♦

Свойство 2. $\theta(p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}) = \theta(p_1^{\alpha_1})\theta(p_2^{\alpha_2}) \cdot \ldots \cdot \theta(p_n^{\alpha_n})$, *где* $p_1, p_2, \ldots, p_n$ — *различные простые числа.*

Доказательство очевидно. ♦

Свойство 3. *Обратно, мы всегда построим некоторую мультипликативную функцию* $\theta(a)$, *если зададим* $\theta(1) = 1$ *и произвольно определим* $\theta(p^\alpha)$ *для всех простых* p *и всех натуральных* α, *а для остальных натуральных чисел доопределим функцию* $\theta(a)$, *используя равенство*

$$\theta(p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}) = \theta(p_1^{\alpha_1})\theta(p_2^{\alpha_2}) \cdot \ldots \cdot \theta(p_n^{\alpha_n}).$$

Доказательство сразу следует из основной теоремы арифметики. ♦

Пример 2. Пусть $\theta(1) = 1$ и $\theta(p^\alpha) = 2$ для всех p и α. Тогда, для произвольного числа, $\theta(p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}) = 2^n$.

Свойство 4. *Произведение нескольких мультипликативных функций является мультипликативной функцией.*

Доказательство. Сначала докажем для двух сомножителей. Пусть θ_1 и θ_2 — мультипликативные функции $\theta = \theta_1 \cdot \theta_2$, тогда (проверяем аксиомы определения)

1) $\theta(1) = \theta_1(1) \cdot \theta_2(1) = 1$ и, кроме того, существует такое a (это $a = 1$), что $\theta(a) \neq 0$;

2) пусть $(a, b) = 1$ — взаимно просты. Тогда

$$\theta(a \cdot b) = \theta_1(a \cdot b) \cdot \theta_2(a \cdot b) =$$

$$= \theta_1(a)\theta_1(b)\theta_2(a)\theta_2(b) = \theta_1(a)\theta_2(a) \cdot \theta_1(b)\theta_2(b) = \theta(a)\theta(b).$$

Доказательство для большего числа сомножителей проводится стандартным индуктивным рассуждением. ♦

Введем удобное обозначение. Всюду далее символом $\sum_{d|n}$ будем обозначать сумму чего-либо, в которой суммирование проведено по всем делителям d числа n. Следующие менее очевидные, чем предыдущие, свойства мультипликативных функций я сформулирую в виде лемм, ввиду их важности и удобства дальнейших ссылок.

Лемма 1. *Пусть $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$ — каноническое разложение числа $a \in \mathbf{N}$, θ — любая мультипликативная функция. Тогда*

$$\sum_{d\,|\,a} \theta(d) = (1 + \theta(p_1) + \theta(p_1^2) + \ldots + \theta(p_1^{\alpha_1})) \times$$
$$\times (1 + \theta(p_2) + \theta(p_2^2) + \ldots + \theta(p_2^{\alpha_2})) \times \ldots$$
$$\ldots \times (1 + \theta(p_n) + \theta(p_n^2) + \ldots + \theta(p_n^{\alpha_n})).$$

Если $a = 1$, то считаем правую часть равной 1.

Доказательство. Раскроем скобки в правой части. Получим сумму всех (без пропусков и повторений) слагаемых вида

$$\theta(p_1^{\beta_1}) \cdot \theta(p_2^{\beta_2}) \cdot \ldots \cdot \theta(p_n^{\beta_n}),$$

где $0 \leqslant \beta_k \leqslant \alpha_k$, для всех $k \leqslant n$. Так как различные простые числа заведомо взаимно просты, то

$$\theta(p_1^{\beta_1}) \cdot \theta(p_2^{\beta_2}) \cdot \ldots \cdot \theta(p_n^{\beta_n}) = \theta(p_1^{\beta_1} p_2^{\beta_2} \cdot \ldots \cdot p_n^{\beta_n}),$$

а это как раз то, что стоит в доказываемом равенстве слева. ♦

Лемма 2. *Пусть $\theta(a)$ — любая мультипликативная функция. Тогда $\chi(a) = \sum_{d\,|\,a} \theta(d)$ — также мультипликативная функция.*

Доказательство. Проверим для $\chi(a)$ аксиомы определения мультипликативной функции.

1). $\chi(1) = \sum_{d|1} \theta(d) = \theta(1) = 1$.

2). Пусть $(a, b) = 1$; $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$, $b = q_1^{\beta_1} q_2^{\beta_2} \cdot \ldots \cdot q_k^{\beta_k}$, и все p и q различны. Тогда, по предыдущей лемме, имеем (благо, делители у чисел a и b различны):

$$\chi(ab)=\sum_{d\,|\,ab}\theta(d)=\prod_i(1+\theta(p_i)+\theta(p_i^2)+\ldots+\theta(p_i^{\alpha_i}))\times$$
$$\times\prod_j(1+\theta(q_j)+\theta(q_j^2)+\ldots+\theta(q_j^{\beta_j}))=\chi(a)\chi(b).\qquad\blacklozenge$$

Итак, я перечислил шесть свойств мультипликативных функций, которые пригодятся нам в дальнейшем. Просьба хорошенько их запомнить и не унывать даже в самой тяжелой жизненной ситуации.

Задачки

1. Предлагаю читателю самостоятельно доказать обратное утверждение к лемме 2 настоящего пункта, а именно, если $f(a)=\sum\limits_{d\,|\,a}\theta(d)$ — мультипликативная функция и функция $\theta(n)$ всюду определена хотя бы на $\mathbf{N}$, то $\theta(n)$ также обязана быть мультипликативной функцией.

2. Пусть $\theta(p^\alpha)=\alpha$ для всех простых p. Вычислите
а) $\theta(864)$; б) $\theta(49500)$.

3. Пусть $\theta(p^\alpha)=\alpha$ для всех простых p. Вычислите
а) $\sum\limits_{d\,|\,864}\theta(d)$; б) $\sum\limits_{d\,|\,49500}\theta(d)$.

4. Пусть вещественная мультипликативная функция $f(x)$ определена и непрерывна для всех $x>0$. Докажите, что $f(x)=x^s$ для некоторого $s\in\mathbf{R}$, т. е. примером 1 настоящего пункта исчерпываются все непрерывные мультипликативные функции. [1)]

14. Примеры мультипликативных функций

Предыдущий пункт дал нам общие абстрактные знания о мультипликативных функциях вообще. Благодаря этому, в этом пункте мы сможем во всеоружии встретить целую серию примеров полезных мультипликативных функций. Большинство этих примеров строятся с использованием лемм предыдущего пункта, а в качестве исходного строительного материала берется

[1)] Самым первым на планете Земля этот факт установил О. Коши, интересовавшийся решениями функциональных уравнений следующих четырех видов:
$$f(x+y)=f(x)+f(y);\quad f(x+y)=f(x)f(y);$$
$$f(xy)=f(x)+f(y);\qquad f(xy)=f(x)f(y).$$
Он установил, что непрерывные решения этих уравнений имеют, соответственно, вид
$$Cx;\quad e^{Cx};\quad C\ln x;\quad x^C\quad(x>0)$$
(в классе разрывных функций могут быть и другие решения).

какая-нибудь конкретная степенная функция $\theta(a) = a^s$, которая, конечно, мультипликативна. Вы готовы? Начинаем.

Пример 1. Число делителей данного числа.

Пусть $\theta(a) = a^0 \equiv 1$ — тождественная единица (заведомо мультипликативная функция). Тогда, если $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$, то тождество леммы 1 п. 13 принимает вид:

$$\tau(a) = \sum_{d|a} \theta(d) = (1+\alpha_1)(1+\alpha_2) \cdot \ldots \cdot (1+\alpha_n) = \sum_{d|a} 1$$

— это не что иное, как количество делителей числа a. По лемме 2 п. 13, количество делителей $\tau(a)$ числа a есть мультипликативная функция.

Численный примерчик.

$$\tau(720) = \tau(2^4 \cdot 3^2 \cdot 5) = (4+1)(2+1) \cdot (1+1) = 30.$$

Пример 2. Сумма делителей данного числа.

Пусть $\theta(a) = a^1 \equiv a$ — тождественная мультипликативная функция. Тогда, если $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$, то тождество леммы 1 п. 13 принимает вид:

$$S(a) = \sum_{d|a} d = \sum_{d|a} \theta(d) = \underbrace{(1 + p_1 + p_1^2 + \ldots + p_1^{\alpha_1})}_{\substack{\text{сумма первых } (\alpha_1+1) \text{ членов} \\ \text{геометрической прогрессии}}} \times$$

$$\times\ (1 + p_2 + p_2^2 + \ldots + p_2^{\alpha_2}) \cdot \ldots \cdot (1 + p_n + p_n^2 + \ldots + p_n^{\alpha_n}) =$$

$$= \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_n^{\alpha_n+1} - 1}{p_n - 1}$$

— сумма всех делителей числа a. По лемме 2 п. 13, сумма всех делителей есть мультипликативная функция.

Численный примерчик.

$$S(720) = S(2^4 \cdot 3^2 \cdot 5) = \frac{2^5 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} = 2418.$$

Пример 3. Функция Мёбиуса.

Функция Мёбиуса $\mu(a)$ — это мультипликативная функция, определяемая следующим образом: если p — простое число, то $\mu(p) = -1$; $\mu(p^\alpha) = 0$, при $\alpha > 1$; на остальных натуральных числах функция доопределяется по мультипликативности.

Таким образом, если число a делится на квадрат натурального числа, отличный от единицы, то $\mu(a) = 0$; если же $a = p_1 p_2 \cdot \ldots \cdot p_k$ (теоретик-числовик сказал бы на своем жаргоне: «если a свободно от квадратов»), то $\mu(a) = (-1)^k$, где k — число различных простых делителей a. Понятно, что $\mu(1) = (-1)^0 = 1$, как и должно быть.

Лемма 1. *Пусть $\theta(a)$ — произвольная мультипликативная функция, $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$. Тогда*

$$\sum_{d|a} \mu(d)\theta(d) = (1 - \theta(p_1))(1 - \theta(p_2)) \cdot \ldots \cdot (1 - \theta(p_n)),$$

(*при $a = 1$ считаем правую часть равной* 1).

Доказательство. Рассмотрим функцию $\theta_1(x) = \mu(x) \cdot \theta(x)$. Эта функция мультипликативна как произведение мультипликативных функций. Для $\theta_1(x)$ имеем (p — простое): $\theta_1(p) = -\theta(x)$; $\theta_1(p^\alpha) = 0$, при $\alpha > 1$. Следовательно, для $\theta_1(x)$ тождество леммы 1 п. 13 выглядит так:

$$\sum_{d|a} \theta_1(d) = \prod_{k=1}^{n} (1 - \theta(p_k)). \qquad \blacklozenge$$

Следствие. *Пусть $\theta(d) = d^{-1} = \dfrac{1}{d}$* (это, конечно, мультипликативная функция), *$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$, $a > 1$. Тогда*

$$\sum_{d|a} \frac{\mu(d)}{d} = \Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big) \cdot \ldots \cdot \Big(1 - \frac{1}{p_n}\Big).$$

Воздержусь от доказательства этого следствия в силу банальности сего доказательства, но вот на правую часть этого тождества попрошу обратить внимание, так как она еще неоднократно у нас встретится. Физический смысл этой правой части раскрывает пример следующей функции.

Пример 4. Функция Эйлера.

Функция Эйлера, пожалуй, самая знаменитая и «дары приносящая» функция из всех функций, рассматриваемых в этом пункте. Функция Эйлера $\varphi(a)$ есть количество чисел из ряда $0, 1, 2, \ldots, a - 1$, взаимно простых с a. Полезность и практическое применение этой функции я продемонстрирую в следующих пунктах, а сейчас давайте поймем, как ее вычислять.

Лемма 2. *Пусть* $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$. *Тогда*

1) $\varphi(a) = a\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big) \cdot \ldots \cdot \Big(1 - \frac{1}{p_n}\Big)$ (формула Эйлера);

2) $\varphi(a) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdot \ldots \cdot (p_n^{\alpha_n} - p_n^{\alpha_n - 1})$, *в частности*, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, $\varphi(p) = p - 1$.

Доказательство. Пусть x пробегает числа $0, 1, 2, \ldots, a-1$. Положим $\delta_x = (x, a)$ — наибольший общий делитель. Тогда $\varphi(a)$ есть число значений δ_x, равных 1. Придумаем такую функцию $\chi(\delta_x)$, чтобы она была единицей, когда δ_x единица, и была нулем в остальных случаях. Вот подходящая кандидатура:

$$\chi(\delta_x) = \sum_{d|\delta_x} \mu(d) = \begin{cases} 0, & \text{если } \delta_x > 1, \\ 1, & \text{если } \delta_x = 1. \end{cases}$$

Последнее легко понять, если вспомнить лемму 1 из этого пункта и в ее формулировке взять $\theta(d) \equiv 1$. Далее, сделав над собой некоторое усилие, можно заметить, что

$$\varphi(a) = \sum_{0 \leqslant x < a} \chi(\delta_x) = \sum_{0 \leqslant x < a} \Big(\sum_{d|\delta_x} \mu(d) \Big).$$

Поскольку справа сумма в скобках берется по всем делителям d числа $\delta_x = (x, a)$, то d делит x и d делит a. Значит, в первой сумме справа в суммировании участвуют только те x, которые кратны d. Таких x среди чисел $0, 1, 2, \ldots, a-1$ ровно $\frac{a}{d}$ штук. Получается, что

$$\varphi(a) = \sum_{d|a} \frac{a}{d} \mu(d) = a \sum_{d|a} \frac{\mu(d)}{d} = a\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big) \cdot \ldots \cdot \Big(1 - \frac{1}{p_n}\Big),$$

что и требовалось.

Пояснение для читателей. Имеем

$$\varphi(a) = \sum_{0 \leqslant x < a} \Big(\sum_{d|(x,a)} \mu(d) \Big).$$

Зафиксируем некоторое d_0 такое, что d_0 делит a, d_0 делит x, $x < a$. Значит, в сумме справа в скобках слагаемых $\mu(d_0)$ ровно $\frac{a}{d_0}$ штук и $\varphi(a)$ есть просто сумма $\sum\limits_{d_0|a} \frac{a}{d_0}$. После этого равенство

$$a \sum_{d|a} \frac{\mu(d)}{d} = a\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big) \cdot \ldots \cdot \Big(1 - \frac{1}{p_n}\Big)$$

получается применением следствия из леммы 1 этого пункта.

Второе утверждение леммы следует из первого внесением впереди стоящего множителя a внутрь скобок. ♦

Оказывается, только что доказанная формула

$$\varphi(a) = a\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big) \cdot \ldots \cdot \Big(1 - \frac{1}{p_n}\Big)$$

для вычисления функции Эйлера имеет ясный «физический смысл». Дело в том, что в ней отражено так называемое правило включений и исключений.

Правило включений и исключений. *Пусть задано множество* $\mathbf{A}$ *и выделено* $\mathbf{k}$ *его подмножеств. Количество элементов множества* $\mathbf{A}$, *которые не входят ни в одно из выделенных подмножеств*, *подсчитывается так*: *надо из общего числа элементов* $\mathbf{A}$ *вычесть количества элементов всех* $\mathbf{k}$ *подмножеств*, *прибавить количества элементов всех их попарных пересечений*, *вычесть количества элементов всех тройных пересечений*, *прибавить количества элементов всех пересечений по четыре и т. д. вплоть до пересечения всех* $\mathbf{k}$ *подмножеств.*

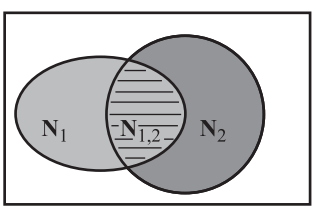


Рис. 4

Проиллюстрирую это правило на примере подсчета функции Эйлера для чисел вида $a = p_1^{\alpha_1} p_2^{\alpha_2}$. Посмотрите на рис. 4.

Прямоугольник изображает множество всех целых чисел от 0 до a; овал $\mathbf{N}_1$ — множество чисел, кратных p_1; кружок $\mathbf{N}_2$ — числа, кратные p_2; пересечение $\mathbf{N}_{1,2}$ — множество чисел, делящихся одновременно на p_1 и p_2, т. е. на $p_1 p_2$; числа вне овала и кружочка взаимно просты с a. Для подсчета числа чисел, взаимно простых с a, нужно из a вычесть количество чисел в $\mathbf{N}_1$ и количество чисел в $\mathbf{N}_2$ (их, соответственно, $\frac{a}{p_1}$ и $\frac{a}{p_2}$ штук), при этом общая часть $\mathbf{N}_{1,2}$ (там $\frac{a}{p_1 p_2}$ штук чисел) вычтется дважды, значит ее надо один раз прибавить (вот оно, «включение–исключение»!). В результате получим

$$\varphi(a) = a - \frac{a}{p_1} - \frac{a}{p_2} + \frac{a}{p_1 p_2} = a\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big),$$

что я вам и утверждал. Мне кажется, что таким способом можно объяснить формулу Эйлера любому смышленому школьнику.

Кстати, любому смышленому школьнику вполне возможно объяснить и то, что при $a > 2$ число $\varphi(a)$ всегда четное. Действительно, если k взаимно просто с a и $k < a$, то число $a - k$ тоже меньше a, взаимно просто с a и не равно k. (Если бы a и $a - k$ имели общий делитель, то их разность $a - (a - k) = k$ тоже делилась бы на этот делитель, что противоречит взаимной простоте a и k.) Значит, числа, взаимно простые с a, разбиваются на пары k и $a - k$, следовательно, их четное число.

Из леммы 2 вытекают приятные следствия.

Следствие 2. *Функция Эйлера мультипликативна.*

Доказательство. Имеем

$$\varphi(a) = \left(\sum_{d|a} \frac{\mu(d)}{d}\right) \cdot a$$

— произведение двух мультипликативных функций, первая из которых мультипликативна по лемме 2 п. 13. Значит, $\varphi(a)$ — мультипликативна. ♦

Следствие 3. $\sum\limits_{d|a} \varphi(d) = a.$

Доказательство. Пусть $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$. Тогда, по лемме 1 п. 13 имеем

$$\sum_{d|a} \varphi(d) = \prod_{k=1}^{n} (1 + \varphi(p_k) + \varphi(p_k^2) + \ldots + \varphi(p_k^{\alpha_k})) =$$

$$= \prod_{k=1}^{n} (1 + (p_k - 1) + (p_k^2 - p_k) + \ldots + (p_k^{\alpha_k} - p_k^{\alpha_k - 1})) =$$

$$= p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n} = a. \quad ♦$$

Численные примерчики.

$$\varphi(5) = 5 - 1 = 4,$$

$$\varphi(30) = \varphi(2 \cdot 3 \cdot 5) = (2 - 1)(3 - 1)(5 - 1) = 8,$$

$$\varphi(60) = 60 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 16,$$

$$\sum_{d|30}\varphi(d)=\varphi(1)+\varphi(2)+\varphi(3)+\varphi(5)+\varphi(6)+\varphi(10)+$$
$$+\ \varphi(15)+\varphi(30)=1+1+2+4+2+4+8+8=30.$$

На этом, пожалуй, п. 14 закончим.

Задачки

1. Потренируйтесь и найдите число делителей и сумму делителей чисел: а) 5600; б) 116424.

2. Найдите сумму собственных делителей (т. е. делителей, отличных от самого числа) чисел: а) 6; б) 28; в) 496; г) 8128. Подивитесь полученному результату. [1])

3. Составьте таблицу значений функции Мёбиуса $\mu(n)$ для всех значений n от 1 до 100. Бережно сохраните результат.

4. Составьте таблицу значений функции Эйлера $\varphi(n)$ для всех значений n от 1 до 100. Бережно сохраните результат.

5. Используя формулу Эйлера для $\varphi(n)$, еще раз докажите бесконечность множества простых чисел.

6. Докажите, что существует бесконечно много чисел $n\in\mathbf{N}$, удовлетворяющих для всех $k=1,2,\ldots,n-1$ неравенствам
$$\frac{S(n)}{n}>\frac{S(k)}{k},$$
где $S(n)$ — сумма всех делителей числа n.

[1]) Числа, равные сумме собственных делителей, древние греки назвали совершенными. В формулировке задачи указаны первые четыре (известных еще Пифагору) совершенных числа. Евклид обнаружил, что если число 2^k-1 — простое, то число $(2^k-1)\cdot 2^{k-1}$ обязано быть совершенным. Эйлер доказал, что все четные совершенные числа имеют такой вид. Неизвестно, существуют ли вообще нечетные совершенные числа; во всяком случае, такие числа должны быть больше 10^{100} — результат хорошо организованной машинной проверки. Имеется ровно 24 значения $k<20000$, для которых число 2^k-1 — простое (в этом случае k само обязано быть простым). Простые числа вида 2^k-1 называются числами Мерсенна, по имени французского математика, который в 1644 г. указал в большей части верный список всех таких простых, меньших 10^{79}. Изрядно потрудившись, читатель сам может выписать наибольшее известное на сегодняшний день совершенное число, отталкиваясь от наибольшего известного на сегодня простого числа Мерсенна, указанного в п. 6 этой книжки. Предполагается, что совершенные числа были известны уже в древнем Вавилоне и Египте, где рука с загнутым безымянным пальцем обозначала число шесть — первое совершенное число. Тем самым этот палец сам стал причастен к совершенству и за ним закрепилась привилегия носить обручальное кольцо.

7. Докажите, что для любого натурального n выполняются неравенства

$$\frac{n^2}{2} < \varphi(n) \cdot S(n) < n^2.$$

8. На кафтане площадью 1 нашито 5 заплат, площадь каждой из которых не меньше $1/2$. Докажите, что найдутся две заплаты, площадь общей части которых не меньше $1/5$.

9. Клуб регулярно посещают 220 человек. При клубе имеется шесть спортивных секций. В эти секции записались, соответственно, 30, 26, 32, 31, 28 и 36 человек. В несколько секций записались 53 члена клуба, из них 24 посещают три или больше секций, 9 — не меньше четырех секций и 3 — даже пять секций. В последнюю тройку входит один чудак, который записался во все шесть секций. Директор клуба хочет знать, сколько членов клуба не записались ни в одну секцию?

10. Пусть k — натуральное число, d пробегает все делители числа a с условием $\varphi(d) = k$. Докажите, что

$$\sum_d \mu(d) = 0.$$

11. Пусть k — четное натуральное число, d пробегает все делители свободного от квадратов числа $a = p_1 p_2 \cdot \ldots \cdot p_k$ с условием $0 < d < \sqrt{a}$. Докажите, что

$$\sum_d \mu(d) = 0.$$

15. ζ-функция Римана

Этот пункт несколько сложнее предыдущих, так как для его понимания потребуются определенные знания из области математического анализа и теории функций комплексного переменного. Но было бы просто неправильно в параграфе под названием «Важнейшие функции в теории чисел» умолчать об одной из самых загадочных и влиятельных в математике функций — ζ-функции Римана, поэтому сделаем над собой некоторое усилие, отбросим внутреннюю скованность и попытаемся подойти к ζ-функции, чтобы познакомиться. Всюду ниже буквой $\mathbf{C}$ обозначается поле комплексных чисел.

Определение. Пусть $s \in \mathbf{C}$, действительная часть $\mathrm{Re}\,(s) > 1$. *ζ-функцией Римана* называется функция комплексного перемен-

ного, задаваемая рядом

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Правомерность такого определения подтверждает следующее наблюдение.

Наблюдение. *В полуплоскости* $\operatorname{Re}(s) > 1$ *ряд* $\sum\limits_{n=1}^{\infty} \frac{1}{n^s}$ *сходится абсолютно.*

Доказательство. Пусть $s \in \mathbf{C}$, $\operatorname{Re}(s) > 1$, $s = \sigma + i\varphi$ (см. рис. 5).

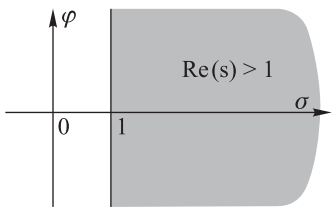


Рис. 6

Вычислим абсолютные величины членов ряда:

$$\left|n^{-s}\right| = \left|e^{-s\ln n}\right| = \left|e^{-\sigma\ln n - i\varphi\ln n}\right| =$$

$$= \left|e^{-\sigma\ln n}(\cos(\varphi\ln n) - i\sin(\varphi\ln n))\right| = \left|e^{-\sigma\ln n}\right| = \left|\frac{1}{n^\sigma}\right| = \frac{1}{n^\sigma}.$$

Теперь воспользуемся интегральным признаком сходимости (мы помним, что $\sigma > 1$):

$$\sum_{n=1}^{\infty}\left|\frac{1}{n^s}\right| = \sum_{n=1}^{\infty}\frac{1}{n^\sigma} \leqslant \int_1^{\infty}\frac{1}{x^\sigma}dx = \lim_{N\to\infty}\left.\frac{x^{-\sigma+1}}{-\sigma+1}\right|_1^N =$$

$$= \lim_{N\to\infty}\left(\frac{N^{-\sigma+1}}{-\sigma+1} - \frac{1}{-\sigma+1}\right) = \frac{1}{\sigma-1}.$$

Значит, при $\sigma > 1$ ряд $\sum\limits_{n=1}^{\infty}\frac{1}{n^s}$ сходится абсолютно. ♦

Из этого наблюдения вытекает

Следствие. *Функция* $\zeta(s)$ *аналитична в полуплоскости* $\operatorname{Re}(s) > 1$.

Доказательство. Действительно, при всяком $\varepsilon > 0$ и фиксированном $\rho > 1 + \varepsilon$ числовой ряд $\sum\limits_{n=1}^{\infty} \frac{1}{n^{\rho}}$ мажорирует ряд из абсолютных величин $\sum\limits_{n=1}^{\infty} \left| \frac{1}{n^s} \right| = \sum\limits_{n=1}^{\infty} \frac{1}{n^{\sigma}}$, где $\sigma \geqslant \rho$, откуда, по теореме Вейерштрасса, следует равномерная сходимость ряда $\sum\limits_{n=1}^{\infty} \frac{1}{n^s}$ в полуплоскости $\mathrm{Re}\,(s) \geqslant \rho$. Сумма же **равномерно** сходящегося ряда из аналитических функций сама является аналитической функцией.

Теперь осталось только неограниченно приблизиться к вертикальной пунктирной прямой $\mathrm{Re}\,(s) = 1$ на рис. 5, устремляя ε к нулю. Получается, что во всех полуплоскостях, граница которых сколь угодно близко подходит к прямой $\mathrm{Re}\,(s) = 1$, ряд $\sum\limits_{n=1}^{\infty} \frac{1}{n^s}$ сходится абсолютно и равномерно, а его сумма — аналитическая функция. ♦

Нематематическое (значит, лирическое) отступление

Справедливости ради следует сказать, что функцию $\zeta(s) = \sum\limits_{n=1}^{\infty} \frac{1}{n^s}$ впервые рассматривал Эйлер, который узнал много ее свойств и открыл свою знаменитую формулу: $\zeta(s) = \sum\limits_{n=1}^{\infty} \frac{1}{n^s} = \prod\limits_{j=1}^{\infty} \left(1 - \frac{1}{p_j^s}\right)^{-1}$, связывающую $\zeta(s)$ с простыми числами. Поэтому правильнее было бы называть главную героиню этого пункта дзета-функцией Эйлера. Однако, уж так повелось, что ее называют «дзета-функция Римана». (Ортодоксальные математики до сих пор, например, условия аналитичности Даламбера–Эйлера функции комплексного переменного называют условиями Коши–Римана.) Разумеется, Риман тоже изучал функцию $\zeta(s)$ и высказал про нее много интересного, но мы не будем осуждать здесь ортодоксальных математиков за неправильное именование функции $\zeta(s)$, ибо само по себе имя ярчайшей звезды математического небосклона Георга Фридриха Бернгарда Римана есть вечная награда для любой функции, а $\zeta(s)$ такой орден, несомненно, заслужила.

Несколько слов о Бернгарде Римане (1826–1866), человеке, который в очень большой степени определил лицо современной математики. Риман был сыном деревенского священника, учился в Гёттингенском университете, где в 1851 г. получил степень доктора, в 1854 г. стал приват-доцентом, в 1859 г. — профессором, переемником Дирихле на

кафедре математики. Болезненный, он провел последние несколько месяцев жизни в Италии, где и умер в сорокалетнем возрасте. За свою короткую жизнь Риман опубликовал небольшое число работ, но каждая из них — настоящая жемчужина, открывающая новые и плодотворные области. Именно Риману мы обязаны введением в анализ топологических представлений, понятию римановой поверхности, определению интеграла Римана, исследованию гипергеометрических рядов и абелевых функций, и т. д., и т. д. Именно ему мы обязаны новому взгляду на геометрию, при котором пространство вводится как топологическое многообразие с метрикой, задаваемой произвольной квадратичной дифференциальной формой (теперь мы говорим — римановы пространства). В работе 1859 г. он исследовал количество простых чисел, меньших заданного числа, и дал точную формулу для нахождения этого числа с участием функции $\zeta(s)$. В этой знаменитой работе сформулирована не менее знаменитая «Гипотеза Римана» о нулях аналитического продолжения $\zeta(s)$ на всю комплексную плоскость. (Верно ли, что все недействительные нули дзета-функции лежат на прямой $\mathrm{Re}\,(s) = \dfrac{1}{2}$?) Эта гипотеза, пожалуй, является одной из самых старых, трудных и насущных математических проблем. Она до сих пор не доказана и не опровергнута.

Далее нам потребуются некоторые сведения из математического анализа и теории функций комплексного переменного о бесконечных произведениях. Бесконечные произведения — забавная и полезная потеха, которой почему-то, в отличие от бесконечных сумм, на лекциях в университете уделяют мало внимания. Исправим, отчасти, сие недоразумение.

Определение. Пусть $u_1, u_2, \ldots, u_n, \ldots$ — бесконечная последовательность комплексных чисел и все $u_j \neq -1$. Выражение вида

$$\prod_{n=1}^{\infty} (1 + u_n) = (1 + u_1)(1 + u_2) \cdot \ldots \cdot (1 + u_n) \cdot \ldots \qquad (\spadesuit)$$

называется *бесконечным произведением*, а выражения

$$\prod_{n=1}^{k} (1 + u_n) = (1 + u_1)(1 + u_2) \cdot \ldots \cdot (1 + u_k) = v_k$$

— *частичными произведениями* бесконечного произведения ($\spadesuit$).

Если последовательность частичных произведений v_k при $k \to \infty$ сходится к числу $v \neq 0$, то говорят, что бесконечное произведение (♠) сходится и равно v. В противном случае, если v_k не сходится (или $v_k \to 0$), то говорят, что бесконечное произведение (♠) расходится (соответственно, расходится к нулю).

Честно говоря, при первом знакомстве, словосочетание «расходится к нулю» вызвало у меня недоумение. Однако при дальнейшем изучении конструкции бесконечного произведения, это недоумение рассеялось, так как выделение особого случая $v_k \to 0$ связано с традицией логарифмировать бесконечные произведения, чтобы перейти к рядам — более знакомым объектам, а логарифм нуля не имеет смысла и, видимо, находится далеко за пределами нашего разумения.

Теорема 1 (признак сходимости (♠)). *Если ряд*

$$u_1 + u_2 + \ldots + u_n + \ldots$$

сходится абсолютно, то бесконечное произведение (♠) *сходится.*

Доказательство. Пусть $\sum\limits_{n=1}^{\infty} |u_n|$ — сходится, значит, общий член этого ряда стремится к нулю и можно считать, что, например, $|u_n| \leqslant \dfrac{1}{2}$ для всех $n > n_0 \in \mathbf{N}$. Пусть сначала $u_n \in \mathbf{R}$. Тогда, в силу замечательного предела $\lim\limits_{u_n \to 0} \dfrac{|\ln(1+u_n)|}{|u_n|} = 1$, начиная с некоторого номера $n > n_0$, имеем $|\ln(1+u_n)| \leqslant 2\,|u_n|$. Значит, последовательность логарифмов частичных произведений

$$S_n = \ln(1+u_1) + \ln(1+u_2) + \ldots + \ln(1+u_n) = \ln v_n$$

сходится, так как $|S_n| \leqslant 2 \sum\limits_{k=1}^{n} |u_k|$, а справа в последнем неравенстве стоят частичные суммы сходящегося ряда. Следовательно, сходится и бесконечное произведение (♠).

Пусть теперь u_n — произвольные комплексные числа. Надо доказать, что при $n \to \infty$ сходятся две последовательности действительных чисел:

$$|v_n| = |(1+u_1) \cdot \ldots \cdot (1+u_n)| = |1+u_1| \cdot \ldots \cdot |1+u_n| \qquad (1)$$

и

$$\arg v_n = \arg\left((1+u_1)\cdot\ldots\cdot(1+u_n)\right) = \\ = \arg(1+u_1)+\ldots+\arg(1+u_n). \quad (2)$$

Пусть $u_n = \alpha_n + i\beta_n$. Ясно, что для сходимости последовательности $|v_n|$ необходимо и достаточно сходимости последовательности $|v_n|^2$. Но $|1+u_n|^2 = |1+\alpha_n+i\beta_n|^2 = 1+\alpha_n^2+\beta_n^2+2\alpha_n$ и, так как $|\alpha_n^2+\beta_n^2+2\alpha_n| \leqslant |u_n|^2+2|u_n|$, то сходимость (1) следует из уже доказанного. Сходимость (2) следует из того, что при всех n, больших некоторого n_0, $|\arg(1+u_n)| = \left|\arcsin\dfrac{\beta_n}{\sqrt{(1+\alpha_n)^2+\beta_n^2}}\right| < \pi|\beta_n|$ (здесь опять использован замечательный предел $\lim\limits_{x\to 0}\dfrac{\arcsin x}{x} = 1$), а $|\beta_n| \to 0$ так как $u_n \to 0$. ♦

Ключ к пониманию огромной роли функции $\zeta(s)$ в теории чисел кроется в уже упоминавшейся выше замечательной формуле Эйлера.

Теорема 2 (формула Эйлера). Функция

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s} = \prod_{j=1}^{\infty}\left(1-\frac{1}{p_j^s}\right)^{-1},$$

где p_j – j-е простое число и, таким образом, бесконечное произведение справа берется по всем простым числам.

Доказательство. Пусть $\mathbf{X} \geqslant 1$, $\mathrm{Re}\,(s) > 1$. Ряды

$$1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\frac{1}{p^{3s}}+\ldots$$

абсолютно сходятся (ибо мажорируются геометрическими прогрессиями). По теореме 1 это значит, что бесконечное произведение в формуле Эйлера сходится. Имеем (значок $\prod\limits_{p\leqslant X}$ означает произведение по всем простым числам, не превосходящим $\mathbf{X}$):

$$\prod_{p\leqslant X}\left(1-\frac{1}{p^s}\right)^{-1} = \prod_{p\leqslant X}\left(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\ldots\right) = \sum_{n\leqslant X}\frac{1}{n^s}+R(s,X).$$

Здесь при получении первого равенства использовалась формула суммы геометрической прогрессии, при получении последнего равенства существенную роль сыграла основная теорема арифметики. Через $R(s,X)$ обозначен остаточный член, приписывание которого в нужном месте, вообще-то, позволяет поставить знак равенства между любыми величинами. На самом же деле, $R(s,X)$ содержит бесконечное число слагаемых вида $\frac{1}{n^s}$, не вошедших в стоящую перед ним сумму. Оценим остаточный член:

$$|R(s,X)| \leqslant \sum_{n>X} \left|\frac{1}{n^s}\right| = \sum_{n>X} \frac{1}{n^\sigma} \leqslant \frac{1}{\sigma-1} X^{1-\sigma},$$

т. е. $R(s,X) \to 0$, при $X \to \infty$. Это и означает справедливость формулы Эйлера. ♦

Следствие 2. *При* $\mathrm{Re}\,(s) > 1$ *функция* $\zeta(s)$ *не имеет нулей.*

Доказательство. Имеем

$$\frac{1}{|\zeta(s)|} = \left|\prod_p \left(1-\frac{1}{p^s}\right)\right| \leqslant \prod_p \left(1+\frac{1}{p^\sigma}\right) <$$

$$< \sum_{n=1}^{\infty} \frac{1}{n^\sigma} \leqslant 1 + \int\limits_1^\infty \frac{dx}{x^\sigma} = 1 + \frac{1}{\sigma-1},$$

значит, $|\zeta(s)| > \dfrac{\sigma-1}{\sigma} > 0$. ♦

Продолжим $\zeta(s)$ в полуплоскость $\mathrm{Re}\,(s) > 0$. Следующие лемма и следствие из нее призваны лишь показать один из возможных способов реализации такого продолжения, поэтому их доказательство можно пропустить без всякого ущерба для дальнейшего понимания.

Лемма 1. *При* $\mathrm{Re}\,(s) > 0$ и $N \geqslant 1$ *выполнено*

$$\zeta(s) = \sum_{n=1}^{N} \frac{1}{n^s} + \frac{N^{1-s}}{s-1} - \frac{1}{2} N^{-s} + s \int\limits_N^\infty \frac{1/2 - \{u\}}{u^{s+1}} du.$$

Доказательство. Имеем при $\mathrm{Re}\,(s) > 1$:

$$\sum_{n=N+1}^{\infty} \frac{1}{n^s} = \sum_{n=N}^{\infty} n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) - \frac{1}{N^{s-1}} =$$

$$= -\frac{1}{N^{s-1}} + s \sum_{n=N}^{\infty} n \int\limits_{n}^{n+1} x^{-s-1} dx =$$

$$= -\frac{1}{N^{s-1}} + s \sum_{n=N}^{\infty} \int\limits_{n}^{n+1} [x] \cdot x^{-s-1} dx = -\frac{1}{N^{s-1}} + s \int\limits_{N}^{\infty} [x] \cdot x^{-s-1} dx =$$

$$= -\frac{1}{N^{s-1}} + \frac{sN^{1-s}}{s-1} - s \int\limits_{N}^{\infty} \{x\} x^{-s-1} dx =$$

$$= \frac{N^{1-s}}{s-1} - \frac{1}{2} N^{-s} + s \int\limits_{N}^{\infty} \left(\frac{1}{2} - \{x\} \right) x^{-s-1} dx.$$

Но последний интеграл справа определяет аналитическую функцию даже при $\mathrm{Re}\,(s) > 0$. Поэтому, в силу принципа аналитического продолжения, утверждение леммы 1 справедливо. ♦

Следствие. *Функция $\zeta(s)$ является аналитической в полуплоскости $\mathrm{Re}\,(s) > 0$ за исключением точки $s = 1$; в точке $s = 1$ дзета-функция имеет простой полюс с вычетом, равным* 1. ♦

Оказывается, что дзета-функция имеет бесконечно много нулей в «критической полосе» $1 > \mathrm{Re}\,(s) > 0$. Известно, что эти нули лежат симметрично относительно прямых $\mathrm{Re}\,(s) = \dfrac{1}{2}$ и $\mathrm{Im}\,(s) = 0$; известно, что в области $\mathrm{Re}\,(s) \geqslant 1 - \dfrac{c}{\ln(|b|+2)}$, где $b = \mathrm{Im}\,(s)$, а c — абсолютная постоянная, нулей у $\zeta(s)$ нет (теорема Ш. Валле-Пуссена). Однако знаменитая гипотеза Римана о том, что все нули $\zeta(s)$ лежат на прямой $\mathrm{Re}\,(s) = \dfrac{1}{2}$, до сих пор не доказана, хотя проверена для более 7 миллионов корней. Хотите посмотреть на первые десять корней $\zeta(s) = 0$? Вот они:

$$\rho_{1,2} = \frac{1}{2} \pm 14,134725\, i,$$

$$\rho_{3,4} = \frac{1}{2} \pm 21,022040\, i,$$

$$\rho_{5,6} = \frac{1}{2} \pm 25,010856\, i,$$

$$\rho_{7,8} = \frac{1}{2} \pm 30,424878\, i,$$

$$\rho_{9,10} = \frac{1}{2} \pm 32,935057\, i.$$

(Шутка: предлагаю непосредственной подстановкой убедиться, что это — корни $\zeta(s) = 0$.)

Приведу еще, в качестве красивой картинки, без комментариев, ту самую удивительную формулу Римана, о которой уже упоминалось в этом пункте мелким шрифтом, для числа $\pi(x)$ простых чисел, не превосходящих x:

$$\pi(x) = R(x) - \sum_{\rho} R(x^{\rho}),$$

где суммирование справа ведется по всем нулям $\zeta(s)$, а

$$R(x) = 1 + \sum_{n=1}^{\infty} \frac{1}{n\zeta(n+1)} \cdot \frac{(\ln x)^n}{n!}.$$

К сожалению, рассказ о серьезных и нетривиальных применениях дзета-функции Римана выходит за рамки этой скромной книжки, поэтому, чтобы хоть как-то представить всю мощь этой функции, немного постреляем из пушки по воробьям — докажем с ее помощью пару известных утверждений.

Утверждение 1. *Простых чисел бесконечно много.*

Доказательство первое. Пусть $p_1, p_2, \ldots, p_k$ — все простые. Тогда, так как

$$\prod_{p \leqslant N} \left(1 - \frac{1}{p^s}\right)^{-1} = \sum_{n \leqslant N} \frac{1}{n^s} + R(s; N),$$

получаем (при $s = 1$ и достаточно больших N):

$$\prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right)^{-1} \geqslant \sum_{n \leqslant N} \frac{1}{n},$$

ибо $R(s; N) \underset{N \to \infty}{\longrightarrow} 0$. Но это невозможно, ибо гармонический ряд $\sum\limits_{n=1}^{\infty} \frac{1}{n}$ расходится. ♦

Доказательство второе. Пусть $p_1, p_2, \ldots, p_k$ — все простые. Тогда

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \prod_{j=1}^{k} \left(1 - \frac{1}{p_j^2}\right)^{-1} = \frac{\pi^2}{6},$$

что невозможно, ибо конечное произведение суть рациональное число, чего никак не скажешь о числе $\dfrac{\pi^2}{6}$. ♦

Следующее утверждение гораздо менее известно, чем бесконечность множества простых.

Возмем гармонический ряд $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n}$ и сильно проредим его, оставив в нем только слагаемые, обратные к простым числам, и выкинув все слагаемые, являющиеся обратными к составным. Это действительно сильное прорежение, так как в натуральном ряде имеются сколь угодно длинные промежутки без простых чисел, например:

$$n! + 2,\ n! + 3,\ n! + 4,\ \ldots,\ n! + n.$$

Гармонический ряд, как известно, расходится. Удивительно, что

Утверждение 2. *Ряд* $\displaystyle\sum_{j=1}^{\infty} \frac{1}{p_j}$ *из обратных величин ко всем простым числам расходится.*

Доказательство. Пусть $\mathbf{X} \in \mathbf{N}$. Имеем

$$\prod_{p_k \leqslant X} \left(1 - \frac{1}{p_k}\right)^{-1} = \prod_{p_k \leqslant X} \left(1 + \frac{1}{p_k} + \frac{1}{p_k^2} + \ldots\right) =$$

$$= \sum_{p_k \leqslant X} \frac{1}{p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}} = \sum_{n \leqslant X} \frac{1}{n} + \sum_{n > X}^{\nabla} \frac{1}{n},$$

где значок ∇ означает, что суммирование ведется по всем $n > X$, в разложении которых нет простых сомножителей, больших $\mathbf{X}$. Значит,

$$\prod_{p_k \leqslant X} \left(1 - \frac{1}{p_k}\right)^{-1} > \sum_{n \leqslant X} \frac{1}{n}$$

и

$$\prod_{p_k \leqslant X} \left(1 - \frac{1}{p_k}\right)^{-1} \underset{X\to\infty}{\longrightarrow} \infty,$$

так как гармонический ряд расходится. Из последнего вытекает, что бесконечное произведение

$$\prod_{p_k} \left(1 - \frac{1}{p_k}\right) = 0$$

расходится к нулю, т. е.

$$P_n = \prod_{k=1}^{n} \left(1 - \frac{1}{p_k}\right) \underset{n\to\infty}{\longrightarrow} 0.$$

Значит, [1])

$$\ln P_n = \sum_{k=1}^{n} \ln \left(1 - \frac{1}{p_k}\right) \underset{n\to\infty}{\longrightarrow} -\infty.$$

Мы помним замечательный предел:

$$\lim_{k\to\infty} \frac{\ln\left(1 - \dfrac{1}{p_k}\right)}{-\dfrac{1}{p_k}} = 1,$$

из которого следует, что, начиная с некоторого k,

$$\frac{\ln\left(1 - \dfrac{1}{p_k}\right)}{-\dfrac{1}{p_k}} < 2,$$

откуда моментально

$$\ln\left(1 - \frac{1}{p_k}\right) > 2\left(-\frac{1}{p_k}\right).$$

Таким образом, в ряде

$$2\sum_{k=1}^{\infty} \left(-\frac{1}{p_k}\right)$$

[1]) $1 - \dfrac{1}{p_k} > 0$, так как все $p_k > 1$; $p = 1$ — особое число.

каждый член меньше соответствующего члена расходящегося к $-\infty$ ряда

$$\sum_{k=1}^{\infty} \ln\left(1 - \frac{1}{p_k}\right),$$

следовательно, ряд $\displaystyle\sum_{k=1}^{\infty}\left(\frac{1}{p_k}\right)$ расходится к $+\infty$. ♦

Справедливости ради отмечу: несмотря на то, что ряд $\displaystyle\sum_{k=1}^{\infty}\left(\frac{1}{p_k}\right)$ самым невероятным образом расходится, он расходится все-таки медленнее гармонического. Про частичные суммы этих рядов известно, что $\displaystyle\sum_{k=1}^{n}\frac{1}{k}$ растет как $\ln n$ [1]), в то время, как $\displaystyle\sum_{k=1}^{p_n}\left(\frac{1}{p_k}\right)$ растет только как $\ln(\ln p_n)$.

Позвольте мне быстренько закончить этот уже порядком поднадоевший пункт, а вместе с ним и весь третий параграф, установлением связи между дзета-функцией (которая не мультипликативна) и функцией Мёбиуса $\mu(n)$ (которая мультипликативна). Из этой связи понятно, что $\zeta(s)$ очень близка к мультипликативным функциям — просто единица, деленная на дзета-функцию, есть сумма (правда, бесконечная) мультипликативных функций.

Лемма 2. *Пусть* $\mathrm{Re}\,(s) > 1$. *Тогда*

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}.$$

Доказательство. Пусть $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$. В лемме 1 из п. 14 положим $\theta(x) = \dfrac{1}{x^s}$ — мультипликативная функция. Тогда

$$\sum_{d|n}\frac{\mu(d)}{d^s} = \prod_{j=1}^{k}\left(1 - \frac{1}{p_j^s}\right),$$

[1]) Более того, известен поразительный результат Л. Эйлера о том, что предел

$$\gamma = \lim_{n\to\infty}\left(\sum_{k=1}^{n}\frac{1}{k} - \ln n\right)$$

существует и $\gamma \approx 0{,}5772\ldots$. Число γ называется теперь постоянной Эйлера.

$$\prod_{p_k\leqslant X}\left(1-\frac{1}{p_k^s}\right)=\prod_{p_k\leqslant X}\left(1+\frac{1}{p_k^s}+\frac{1}{p_k^{2s}}+\ldots\right)=$$

$$=\sum_{n\leqslant X}\frac{\mu(n)}{n^s}+\sum_{n>X}^{\nabla}\frac{\mu(n)}{n^s},$$

где значок ∇, как и ранее, означает, что суммирование ведется по всем $n>X$, в разложении которых нет простых сомножителей, больших $\mathbf{X}$. Далее, устремляя $\mathbf{X}$ к бесконечности и вспоминая определение функции Мёбиуса, получаем

$$\left|\sum_{n>X}^{\nabla}\frac{\mu(n)}{n^s}\right|<\sum_{n>X}^{\nabla}\frac{1}{n^s}\underset{X\to\infty}{\longrightarrow}0,$$

следовательно,

$$\prod_{p}\left(1-\frac{1}{p^s}\right)=\frac{1}{\zeta(s)}=\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}. \qquad \blacklozenge$$

Завершим наше знакомство с дзета-функцией, а вместе с этим знакомством завершается и весь третий параграф. Ура!

Задачки

1. Вычислите $\zeta(3)$.

2. Докажите, что ряд, составленный из обратных величин к простым числам, встречающимся в арифметической прогрессии $3,7,11,15,19,23,\ldots$, расходится.

3. Пусть $\Lambda(a)=\ln p$ для $a=p^l$, где p — простое, l — натуральное; $\Lambda(a)=0$ для остальных натуральных a. [1] Докажите, что при $\mathrm{Re}\,(s)>1$ выполнено:

$$\frac{\zeta'(s)}{\zeta(s)}=-\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}.$$

4. Пусть $\mathrm{Re}\,(s)>2$. Докажите, что

$$\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s}=\frac{\zeta(s-1)}{\zeta(s)},$$

где $\varphi(n)$ — функция Эйлера.

[1] Функция $\Lambda(a)$ называется функцией Мангольдта — весьма примечательный персонаж в теории чисел, знакомство с которым осталось, к сожалению, за рамками этой книжки.

5. Определим вероятность P того, что k натуральных чисел $x_1, x_2, \ldots, x_k$ будут взаимно простыми, как предел при $N \to \infty$ вероятности P_N того, что будут взаимно простыми k чисел $x_1, x_2, \ldots, x_k$, каждому из которых независимо от остальных присвоено одно из значений $1, 2, \ldots, N$, принимаемых за равновозможные. [1] Докажите, что

$$\mathsf{P} = \frac{1}{\zeta(k)}.$$

[1] Сравните с определением, данным в п. 3 этой книжки. Обратите внимание, что результат п. 3 — теорема Чезаро — находится в прекрасном соответствии с утверждением этой задачи:

$$\mathsf{P} = \frac{6}{\pi^2} = \frac{1}{\zeta(2)}.$$

Путь к решению этой весьма сложной задачи станет полегче, если вы докажете предварительно следующий факт.

Пусть $k > 1$ и заданы системы $x_1^{(1)}, x_2^{(1)}, \ldots, x_k^{(1)}$; $x_1^{(2)}, x_2^{(2)}, \ldots, x_k^{(2)}$; $\ldots$; $x_1^{(n)}, x_2^{(n)}, \ldots, x_k^{(n)}$ целых чисел, не равных одновременно нулю. Пусть, далее, для этих систем однозначно определена некоторая (произвольная) функция $f(x_1, x_2, \ldots, x_k)$. Тогда

$$S^{\nabla} = \sum \mu(d) S_d,$$

где μ — функция Мёбиуса, S^{∇} обозначает сумму значений $f(x_1, x_2, \ldots, x_k)$, распространенную на системы взаимно простых чисел, S_d обозначает сумму значений $f(x_1, x_2, \ldots, x_k)$, распространенную на системы чисел, одновременно кратных d, а d пробегает натуральные числа.

§ 4. ТЕОРИЯ СРАВНЕНИЙ

Эпиграфом к этому параграфу может послужить крылатая фраза «Все познается в сравнении!». В этом параграфе мы займемся изучением арифметики в кольцах вычетов — в объектах, хорошо знакомых еще из начального университетского курса алгебры. При этом мы будем пользоваться преимущественно терминологией и традиционными теоретико-числовыми обозначениями, нежели обозначениями и терминологией теории колец — такова традиция элементарного изложения этой теории для школьников десятого класса и студентов математико-механического факультета третьего и четвертого курсов. Эта традиция имеет железное обоснование: школьники понятия кольца еще не знают, студенты понятие кольца уже забыли. Но и те, и другие счастливы.

16. Определения и простейшие свойства

Определение. Пусть $a, b \in \mathbf{Z}$, $m \in \mathbf{N}$. Говорят, что число a *сравнимо* с b *по модулю* m, если a и b при делении на m дают одинаковые остатки. Запись этого факта выглядит так:

$$a \equiv b (\mathrm{mod}\, m).$$

Согласитесь, что вместо $a \equiv b (\mathrm{mod}\, m)$ гораздо удобнее было бы писать что-нибудь вроде $a \equiv_m b$, но «привычка свыше нам дана, замена счастию она».

Очевидно, что бинарное отношение сравнимости $\equiv_m$ (неважно, по какому модулю) есть отношение эквивалентности на множестве целых чисел, а любители алгебры скажут, что это отношение является даже конгруэнцией кольца $\mathbf{Z}$, фактор-кольцо по которой $\mathbf{Z} \equiv_m$ называется *кольцом вычетов* и обозначается $\mathbf{Z}_m$.

Ясно, что число a сравнимо с b по модулю m тогда и только тогда, когда $a - b$ делится на m нацело. Очевидно, это, в свою очередь, бывает тогда и только тогда, когда найдется такое целое число t, что $a = b + mt$. Знатоки алгебры добавят к этим

эквивалентным утверждениям, что сравнимость a с b по модулю m означает, что a и b представляют один и тот же элемент в кольце $\mathbf{Z}_m$.

Понять процесс собирания целых чисел в классы сравнимых между собой по модулю m (классы эквивалентности $\equiv_m$) мне помогла следующая картинка. На рис. 7 изображен процесс наматывания цепочки целых чисел на колечко с m делениями, при этом на одно деление автоматически попадают сравнимые между собой числа. Кстати, эта картинка неплохо объясняет и термин «кольцо».

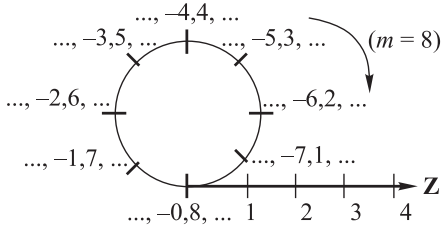


Рис. 7

Перечислим, далее, свойства сравнений, похожие на свойства отношения равенства.

Свойство 1. *Сравнения по одинаковому модулю можно почленно складывать.*

Доказательство. Пусть $a_1 \equiv b_1 (\mathrm{mod}\, m), a_2 \equiv b_2 (\mathrm{mod}\, m)$. Это означает, что $a_1 = b_1 + mt_1, a_2 = b_2 + mt_2$. После сложения последних двух равенств получим $a_1 + a_2 = b_1 + b_2 + m(t_1 + t_2)$, что означает $a_1 + a_2 \equiv b_1 + b_2 (\mathrm{mod}\ m)$. ♦

Свойство 2. *Слагаемое, стоящее в какой-либо части сравнения, можно переносить в другую часть, изменив его знак на обратный.*

Доказательство.

$$\begin{array}{l} \left\{ \begin{array}{l} a + b \equiv c (\mathrm{mod}\ m) \\ -b \equiv -b (\mathrm{mod}\ m) \end{array} \right. + \\ \hline a \equiv c - b (\mathrm{mod}\ m) \end{array}$$

♦

Свойство 3. *К любой части сравнения можно прибавить любое число, кратное модулю.*

Доказательство.

$$\frac{\begin{cases} a \equiv b(\mathrm{mod}\ m) \\ mk \equiv 0(\mathrm{mod}\ m) \end{cases} +}{a + mk \equiv b(\mathrm{mod}\ m)}$$

♦

Свойство 4. *Сравнения по одинаковому модулю можно почленно перемножать.*

Свойство 5. *Обе части сравнения можно возвести в одну и ту же степень.*

Доказательство.

$$\frac{\begin{cases} a_1 \equiv b_1(\mathrm{mod}\ m) \Leftrightarrow a_1 = b_1 + mt_1 \\ a_2 \equiv b_2(\mathrm{mod}\ m) \Leftrightarrow a_2 = b_2 + mt_2 \end{cases} \times}{a_1a_2 = b_1b_2 + m(b_1t_2 + b_2t_1 + mt_1t_2) \Rightarrow a_1a_2 \equiv b_1b_2(\mathrm{mod}\ m).}$$

♦

Как следствие из вышеперечисленных свойств, получаем

Свойство 6. *Если*

$$a_0 \equiv b_0(\mathrm{mod}\ m), \quad a_1 \equiv b_1(\mathrm{mod}\ m), \ldots, a_n \equiv b_n(\mathrm{mod}\ m), \quad x \equiv y(\mathrm{mod}\ m),$$

то

$$a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv b_0y^n + b_1y^{n-1} + \ldots + b_n(\mathrm{mod}\ m).$$

Свойство 7. *Обе части сравнения можно разделить на их общий делитель, взаимно простой с модулем.*

Доказательство. Пусть $a \equiv b(\mathrm{mod}\ m), a = a_1d, b = b_1d$. Тогда $(a_1 - b_1) \cdot d$ делится на m. Поскольку d и m взаимно просты, то на m делится именно $(a_1 - b_1)$, что означает $a_1 \equiv b_1(\mathrm{mod}\ m)$. ♦

Свойство 8. *Обе части сравнения и его модуль можно умножить на одно и то же целое число или разделить на их общий делитель.*

Доказательство.

$$a \equiv b(\mathrm{mod}\ m) \Leftrightarrow a = b + mt \Leftrightarrow ak = bk + mkt \Leftrightarrow$$
$$\Leftrightarrow ak \equiv bk(\mathrm{mod}\ mk).$$ ♦

Свойство 9. *Если сравнение $a \equiv b$ имеет место по нескольким разным модулям, то оно имеет место и по модулю, равному наименьшему общему кратному этих модулей.*

Доказательство. Если $a \equiv b(\mathrm{mod}\ m_1)$ и $a \equiv b(\mathrm{mod}\ m_2)$, то $a - b$ делится на m_1 и на m_2, значит, $a - b$ делится на наименьшее общее кратное m_1 и m_2. ♦

Свойство 10. *Если сравнение имеет место по модулю m, то оно имеет место и по модулю d, равному любому делителю числа m.*

Доказательство очевидно следует из транзитивности отношения делимости: если $a \equiv b(\mathrm{mod}\ m)$, то $a - b$ делится на m, значит, $a - b$ делится на d, где $d \,|\, m$. ♦

Свойство 11. *Если одна часть сравнения и модуль делятся на некоторое число, то и другая часть сравнения должна делиться на то же число.*

Доказательство. $a \equiv b(\mathrm{mod}\ m) \Leftrightarrow a = b + mt \ldots$. ♦

Теперь, чтобы с легким сердцем закончить этот пункт, осталось привести пример использования сформулированных выше свойств сравнений для решения стандратных задач.

Пример. Доказать, что при любом натуральном n число

$$37^{n+2} + 16^{n+1} + 23^n$$

делится на 7.

Решение. Очевидно, что

$$37 \equiv 2(\mathrm{mod}\,7), \quad 16 \equiv 2(\mathrm{mod}\,7), \quad 23 \equiv 2(\mathrm{mod}\,7).$$

Возведем первое сравнение в степень $n+2$, второе — в степень $n+1$, третье — в степень n и сложим:

$$\begin{array}{r} 37^{n+2} \equiv 2^{n+2}(\mathrm{mod}\,7) \\ +\ 16^{n+1} \equiv 2^{n+1}(\mathrm{mod}\,7) \\ 23^n \equiv 2^n(\mathrm{mod}\,7) \\ \hline 37^{n+2} + 16^{n+1} + 23^n \equiv 2^n \cdot 7(\mathrm{mod}\,7), \end{array}$$

т. е. $37^{n+2} + 16^{n+1} + 23^n$ делится на 7. Как видите, ровным счетом ничего сложного в решении подобных школьных задач «повышенной трудности» нет.

С удовольствием заканчиваю настоящий пункт, чтобы устремиться к следующему, т. е. устремиться из прошлого в будущее.

Задачки

1. Докажите, что $3^{105} + 4^{105}$ делится на 181.

2. Докажите, что число $5^{2n-1} \cdot 2^{n+1} + 3^{n+1} \cdot 2^{2n-1}$ при любом натуральном n делится на 19.

3. Найдите остаток от деления числа $(9674^6 + 28)^{15}$ на 39.

4. При делении натурального числа N на 3 и на 37 получаются, соответственно, остатки 1 и 33. Найдите остаток от деления N на 111.

5. Докажите, что при любых нечетных положительных значениях n число $S_m = 1^n + 2^n + 3^n + \ldots + m^n$ делится нацело на число $1 + 2 + 3 + \ldots + m$.

6. Докажите, что число $20^{15} - 1$ делится на $11 \cdot 31 \cdot 61$.

7. Докажите, что число $p^2 - q^2$, где p и q — простые числа, большие 3, делится на 24.

8. Докажите, что если натуральное число делится на 99, то сумма его цифр в десятичной записи не менее 18.

9. Докажите, что если при делении многочлена $M(x)$ с целыми коэффициентами на $x - a$ в частном получится $Q(x)$, а в остатке R, то $(1 - a)S(Q) = S(M) - R$, где через $S(A)$ обозначена сумма коэффициентов многочлена A.

10. Докажите, что ни при каких натуральных n и k, $k > 1$, число $3^{n^k} + 1$ не делится на 5.

17. Полная и приведенная системы вычетов

В предыдущем пункте было отмечено, что отношение $\equiv_m$ сравнимости по произвольному модулю m есть отношение эквивалентности на множестве целых чисел. Это отношение эквивалентности индуцирует разбиение множества целых чисел на классы эквивалентных между собой элементов, т. е. в один класс объединяются числа, дающие при делении на m одинаковые остатки. Число классов эквивалентности $\equiv_m$ (знатоки скажут — «индекс эквивалентности $\equiv_m$») в точности равно m.

Определение. Любое число из класса эквивалентности $\equiv_m$ будем называть *вычетом по модулю* m. Совокупность вычетов, взятых по одному из каждого класса эквивалентности $\equiv_m$, называется *полной системой вычетов по модулю* m (в полной системе вычетов, таким образом, всего m штук чисел). Непосредственно сами остатки при делении на m называются *наименьшими неотрицательными вычетами* и, конечно, образуют полную систему вычетов по модулю m. Вычет ρ называется

абсолютно наименьшим, если $|\rho|$ наименьший среди модулей вычетов данного класса.

Пример. Пусть $m = 5$. Тогда

$0, 1, 2, 3, 4$ — наименьшие неотрицательные вычеты;
$-2, -1, 0, 1, 2$ — абсолютно наименьшие вычеты.

Обе приведенные совокупности чисел образуют полные системы вычетов по модулю **5**.

Лемма 1. 1). *Любые m штук попарно несравнимых по модулю m чисел образуют полную систему вычетов по модулю m.*

2). *Если a и m взаимно просты, а x пробегает полную систему вычетов по модулю m, то значения линейной формы $ax + b$, где b — любое целое число, тоже пробегают полную систему вычетов по модулю m.*

Доказательство. Утверждение 1) очевидно. Докажем утверждение 2). Чисел $ax + b$ ровно m штук. Покажем, что они между собой не сравнимы по модулю m. Пусть для некоторых различных x_1 и x_2 из полной системы вычетов оказалось, что $ax_1 + b \equiv ax_2 + b (\mathrm{mod}\ m)$. Тогда, по свойствам сравнений из предыдущего пункта, получаем

$$ax_1 \equiv ax_2 (\mathrm{mod}\ m),$$
$$x_1 \equiv x_2 (\mathrm{mod}\ m)$$

— противоречие с тем, что x_1 и x_2 различны и взяты из полной системы вычетов. ♦

Поскольку все числа из данного класса эквивалентности $\equiv_m$ получаются из одного числа данного класса прибавлением числа, кратного m, то все числа из данного класса имеют с модулем m один и тот же наибольший общий делитель. По некоторым соображениям, повышенный интерес представляют те вычеты, которые имеют с модулем m наибольший общий делитель, равный единице, т. е. вычеты, которые взаимно просты с модулем.

Определение. *Приведенной системой вычетов по модулю m* называется совокупность всех вычетов из полной системы, взаимно простых с модулем m.

Приведенную систему обычно выбирают из наименьших неотрицательных вычетов. Ясно, что приведенная система вычетов по

модулю m содержит $\varphi(m)$ штук вычетов, где $\varphi(m)$ — функция Эйлера — число чисел, меньших m и взаимно простых с m. Если к этому моменту вы уже забыли функцию Эйлера, загляните в п. 14 и убедитесь, что про нее там кое-что говорилось.

Пример. Пусть $m = 42$. Тогда приведенная система вычетов суть:

$$1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41.$$

Лемма 2. 1). *Любые $\varphi(m)$ чисел, попарно не сравнимые по модулю m и взаимно простые с модулем, образуют приведенную систему вычетов по модулю m.*

2). *Если $(a, m) = 1$ и x пробегает приведенную систему вычетов по модулю m, то $a \cdot x$ так же пробегает приведенную систему вычетов по модулю m.*

Доказательство. Утверждение 1) — очевидно. Докажем утверждение 2). Числа ax попарно несравнимы (это доказывается так же, как в лемме 1 этого пункта), их ровно $\varphi(m)$ штук. Ясно также, что все они взаимно просты с модулем, ибо $(a, m) = 1, (x, m) = 1 \Rightarrow (ax, m) = 1$. Значит, числа ax образуют приведенную систему вычетов. ♦

Таковы определения и основные свойства полной и приведенной систем вычетов, однако в багаже математических знаний существует еще целый ряд очень интересных и полезных фактов, касающихся систем вычетов. Кроме того, без знакомства с дальнейшими важными свойствами систем вычетов п. 17 получится весьма куцым. Продолжим.

Лемма 3. *Пусть $m_1, m_2, \ldots, m_k$ — попарно взаимно просты и*

$$m_1 m_2 \cdot \ldots \cdot m_k = M_1 m_1 = M_2 m_2 = \ldots = M_k m_k,$$

где $M_j = m_1 \cdot \ldots \cdot m_{j-1} m_{j+1} \cdot \ldots \cdot m_k$.

1). *Если $x_1, x_2, \ldots, x_k$ пробегают полные системы вычетов по модулям $m_1, m_2, \ldots, m_k$ соответственно, то значения линейной формы $M_1 x_1 + M_2 x_2 + \ldots + M_k x_k$ пробегают полную систему вычетов по модулю $m = m_1 m_2 \cdot \ldots \cdot m_k$.*

2). *Если $\xi_1, \xi_2, \ldots, \xi_k$ пробегают приведенные системы вычетов по модулям $m_1, m_2, \ldots, m_k$ соответственно, то значения линейной формы $M_1 \xi_1 + M_2 \xi_2 + \ldots + M_k \xi_k$ пробегают приведенную систему вычетов по модулю $m = m_1 m_2 \cdot \ldots \cdot m_k$.*

Доказательство. 1). Форма $M_1x_1 + M_2x_2 + \ldots + M_kx_k$ принимает, очевидно, $m_1m_2 \cdot \ldots \cdot m_k = m$ значений. Покажем, что эти значения попарно несравнимы. Пусть

$$M_1x_1 + M_2x_2 + \ldots + M_kx_k \equiv M_1x_1^{\nabla} + M_2x_2^{\nabla} + \ldots + M_kx_k^{\nabla} (\mathrm{mod}\ m).$$

Всякое M_j, отличное от M_s, кратно m_s. Убирая слева и справа в последнем сравнении слагаемые, кратные m_s, получим

$$M_sx_s \equiv M_sx_s^{\nabla} (\mathrm{mod}\ m_s) \Rightarrow x_s \equiv x_s^{\nabla} (\mathrm{mod}\ m_s)$$

— противоречие с тем, что x_s пробегает полную систему вычетов по модулю m_s.

2). Форма $M_1\xi_1 + M_2\xi_2 + \ldots + M_k\xi_k$ принимает, очевидно, $\varphi(m_1)\varphi(m_2) \cdot \ldots \cdot \varphi(m_k) = \varphi(m_1m_2 \cdot \ldots \cdot m_k) = \varphi(m)$ (функция Эйлера мультипликативна!) различных значений, которые между собой по модулю $m = m_1m_2 \cdot \ldots \cdot m_k$ попарно несравнимы. Последнее легко доказывается рассуждениями, аналогичными рассуждениям, проведенным при доказательстве утверждения 1) этой леммы. Так как

$$(M_1\xi_1 + M_2\xi_2 + \ldots + M_k\xi_k, m_s) = (M_s\xi_s, m_s) = 1$$

для каждого $1 \leqslant s \leqslant k$, то $(M_1\xi_1 + M_2\xi_2 + \ldots + M_k\xi_k, m) = 1$, следовательно множество значений формы $M_1\xi_1 + M_2\xi_2 + \ldots + M_k\xi_k$ образует приведенную систему вычетов по модулю m. ♦

Лемма 4. *Пусть $x_1, x_2, \ldots, x_k, x$ пробегают полные, а $\xi_1, \xi_2, \ldots, \xi_k, \xi$ пробегают приведенные системы вычетов по модулям $m_1, m_2, \ldots, m_k$ и $m = m_1m_2 \cdot \ldots \cdot m_k$ соответственно, где $(m_i, m_j) = 1$ при $i \neq j$. Тогда дроби*

$$\left\{\frac{x_1}{m_1} + \frac{x_2}{m_2} + \ldots + \frac{x_k}{m_k}\right\} \quad \textit{совпадают с дробями} \quad \left\{\frac{x}{m}\right\},$$

а дроби

$$\left\{\frac{\xi_1}{m_1} + \frac{\xi_2}{m_2} + \ldots + \frac{\xi_k}{m_k}\right\} \quad \textit{совпадают с дробями} \quad \left\{\frac{\xi}{m}\right\}.$$

Доказательство обоих утверждений леммы 4 легко получается применением предыдущей леммы 3 после того, как вы приведете каждую сумму

$$\left\{\frac{x_1}{m_1} + \frac{x_2}{m_2} + \ldots + \frac{x_k}{m_k}\right\} \text{ и } \left\{\frac{\xi_1}{m_1} + \frac{\xi_2}{m_2} + \ldots + \frac{\xi_k}{m_k}\right\}$$

к общему знаменателю:

$$\left\{\frac{x_1}{m_1}+\frac{x_2}{m_2}+\ldots+\frac{x_k}{m_k}\right\}=\left\{\frac{M_1x_1+M_2x_2+\ldots+M_kx_k}{m}\right\},$$

$$\left\{\frac{\xi_1}{m_1}+\frac{\xi_2}{m_2}+\ldots+\frac{\xi_k}{m_k}\right\}=\left\{\frac{M_1\xi_1+M_2\xi_2+\ldots+M_k\xi_k}{m}\right\},$$

где $M_j=m_1\ldots m_{j-1}m_{j+1}\ldots m_k$. Если теперь принять во внимание, что дробные части чисел, получающихся при делении на модуль m любых двух чисел, сравнимых по модулю m, одинаковы (они равны $\frac{r}{m}$, где r — наименьший неотрицательный вычет из данного класса), то утверждения настоящей леммы становятся очевидными. ♦

В оставшейся части этого пункта произойдет самое интересное — мы будем суммировать комплексные корни m-й степени из единицы, при этом нам откроются поразительные связи между суммами корней, системами вычетов и уже знакомой мультипликативной функцией Мёбиуса $\mu(m)$.

Обозначим через ε_k k-й корень m-й степени из единицы:

$$\varepsilon_k=\cos\frac{2\pi k}{m}+i\sin\frac{2\pi k}{m}=e^{i\frac{2\pi k}{m}}$$

— эти формы записи комплексных чисел мы хорошо помним с первого курса. Здесь $k=0,1,\ldots,m-1$ — пробегает полную систему вычетов по модулю m.

Напомню, что сумма $\varepsilon_0+\varepsilon_1+\ldots+\varepsilon_{m-1}$ всех корней m-й степени из единицы равна нулю для любого m. Действительно, пусть $\varepsilon_0+\varepsilon_1+\ldots+\varepsilon_{m-1}=a$. Умножим эту сумму на ненулевое число ε_1. Такое умножение геометрически в комплексной плоскости означает поворот правильного m-угольника, в вершинах которого расположены корни $\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{m-1}$, на ненулевой угол $\frac{2\pi}{m}$. Ясно, что при этом корень ε_0 перейдет в корень ε_1, корень ε_1 перейдет в корень ε_2, и т. д., а корень ε_{m-1} перейдет в корень ε_0, т. е. сумма $\varepsilon_0+\varepsilon_1+\ldots+\varepsilon_{m-1}$ не изменится. Имеем $\varepsilon_1a=a$, откуда $a=0$.

Теорема 1. *Пусть $m>0$ — целое число, $a\in\mathbf{Z}$, x пробегает полную систему вычетов по модулю m. Тогда, если a кратно m, то*

$$\sum_x e^{2\pi i\frac{ax}{m}}=m;$$

в противном случае, при a, не кратном m,

$$\sum_x e^{2\pi i \frac{ax}{m}} = 0.$$

Доказательство. При a, кратном m, имеем $a = md$ и

$$\sum_x e^{2\pi i \frac{ax}{m}} = \sum_x (\cos(2\pi dx) + i \sin(2\pi dx)) = \sum_x 1 = m.$$

При a, не делящемся на m, разделим числитель и знаменатель дроби $\frac{a}{m}$ на d — наибольший общий делитель a и m, получим несократимую дробь $\frac{a_1}{m_1}$. Тогда, по лемме 1, $a_1 x$ будет пробегать полную систему вычетов по модулю m. Имеем

$$\sum_x e^{2\pi i \frac{ax}{m}} = \sum_x e^{2\pi i \frac{a_1 x}{m_1}} = d \sum_{k=0}^{m_1-1} \left(\cos\left(\frac{2\pi k}{m_1}\right) + i \sin\left(\frac{2\pi k}{m_1}\right)\right) = 0,$$

ибо сумма всех корней степени m_1 из единицы равна нулю. ♦

Напомню, что корень ε_k m-й степени из единицы называется первообразным, если его индекс k взаимно прост с m. В этом случае, как доказывалось на первом курсе, последовательные степени $\varepsilon_k^1, \varepsilon_k^2, \ldots, \varepsilon_k^{m-1}$ корня ε_k образуют всю совокупность корней m-й степени из единицы или, другими словами, ε_k является порождающим элементом циклической группы всех корней m-й степени из единицы.

Очевидно, что число различных первообразных корней m-й степени из единицы равно $\varphi(m)$, где φ — функция Эйлера, так как индексы у первообразных корней образуют приведенную систему вычетов по модулю m.

Теорема 2. *Пусть $m > 0$ — целое число, ξ пробегает приведенную систему вычетов по модулю m. Тогда* (*сумма первообразных корней степени m*):

$$\sum_\xi e^{2\pi i \frac{\xi}{m}} = \mu(m),$$

где $\mu(m)$ — функция Мёбиуса.

Доказательство. Пусть $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ — каноническое разложение числа m; $m_1 = p_1^{\alpha_1}, m_2 = p_2^{\alpha_2}, \ldots, m_k = p_k^{\alpha_k}$; ξ_i пробегает приведенную систему вычетов по модулю m_i. Имеем

$$\sum_{\xi_1} e^{2\pi i \frac{\xi_1}{m_1}} \cdot \sum_{\xi_2} e^{2\pi i \frac{\xi_2}{m_2}} \cdot \ldots \cdot \sum_{\xi_k} e^{2\pi i \frac{\xi_k}{m_k}} =$$

$$= \sum_{\xi_1, \xi_2, \ldots, \xi_k} e^{2\pi i \left(\frac{\xi_1}{m_1} + \frac{\xi_2}{m_2} + \ldots + \frac{\xi_k}{m_k} \right)} =$$

$$= \sum_{\xi_1, \xi_2, \ldots, \xi_k} e^{2\pi i \frac{\xi_1 M_1 + \xi_2 M_2 + \ldots + \xi_k M_k}{m}} = \sum_{\xi} e^{2\pi i \frac{\xi}{m}}.$$

При $\alpha_s = 1$ получается, что только корень $\varepsilon_0 = 1$ не является первообразным, поэтому сумма всех первообразных корней есть сумма всех корней минус единица:

$$\sum_{\xi_s} e^{2\pi i \frac{\xi_s}{m_s}} = \sum_{x_s} e^{2\pi i \frac{x_s}{m_s}} - 1 = -1,$$

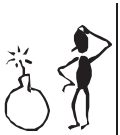
стало быть, если m свободно от квадратов (т. е. не делится на r^2, при $r > 1$), то

$$\sum_{\xi} e^{2\pi i \frac{\xi}{m}} = (-1)^k = \mu(m).$$

Если же какой-нибудь показатель α_s больше единицы (т. е. m делится на r^2, при $r > 1$), то сумма всех первообразных корней степени m_s есть сумма всех корней степени m_s минус сумма всех не первообразных корней, т. е. всех корней некоторой степени, меньшей m_s. Именно, если $m_s = p_s m_s^*$, то

$$\sum_{\xi_s} e^{2\pi i \frac{\xi_s}{m_s}} = \sum_{x_s} e^{2\pi i \frac{x_s}{m_s}} - \sum_{u=0}^{m_s^* - 1} e^{2\pi i \frac{u}{m_s^*}} = 0 - 0 = 0. \qquad \blacklozenge$$

Задачки



1. Выпишите на листочке все наименьшие неотрицательные вычеты и все абсолютно наименьшие вычеты:
а) по модулю 6, б) по модулю 8.
Чуть ниже выпишите приведенные системы вычетов по этим модулям. Нарисуйте отдельно на комплексной плоскости корни шестой и корни восьмой степеней из единицы, на обоих рисунках обведите кружочком первообразные корни и найдите в каждом случае их сумму.

2. Пусть ε — первообразный корень степени $2n$ из единицы. Найдите сумму $1+\varepsilon+\varepsilon^2+\ldots+\varepsilon^{n-1}$.

3. Найдите сумму всех первообразных корней: а) 15-й; б) 24-й; в) 30-й степени из единицы.

4. Найдите сумму всевозможных произведений первообразных корней n-й степени из единицы, взятых по два.

5. Найдите сумму k-х степеней всех корней n-й степени из единицы.

6. Пусть $m>1$, $(a,m)=1$, b — целое число, x пробегает полную, а ξ — приведенную систему вычетов по модулю m. Докажите, что:

$$\text{а)}\ \sum_x \left\{\frac{ax+b}{m}\right\}=\frac{1}{2}(m-1);\quad \text{б)}\ \sum_\xi \left\{\frac{a\xi}{m}\right\}=\frac{1}{2}\varphi(m).$$

7. Докажите, что:

$$\varphi(a)=\sum_{n=0}^{a-1}\prod_p\left(1-\frac{1}{p}\sum_{l=0}^{p-1}e^{2\pi i\frac{nl}{p}}\right),$$

где p пробегает все простые делители числа a.

18. Теорема Эйлера и теорема Ферма

В этом пункте я расскажу две знаменитые теоремы теории чисел и приведу несколько показательных примеров их удивительной работоспособности, проявляющейся при решении специфических школьных «олимпиадных» задач. Первая теорема этого пункта носит имя Леонарда Эйлера и, как мне кажется, настал черед небольшого исторического отступления об этом великом математике.

Небольшое эссе про Эйлера

Леонард Эйлер (1707–1783) — самомый плодовитый математик восемнадцатого столетия, если только не всех времен. Опубликовано более двухсот томов его научных трудов, но это еще далеко не полное собрание сочинений. От такой напряженной работы Эйлер ослеп в 1735 г. на один глаз, а в 1766 г. — на второй, но слепота не смогла ослабить его огромную продуктивность.

Как ученый, Эйлер сформировался в швейцарском городе Базеле, университет которого долгое время был средоточием европейской науки того времени. Леонард изучал математику под руководством Иоганна Бернулли, а когда в 1725 г. сын Иоганна Николай уехал в

Петербург, молодой Эйлер последовал за ним в недавно учрежденную Российскую (Петербургскую) Академию наук. Эйлер жил в России до 1741 г., потом переехал в Берлинскую академию под особое покровительство Фридриха Второго, а с 1766 г. до самой своей физической смерти он — снова в России. Мне кажется, что Эйлера с полным правом можно считать российским ученым, ибо основные годы его творчества прошли в Петербурге и он являлся академиком именно Петербургской Академии наук под особым покровительством Екатерины Великой.

Слепой Эйлер, пользуясь своей феноменальной памятью, диктовал свои работы, общее число которых достигло 886. Его работы посвящены анализу, алгебре, дискретной математике (теории графов), вариационному исчислению, функциям комплексного переменного, астрономии, гидравлике, теоретической механике, кораблестроению, артиллерии, теории музыки и т. д., и т. п. Колоссальная продуктивность и «пробивная сила» Эйлера в разных областях математики и нематематики была и остается поводом для изумления. А какое изящество! Возьмите известную книжку Д. Пойа «Математика и правдоподобные рассуждения» и прочитайте там, как Эйлер находил сумму ряда

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \dots ,$$

и вы испытаете чисто эстетическое наслаждение. Обозначения Эйлера почти современны, точнее сказать, что наша математическая символика почти эйлерова. Можно составить длиннющий список известных и важных математических открытий, приоритет в которых принадлежит Эйлеру. Можно составить огромный перечень его идей, которые еще ждут своей разработки. «Читайте Эйлера, — обычно говорил молодым математикам Лаплас, — читайте Эйлера, это наш общий учитель». Гаусс выразился еще более определенно: «Изучение работ Эйлера остается наилучшей школой в различных областях математики, и ничто другое не может это заменить».

Но давайте вернемся к математике.

Теорема (Эйлер). *Пусть* $m > 1$, $(a, m) = 1$, $\varphi(m)$ — *функция Эйлера. Тогда*

$$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\ m).$$

Доказательство. Пусть x пробегает приведенную систему вычетов по mod m:

$$x = r_1, r_2, \dots, r_c,$$

где $c = \varphi(m)$ — их число, $r_1, r_2, \dots, r_c$ — наименьшие неотрицательные вычеты по mod m. Следовательно, наименьшие неот-

рицательные вычеты, соответствующие числам ax, суть соответственно

$$\rho_1, \rho_2, \ldots, \rho_c$$

— тоже пробегают приведенную систему вычетов, но в другом порядке (см. лемму 2 из п. 17). Значит,

$$\begin{aligned} a \cdot r_1 &\equiv \rho_{j_1} (\mathrm{mod}\ m), \\ a \cdot r_2 &\equiv \rho_{j_2} (\mathrm{mod}\ m), \\ &\vdots \\ a \cdot r_c &\equiv \rho_{j_c} (\mathrm{mod}\ m). \end{aligned}$$

Перемножим эти c штук сравнений. Получится

$$a^c r_1 r_2 \cdot \ldots \cdot r_c \equiv \rho_1 \rho_2 \cdot \ldots \cdot \rho_c (\mathrm{mod}\ m).$$

Так как $r_1 r_2 \cdot \ldots \cdot r_c = \rho_1 \rho_2 \cdot \ldots \cdot \rho_c \neq 0$ и **взаимно просто с модулем** m, то, поделив последнее сравнение на $r_1 r_2 \ldots r_c$, получим $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\ m)$. ♦

Вторая теорема этого пункта — теорема Ферма — является непосредственным следствием теоремы Эйлера (конечно, при схеме изложения материала, принятой в этой книжке).

Теорема (Ферма). *Пусть p — простое число, p не делит a. Тогда*

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p).$$

Доказательство 1 теоремы Ферма. Положим в условии теоремы Эйлера $m = p$, тогда $\varphi(m) = p - 1$ (см. п. 14). Получаем $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$. ♦

Необходимо отметить важность условия взаимной простоты модуля и числа a в формулировках теорем Эйлера и Ферма. Простой пример: сравнение $6^2 \equiv 1 (\mathrm{mod}\, 3)$ очевидно не выполняется. Однако можно легко подправить формулировку теоремы Ферма, чтобы снять ограничение взаимной простоты.

Следствие 1. *Без всяких ограничений на $a \in \mathbf{Z}$ верно*

$$a^p \equiv a (\mathrm{mod}\, p).$$

Доказательство. Умножим обе части сравнения $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$ на a. Ясно, что получится сравнение, справедливое и при a, кратном p. ♦

Конечно, доказательство 1 теоремы Ферма получилось столь коротким благодаря проведенной мощной предварительной подготовке (доказана теорема Эйлера и изучены свойства функции $\varphi(m)$). Но многие читатели этой книжки очень скоро будут преподавать математику в средней школе, а некоторые, может быть, уже сейчас занимаются этой благородной деятельностью. Поэтому я не могу удержаться и приведу здесь еще один изящный вариант доказательства теоремы Ферма, доступный среднему школьнику или, по крайней мере, школьнику из школы с углубленным изучением математики.

Доказательство 2 теоремы Ферма. Так как p — простое число, то все биномиальные коэффициенты

$$C_p^k = \frac{p(p-1)(p-2)\cdot\ldots\cdot(p-k+1)}{1\cdot 2\cdot 3\cdot\ldots\cdot k}$$

(кроме C_p^0 и C_p^p) делятся на p, ибо числитель выписанного выражения содержит p, а знаменатель не содержит этого множителя. Если вспомнить бином Ньютона, то становится понятно, что разность $(A+B)^p - A^p - B^p = C_p^1 A^{p-1}B^1 + C_p^2 A^{p-2}B^2 + \ldots + C_p^{p-2}A^2B^{p-2} + C_p^{p-1}A^1B^{p-1}$, где A и B — какие угодно целые числа, всегда делится на p. Последовательным применением этого незатейливого наблюдения получаем, что $(A+B+C)^p - A^p - B^p - C^p = \{[(A+B)+C]^p - (A+B)^p - C^p\} + (A+B)^p - A^p - B^p$ всегда делится на p; $(A+B+C+D)^p - A^p - B^p - C^p - D^p$ всегда делится на p; и вообще, $(A+B+C+\ldots+K)^p - A^p - B^p - C^p - \ldots - K^p$ всегда делится на p. Положим теперь в последнем выражении $A = B = C = \ldots = K = 1$ и возьмем количество этих чисел равным a. Получится, что $a^p - a$ делится на p, а это и есть теорема Ферма в более общей формулировке. ♦

Следствие 2. $(a+b)^p \equiv a^p + b^p \pmod p$. ♦

Приведу теперь почти без комментариев несколько обещанных примеров применения теорем Ферма и Эйлера. Отмечу сразу, что эффективность применения теорем Ферма и Эйлера отчасти основывается на том, что сравнения, даваемые этими теоремами, удобно возводить в степень, так как справа в них стоит единица, которая на возведение в степень не реагирует.

Пример 1. Девятая степень однозначного числа оканчивается на 7. Найти это число.

Решение. $a^9 \equiv 7 (\mathrm{mod}\, 10)$ — это дано. Кроме того, очевидно, что $(7, 10) = 1$ и $(a, 10) = 1$. По теореме Эйлера, $a^{\varphi(10)} \equiv \equiv 1 (\mathrm{mod}\, 10)$. Следовательно, $a^4 \equiv 1 (\mathrm{mod}\, 10)$ и, после возведения в квадрат, $a^8 \equiv 1 (\mathrm{mod}\, 10)$. Поделим почленно $a^9 \equiv 7 (\mathrm{mod}\, 10)$ на $a^8 \equiv 1 (\mathrm{mod}\, 10)$ и получим $a \equiv 7 (\mathrm{mod}\, 10)$. Это означает, что $a = 7$.

Пример 2. Доказать, что $1^{18} + 2^{18} + 3^{18} + 4^{18} + 5^{18} + 6^{18} \equiv \equiv -1 (\mathrm{mod}\, 7)$.

Доказательство. Числа 1, 2, 3, 4, 5, 6 взаимно просты с 7. По теореме Ферма имеем

$$\begin{cases} 1^6 \equiv 1 (\mathrm{mod}\, 7), \\ 2^6 \equiv 1 (\mathrm{mod}\, 7), \\ \qquad \vdots \\ 6^6 \equiv 1 (\mathrm{mod}\, 7). \end{cases}$$

Возведем эти сравнения в куб и сложим:

$$1^{18} + 2^{18} + 3^{18} + 4^{18} + 5^{18} + 6^{18} \equiv 6 (\mathrm{mod}\, 7) \equiv -1 (\mathrm{mod}\, 7).$$

Пример 3. Найти остаток от деления 7^{402} на 101.

Решение. Число 101 — простое, $(7, 101) = 1$, следовательно, по теореме Ферма: $7^{100} \equiv 1 (\mathrm{mod}\, 101)$. Возведем это сравнение в четвертую степень: $7^{400} \equiv 1 (\mathrm{mod}\, 101)$, домножим его на очевидное сравнение $7^2 \equiv 49 (\mathrm{mod}\, 101)$, получим $7^{402} \equiv 49 (\mathrm{mod}\, 101)$. Значит, остаток от деления 7^{402} на 101 равен 49.

Пример 4. Найти две последние цифры числа 243^{402}.

Решение. Две последние цифры этого числа суть остаток от деления его на 100. Имеем: $243 = 200 + 43$; $200 + \\ + 43 \equiv 43 (\mathrm{mod}\, 100)$ и, возведя последнее очевидное сравнение в 402-ю степень, раскроем его левую часть по биному Ньютона (мысленно, конечно). В этом гигантском выражении все слагаемые, кроме последнего, содержат степень числа 200, т. е. делятся на 100, поэтому их можно выкинуть из сравнения, после чего понятно, почему $243^{402} \equiv 43^{402} (\mathrm{mod}\, 100)$. Далее, 43 и 100 взаимно просты, значит, по теореме Эйлера, $43^{\varphi(100)} \equiv 1 (\mathrm{mod}\, 100)$. Считаем:

$$\varphi(100) = \varphi(2^2 \cdot 5^2) = (10 - 5)(10 - 2) = 40.$$

Имеем сравнение: $43^{40} \equiv 1 (\mathrm{mod}\, 100)$, которое немедленно возведем в десятую степень и умножим почленно на очевидное сравнение, проверенное на калькуляторе: $43^2 \equiv 49 (\mathrm{mod}\, 100)$. Получим

$$\begin{array}{rl} & 43^{400} \equiv 1 (\mathrm{mod}\, 100) \\ \times & 43^{2} \equiv 49 (\mathrm{mod}\, 100) \\ \hline & 43^{402} \equiv 49 (\mathrm{mod}\, 100), \end{array}$$

следовательно, две последние цифры числа 243^{402} суть 4 и 9 .

Пример 5. Доказать, что $(73^{12} - 1)$ делится на 105.

Решение. Имеем: $105 = 3 \cdot 5 \cdot 7, (73, 3) = (73, 5) = (73, 7) = 1$. По теореме Ферма:

$$73^2 \equiv 1 (\mathrm{mod}\, 3),$$
$$73^4 \equiv 1 (\mathrm{mod}\, 5),$$
$$73^6 \equiv 1 (\mathrm{mod}\, 7).$$

Перемножая, получаем $73^{12} \equiv 1 (\mathrm{mod}\, 3), (\mathrm{mod}\, 5), (\mathrm{mod}\, 7)$, откуда, по свойствам сравнений, изложенным в пункте 16, немедленно следует

$$73^{12} - 1 \equiv 0 (\mathrm{mod}\, 105),$$

ибо 105 — наименьшее общее кратное чисел 3, 5 и 7. Именно это и требовалось.

Читатель, безусловно, понимает, что подобных примеров использования теорем Эйлера и Ферма можно придумать великое множество, да их и придумано великое множество для разнообразных школьных и студенческих математических олимпиад. Мы, естественно, не будем далее продолжать усердствовать, ибо, как сказал Козьма Прутков: «Усердствуя в малом, можешь оказаться неспособным к великому». Впереди нас ждут великие дела, поэтому на этом п. 18 закончим.

Задачки

1. Докажите, что мультипликативная группа кольца вычетов $\mathbf{Z}_n$, где $n = p_1^{m_1} p_2^{m_2} \cdot \ldots \cdot p_r^{m_r}$, является прямым произведением мультипликативных групп колец вычетов по модулям $p_1^{m_1}, p_2^{m_2}, \ldots, p_r^{m_r}$.

Чтобы окончательно понять строение мультипликативной группы кольца $\mathbf{Z}_n$, докажите, что:

а) если p — нечетное простое число, то мультипликативная группа кольца $\mathbf{Z}_{p^m}$ циклическая;

б) мультипликативные группы колец $\mathbf{Z}_2$ и $\mathbf{Z}_4$ есть циклические порядков 1 и 2 соответственно, в то время как мультипликативная группа кольца $Z_{2^m}, m \geqslant 3$, — прямое произведение циклической группы порядка 2^{m-2} и циклической группы порядка 2.

2. Докажите, что:
а) $13^{176} - 1$ делится на 89; б) $52^{60} - 1$ делится на 385.

3. Докажите, что $3^{100} - 3^{60} - 3^{40} + 1$ делится на 77.

4. Докажите, что:
а) $1^{19} + 2^{19} + 4^{19} + 5^{19} + 7^{19} + 8^{19} \equiv 0 (\mathrm{mod}\, 9)$;
б) $1^{14} + 3^{14} + 7^{14} + 9^{14} \equiv 0 (\mathrm{mod}\, 10)$.

5. Найдите две последние цифры десятичной записи числа:
а) 19^{321}; б) 131^{161}.

6. Найдите остаток от деления:
а) числа $3^{200} + 7^{200}$ на 101; б) числа $7^{65} + 11^{65}$ на 80.

7. Докажите, что существует такая степень числа 2, все последние 1000 цифр которой в десятичной записи будут единицами и двойками.

8. Пусть $a, a + d, a + 2d, \ldots$ — произвольная бесконечная арифметическая прогрессия, первый член и разность которой являются натуральными числами. Докажите, что эта прогрессия содержит бесконечно много членов, каноническое разложение которых состоит из одних и тех же простых чисел (взятых, разумеется, в разных степенях).

9. Выведите теорему Эйлера из теоремы Ферма.

Вступление к следующим трем пунктам

В следующих трех довольно скучноватых пунктах мы с вами будем рассматривать и учиться решать сравнения с одним неизвестным вида

$$f(x) \equiv 0 (\mathrm{mod}\ m),$$

где $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$ — многочлен с целыми коэффициентами. Если m не делит a_0, то говорят, что n — *степень сравнения*. Ясно, что если какое-нибудь число x подходит в сравнение, то в это же сравнение подойдет и любое другое число, сравнимое с x по $\mathrm{mod}\ m$. Запомните хорошенько (спрошу на экзамене!):

Решить сравнение — значит, найти все те x, которые удовлетворяют данному сравнению, при этом весь класс чисел по $\mathrm{mod}\ m$ *считается за одно решение.*

Таким образом, число решений сравнения есть число вычетов из полной системы, которые этому сравнению удовлетворяют.

Пример. Дано сравнение: $x^5 + x + 1 \equiv 0 (\mathrm{mod}\, 7)$.

Из чисел: 0, 1, 2, 3, 4, 5, 6, этому сравнению удовлетворяют два: $x_1 = 2; x_2 = 4$. Это означает, что у данного сравнения **два решения**:

$$x \equiv 2 (\mathrm{mod}\, 7) \ \text{ и } \ x \equiv 4 (\mathrm{mod}\, 7).$$

Сравнения называются равносильными, если они имеют одинаковые решения — полная аналогия с понятием равносильности уравнений. Однако (забегая вперед, открою приятный секрет), в отличие от алгебраических уравнений, которые частенько неразрешимы в радикалах, сравнение любой степени всегда решается, хотя бы, например, перебором всех вычетов по $\mathrm{mod}\ m$. Правда, перебор и подстановка всех вычетов — зачастую весьма долгий процесс (особенно, при больших m и n), но и здесь математики придумали хитроумные наборы инструкций, исполняя которые можно всегда найти все решения данного сравнения любой степени, минуя нудный процесс перебора.

19. Сравнения первой степени

В этом пункте детально рассмотрим только сравнения первой степени вида

$$ax \equiv b (\mathrm{mod}\ m),$$

оставив более высокие степени на съедение следующим пунктам. Как решать такое сравнение? Рассмотрим два случая.

Случай 1. Пусть a и m взаимно просты. Тогда несократимая дробь $\dfrac{m}{a}$ сама просится разложиться в цепную дробь:

$$\frac{m}{a} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots \cfrac{\ddots}{q_{n-1} + \cfrac{1}{q_n}}}}}.$$

Эта цепная дробь, разумеется, конечна, так как $\dfrac{m}{a}$ — рациональное число. Рассмотрим две ее последние подходящие дроби:

$$\delta_{n-1} = \frac{P_{n-1}}{Q_{n-1}}; \quad \delta_n = \frac{P_n}{Q_n} = \frac{m}{a}.$$

Вспоминаем (п. 9) важное свойство числителей и знаменателей подходящих дробей: $mQ_{n-1} - aP_{n-1} = (-1)^n$. Далее (слагаемое mO_{n-1}, кратное m, можно выкинуть из левой части сравнения):

$$-aP_{n-1} \equiv (-1)^n (\mathrm{mod}\ m),$$

т. е.

$$aP_{n-1} \equiv (-1)^{n-1} (\mathrm{mod}\ m),$$

т. е.

$$a\left[(-1)^{n-1} P_{n-1} b\right] \equiv b (\mathrm{mod}\ m),$$

и единственное решение исходного сравнения есть

$$x \equiv (-1)^{n-1} P_{n-1} b (\mathrm{mod}\ m). \quad \blacklozenge$$

Пример. Решить сравнение $111x \equiv 75 (\mathrm{mod}\, 322)$.

Р е ш е н и е. $(111, 322) = 1$. Включаем алгоритм Евклида:

$$\begin{aligned} 32 &= 11 \cdot \underline{2} + 100, \\ 111 &= 100 \cdot \underline{1} + 11, \\ 100 &= 11 \cdot \underline{9} + 1, \\ 11 &= 1 \cdot \underline{11}. \end{aligned}$$

(В равенствах подчеркнуты неполные частные.) Значит, $n = 4$, а соответствующая цепная дробь такова:

$$\frac{m}{a} = \frac{322}{111} = 2 + \cfrac{1}{1 + \cfrac{1}{9 + \cfrac{1}{11}}}.$$

Посчитаем числители подходящих дробей, составив для этого стандартную таблицу:

q_n	0	2	1	9	11
P_n	1	2	3	29	322

Числитель предпоследней подходящей дроби равен 29, следовательно, готовая формула дает ответ: $x \equiv (-1)^3 \cdot 29 \cdot 75 \equiv -2175 \equiv 79 (\mathrm{mod}\, 322)$. $\blacklozenge$

Ох, уж эти мне теоретико-числовые рассуждения из разных учебников, продиктованные традицией изложения и необходимостью обя-

зательно использовать ранее изложенную теорию! О чем идет речь в нескольких строках выше? Дано сравнение $ax \equiv b(\mathrm{mod}\ m)$, где a и m взаимно просты. Ну, возьмите вы алгоритм Евклида, найдите те самые пресловутые $u, v \in \mathbf{Z}$ такие, что $au + vm = 1$, умножьте это равенство на b: $aub + vmb = b$, откуда немедленно следует: $aub \equiv b(\mathrm{mod}\ m)$. Значит, решением исходного сравнения является $x \equiv ub(\mathrm{mod}\ m)$. Собственно, и все. Поворчал.

Случай 2. Пусть $(a, m) = d$. В этом случае для разрешимости сравнения $ax \equiv b(\mathrm{mod}\ m)$ необходимо, чтобы d делило b, иначе сравнение вообще выполняться не может. Действительно, $ax \equiv \equiv b(\mathrm{mod}\ m)$ бывает тогда, и только тогда, когда $ax - b$ делится на m нацело, т. е. $ax - b = t \cdot m$, $t \in \mathbf{Z}$, откуда $b = ax - t \cdot m$, а правая часть последнего равенства кратна d.

Пусть $b = db_1$, $a = da_1$, $m = dm_1$. Тогда обе части сравнения $xa_1 d \equiv b_1 d(\mathrm{mod}\ m_1 d)$ и его модуль поделим на d:

$$xa_1 \equiv b_1(\mathrm{mod}\ m_1),$$

где уже a_1 и m_1 взаимно просты. Согласно случаю 1 этого пункта такое сравнение имеет единственное решение x_0:

$$x \equiv x_0(\mathrm{mod}\ m_1) \qquad (*)$$

По исходному модулю m, числа $(*)$ образуют столько решений исходного сравнения, сколько чисел вида $(*)$ содержится в полной системе вычетов: $0, 1, 2, \ldots, m-2, m-1$. Очевидно, что из чисел $x = x_0 + t \cdot m$ в полную систему наименьших неотрицательных вычетов попадают только $x_0, x_0 + m_1, x_0 + 2m_1, \ldots, x_0 + \\ + (d-1)m_1$, т. е. всего d чисел. Значит, у исходного сравнения имеется d решений.

Подведем итог рассмотренных случаев в виде следующей теоремы.

Теорема 1. *Пусть $(a, m) = d$. Если b не делится на d, сравнение $ax \equiv b(\mathrm{mod}\ m)$ не имеет решений. Если b кратно d, сравнение $ax \equiv b(\mathrm{mod}\ m)$ имеет d штук решений.*

Пример. Решить сравнение $111x \equiv 75(\mathrm{mod}\ 321)$.

Р е ш е н и е. $(111, 321) = 3$, поэтому поделим сравнение и его модуль на 3:

$$37x \equiv 25(\mathrm{mod}\ 107), \quad \text{и уже } (37, 107) = 1.$$

Включаем алгоритм Евклида (как обычно, подчеркнуты неполные частные):

$$107 = 37 \cdot \underline{2} + 33,$$
$$37 = 33 \cdot \underline{1} + 4,$$
$$33 = 4 \cdot \underline{8} + 1,$$
$$4 = 1 \cdot \underline{4}.$$

Имеем $n = 4$ и цепная дробь такова:

$$\frac{m}{a} = \frac{107}{37} = 2 + \cfrac{1}{1 + \cfrac{1}{8 + \cfrac{1}{4}}}.$$

Таблица для нахождения числителей подходящих дробей:

q_n	0	2	1	8	4
P_n	1	2	3	26	107

Значит,

$$x \equiv (-1)^3 \cdot 26 \cdot 25 \equiv -650 (\mathrm{mod}\ 107) \equiv$$
$$\equiv -8 (\mathrm{mod}\ 107) \equiv 99 (\mathrm{mod}\ 107).$$

Три решения исходного сравнения:

$$x \equiv 99 (\mathrm{mod}\ 321), \quad x \equiv 206 (\mathrm{mod}\ 321), \quad x \equiv 313 (\mathrm{mod}\ 321),$$

и других решений нет. ♦

Рассмотрим пару других способов решения сравнений первой степени. Эти способы излагаются дальше в виде теорем.

Теорема 2. *Пусть* $m > 1$, $(a, m) = 1$. *Тогда сравнение* $ax \equiv b (\mathrm{mod}\ m)$ *имеет решение* $x \equiv ba^{\varphi(m)-1} (\mathrm{mod}\ m)$.

Доказательство. По теореме Эйлера, имеем $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\ m)$, следовательно, $a \cdot ba^{\varphi(m)-1} \equiv b (\mathrm{mod}\ m)$. ♦

Пример. Решить сравнение $7x \equiv 3 (\mathrm{mod}\ 10)$. Вычисляем

$$\varphi(10) = 4; x \equiv 3 \cdot 7^{4-1} (\mathrm{mod}\ 10) \equiv 1029 (\mathrm{mod}\ 10) \equiv 9 (\mathrm{mod}\ 10).$$

Видно, что этот способ решения сравнений хорош (в смысле минимума интеллектуальных затрат на его осуществление), но может потребовать возведения числа a в довольно большую степень, что довольно трудоемко. Для того чтобы как следует это

прочувствовать, возведите самостоятельно число 24789 в степень 46728.

Теорема 3. *Пусть p — простое число, $0 < a < p$. Тогда сравнение $ax \equiv b(\mathrm{mod}\, p)$ имеет решение*

$$x \equiv b \cdot (-1)^{a-1} \cdot \frac{(p-1)(p-2) \cdot \ldots \cdot (p-a+1)}{1 \cdot 2 \cdot 3 \cdot \ldots \cdot (a-1) \cdot a} (\mathrm{mod}\, p) \equiv$$
$$\equiv b \cdot (-1)^{a-1} \cdot \frac{(p-1)!}{(a!) \cdot (p-a)!} (\mathrm{mod}\, p) \equiv$$
$$\equiv b \cdot (-1)^{a-1} \cdot \frac{p!}{p \cdot (a!) \cdot (p-a)!} (\mathrm{mod}\, p) \equiv$$
$$\equiv b \cdot (-1)^{a-1} \cdot \frac{1}{p} \cdot C_p^a (\mathrm{mod}\, p),$$

где C_p^a — биномиальный коэффициент.

Доказательство непосредственно следует из очевидного сравнения:

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (a-1) \cdot a \cdot b \cdot (-1)^{a-1} \cdot \frac{(p-1)(p-2) \cdot \ldots \cdot (p-a+1)}{1 \cdot 2 \cdot 3 \cdot \ldots \cdot a} \equiv$$
$$\equiv b \cdot 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (a-1) \pmod{p},$$

которое нужно почленно поделить на взаимно простое с модулем число $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (a-1)$. ♦

Пример. Решить сравнение $7x \equiv 2(\mathrm{mod}\, 11)$. Вычисляем

$$C_{11}^7 = \frac{11!}{(7!) \cdot (11-7)!} = \frac{8 \cdot 9 \cdot 10 \cdot 11}{2 \cdot 3 \cdot 4} = 2 \cdot 3 \cdot 5 \cdot 11 = 330;$$

$$x \equiv 2 \cdot (-1)^6 \cdot \frac{1}{11} \cdot 330 \equiv 60 \equiv 5(\mathrm{mod}\, 11).$$

На этом п. 19 можно было бы и закончить, но невозможно, говоря о решении сравнений первой степени, обойти стороной вопрос о решении систем сравнений первой степени. Дело в том, что умение решать простейшие системы сравнений не только является неотъемлемой частью общечеловеческой культуры. Такое умение, кроме всего прочего, пригодится нам при изучении сравнений произвольной степени, о которых пойдет речь в следующих пунктах.

Лемма 1 (китайская теорема об остатках). *Пусть дана простейшая система сравнений первой степени*:

$$\begin{cases} x \equiv b_1 (\mathrm{mod}\ m_1), \\ x \equiv b_2 (\mathrm{mod}\ m_2), \\ \vdots \\ x \equiv b_k (\mathrm{mod}\ m_k), \end{cases} \qquad (*)$$

где $m_1, m_2, \ldots, m_k$ *попарно взаимно просты. Пусть, далее,* $m_1 m_2 \cdot \ldots \cdot m_k = M_s m_s$; $M_s M_s^{\nabla} \equiv 1 (\mathrm{mod}\ m_s)$. [1] *Тогда система* $(*)$ *равносильна одному сравнению*

$$x \equiv x_0 (\mathrm{mod}\ m_1 m_2 \cdot \ldots \cdot m_k),$$

т. е. набор решений $(*)$ *совпадает с набором решений сравнения* $x \equiv x_0 (\mathrm{mod}\ m_1 m_2 \cdot \ldots \cdot m_k)$.

Доказательство. Имеем: m_s делит M_j при $s \neq j$. Следовательно, $x_0 \equiv M_s M_s^{\nabla} b_s (\mathrm{mod}\ m_s)$, откуда $x_0 \equiv b_s (\mathrm{mod}\ m_s)$. Это означает, что система $(*)$ равносильна системе

$$\begin{cases} x \equiv x_0 (\mathrm{mod}\ m_1), \\ x \equiv x_0 (\mathrm{mod}\ m_2), \\ \vdots \\ x \equiv x_0 (\mathrm{mod}\ m_k), \end{cases}$$

которая, очевидно, в свою очередь, равносильна одному сравнению $x \equiv x_0 (\mathrm{mod}\ m_1 m_2 \ldots m_k)$. ♦

Пример. Найти число, которое при делении на 4 дает в остатке 1, при делении на 5 дает в остатке 3, а при делении на 7 дает в остатке 2. Составим систему

$$\begin{cases} x \equiv 1 (\mathrm{mod}\, 4), \\ x \equiv 3 (\mathrm{mod}\, 5), \\ x \equiv 2 (\mathrm{mod}\, 7), \end{cases}$$

[1] Очевидно, что такое число M_s^{∇} всегда можно подобрать хотя бы с помощью алгоритма Евклида, так как $(m_s, M_s) = 1$; $x_0 = M_1 M_1^{\nabla} b_1 + M_2 M_2^{\nabla} b_2 + \ldots + M_k M_k^{\nabla} b_k$.

которую начнем решать, пользуясь леммой 1. Вот ее решение: $b_1 = 1$, $b_2 = 3$, $b_3 = 2$; $m_1m_2m_3 = 4 \cdot 5 \cdot 7 = 4 \cdot 35 = 5 \cdot 28 = 7 \times \times 20 = 140$, т. е. $M_1 = 35$, $M_2 = 28$, $M_3 = 20$. Далее находим:

$$35 \cdot 3 \equiv 1(\mathrm{mod}\ 4),$$
$$28 \cdot 2 \equiv 1(\mathrm{mod}\ 5),$$
$$20 \cdot 6 \equiv 1(\mathrm{mod}\ 7),$$

т. е. $M_1^{\nabla} = 3, M_2^{\nabla} = 2, M_3^{\nabla} = 6$. Значит, $x_0 = 35 \cdot 3 \cdot 1 + 28 \cdot 2 \times \times 3 + 20 \cdot 6 \cdot 2 = 513$. После этого, по лемме 1, сразу получим ответ:

$$x \equiv 513(\mathrm{mod}\ 140) \equiv 93(\mathrm{mod}\ 140),$$

т. е. наименьшее положительное число равно 93.

В следующей лемме, для краткости формулировки, сохранены обозначения леммы 1.

Лемма 2. *Если $b_1, b_2, \ldots, b_k$ пробегают полные системы вычетов по модулям $m_1, m_2, \ldots, m_k$ соответственно, то x_0 пробегает полную систему вычетов по модулю $m_1m_2 \cdot \ldots \cdot m_k$.*

Доказательство. Действительно, $x_0 = A_1b_1 + A_2b_2 + \ldots + + A_kb_k$ пробегает $m_1m_2 \cdot \ldots \cdot m_k$ различных значений. Покажем, что все они попарно не сравнимы по модулю $m_1m_2 \cdot \ldots \cdot m_k$.

Пусть оказалось, что

$$A_1b_1 + A_2b_2 + \ldots + A_kb_k \equiv \equiv A_1b_1' + A_2b_2' + \ldots + A_kb_k'(\mathrm{mod}\ m_1m_2 \cdot \ldots \cdot m_k).$$

Значит,

$$A_1b_1 + A_2b_2 + \ldots + A_kb_k \equiv A_1b_1' + A_2b_2' + \ldots + A_kb_k'(\mathrm{mod}\ m_s)$$

для каждого s, откуда

$$M_sM_s^{\nabla}b_s \equiv M_sM_s^{\nabla}b_s'(\mathrm{mod}\ m_s).$$

Вспомним теперь, что $M_sM_s^{\nabla} \equiv 1(\mathrm{mod}\ m_s)$, значит $M_sM_s^{\nabla} = 1 + + m_s \cdot t$, откуда $(M_sM_s^{\nabla}, m_s) = 1$. Разделив теперь обе части сравнения

$$M_sM_s^{\nabla}b_s \equiv M_sM_s^{\nabla}b_s'(\mathrm{mod}\ m_s)$$

на число $M_sM_s^{\nabla}$, взаимно простое с модулем, получим, что $b_s \equiv \equiv b_s'(\mathrm{mod}\ m_s)$, т. е. $b_s = b_s'$ для каждого s.

Итак, x_0 пробегает $m_1m_2 \cdot \ldots \cdot m_k$ различных значений, попарно не сравнимых по модулю $m_1m_2 \cdot \ldots \cdot m_k$, т. е. полную систему вычетов. ♦

Вот теперь п. 19 с чистой совестью закончим.

Задачки

1. Решите уравнения:
а) $5x \equiv 3 (\mathrm{mod}\, 12)$; б) $256x \equiv 179 (\mathrm{mod}\, 337)$;
в) $1215x \equiv 560 (\mathrm{mod}\, 2755)$; г) $1296x \equiv 1105 (\mathrm{mod}\, 2413)$;
д) $115x \equiv 85 (\mathrm{mod}\, 355)$.

2. Решите систему сравнений

$$\begin{cases} 3x + 4y - 29 \equiv 0 (\mathrm{mod}\, 143), \\ 2x - 9y + 84 \equiv 0 (\mathrm{mod}\, 143). \end{cases}$$

3. Найдите все целые числа, которые при делении на 7 дают в остатке 3, при делении на 11 дают в остатке 5, а при делении на 13 дают в остатке 4.

4. Решите систему сравнений

$$\begin{cases} 3x \equiv 5 (\mathrm{mod}\, 7), \\ 2x \equiv 3 (\mathrm{mod}\, 5), \\ 3x \equiv 3 (\mathrm{mod}\, 9). \end{cases}$$

5. Пусть $(m_1,\ m_2) = d$. Докажите, что система сравнений

$$\begin{cases} x \equiv b_1 (\mathrm{mod}\ m_1), \\ x \equiv b_2 (\mathrm{mod}\ m_2) \end{cases}$$

имеет решения тогда и только тогда, когда $b_1 \equiv b_2 (\mathrm{mod}\, d)$. В случае, когда система разрешима, найдите ее решения.

6. Решите систему сравнений

$$\begin{cases} x \equiv 3 (\mathrm{mod}\, 8), \\ x \equiv 11 (\mathrm{mod}\, 20), \\ x \equiv 1 (\mathrm{mod}\, 15). \end{cases}$$

7. Пусть $(a, m) = 1, 1 < a < m$. Докажите, что разыскание решения сравнения $ax \equiv b (\mathrm{mod}\ m)$ может быть сведено к разысканию решений сравнений вида $b + mt \equiv 0 (\mathrm{mod}\ p)$, где p — простой делитель числа a.

20. Сравнения любой степени по простому модулю

В этом пункте мы рассмотрим сравнения вида $f(x) \equiv \equiv 0 (\mathrm{mod}\, p)$, где p — простое число, $f(x) = ax^n + a_1x^{n-1} + \ldots + + a_n$ — многочлен с целыми коэффициентами, и попытаемся на-

учиться решать такие сравнения. Не отвлекаясь на посторонние природные явления, сразу приступим к работе.

Лемма 1. *Произвольное сравнение* $f(x) \equiv 0 (\mathrm{mod}\, p)$, *где* p — *простое число*, *равносильно некоторому сравнению степени не выше* $p-1$.

Доказательство. Разделим $f(x)$ на многочлен $x^p - x$ (такой многочлен алгебраисты иногда называют «многочлен деления круга») с остатком:

$$f(x) = (x^p - x) \cdot Q(x) + R(x),$$

где, как известно, степень остатка $R(x)$ не превосходит $p-1$. Но ведь, по теореме Ферма, $x^p - x \equiv 0 (\mathrm{mod}\, p)$. Это означает, что $f(x) \equiv R(x) (\mathrm{mod}\, p)$, а исходное сравнение равносильно сравнению

$$R(x) \equiv 0 (\mathrm{mod}\, p). \qquad \blacklozenge$$

Доказанная лемма приятна тем, что с ее помощью можно свести решение сравнения высокой степени к решению сравнения меньшей степени. Идем далее.

Лемма 2. *Если сравнение*

$$ax^n + a_1 x^{n-1} + \ldots + a_n \equiv 0 (\mathrm{mod}\, p)$$

степени n *по простому модулю* p *имеет более* n *различных решений*, *то все коэффициенты* $a, a_1, \ldots, a_n$ *кратны* p.

Доказательство. Пусть сравнение $ax^n + a_1 x^{n-1} + \ldots + a_n \equiv \equiv 0 (\mathrm{mod}\, p)$ имеет $n+1$ решение и $x_1, x_2, \ldots, x_n, x_{n+1}$ — наименьшие неотрицательные вычеты этих решений. Тогда, очевидно, многочлен $f(x)$ представим в виде:

$$\begin{aligned} f(x) = {} & a(x-x_1)(x-x_2)\cdot\ldots\cdot(x-x_{n-2})(x-x_{n-1})(x-x_n) + \\ & + b(x-x_1)(x-x_2)\cdot\ldots\cdot(x-x_{n-2})(x-x_{n-1}) + \\ & + c(x-x_1)(x-x_2)\cdot\ldots\cdot(x-x_{n-2}) + \ldots \\ & \qquad\qquad \vdots \\ & + k(x-x_1)(x-x_2) + \\ & + l(x-x_1) + \\ & + m. \end{aligned}$$

Действительно, коэффициент b нужно взять равным коэффициенту при x^{n-1} в разности $f(x) - a(x-x_1)(x-x_2)\cdot\ldots\cdot(x-x_n)$; коэффициент c — это коэффициент перед x^{n-2} в разности

$$f(x)-a(x-x_1)(x-x_2)\cdot\ldots\cdot(x-x_n)-b(x-x_1)(x-x_2)\cdot\ldots\cdot(x-x_{n-1}),$$

и т. д. Теперь положим последовательно $x = x_1, x_2, \ldots, x_n, x_{n+1}$. Имеем:

1) $f(x_1) = m \equiv 0 (\mathrm{mod}\, p)$, следовательно, p делит m;

2) $f(x_2) = m + l(x_2 - x_1) \equiv l(x_2 - x_1) \equiv 0 (\mathrm{mod}\, p)$, следовательно, p делит l, ибо p не может делить $x_2 - x_1$, так как $x_2 < p, x_1 < p$;

3) $f(x_3) \equiv k(x_3 - x_1)(x_3 - x_2) \equiv 0 (\mathrm{mod}\, p)$, следовательно, p делит k.

И т. д.

Получается, что все коэффициенты $a, b, c, \ldots, k, l$ кратны p. Это означает, что все коэффициенты $a, a_1, \ldots, a_n$ тоже кратны p, ведь они являются суммами чисел, кратных p. (Убедитесь в этом самостоятельно, раскрыв скобки в написанном выше разложении многочлена $f(x)$ на суммы произведений линейных множителей.) ♦

Прошу обратить внимание на важность условия простоты модуля сравнения в формулировке леммы 2. Если модуль — число составное, то сравнение n-й степени может иметь и более n решений, при этом коэффициенты многочлена не обязаны быть кратными p. Пример: сравнение второй степени $x^2 \equiv 1 (\mathrm{mod}\, 16)$ имеет аж целых четыре различных решения (проверьте!):

$$x \equiv 1 (\mathrm{mod}\, 16), \qquad x \equiv 7 (\mathrm{mod}\, 16),$$
$$x \equiv 9 (\mathrm{mod}\, 16), \qquad x \equiv 15 (\mathrm{mod}\, 16).$$

Подведем итог.

Всякое нетривиальное сравнение по $\mathrm{mod}\, p$ *равносильно сравнению степени не выше* $p-1$ *и имеет не более* $p-1$ *решений.*

Наступил момент, когда наших знаний стало достаточно, чтобы легко понять доказательство еще одной замечательной теоремы теории чисел — теоремы Вильсона. Александр Вильсон (1714–1786) — шотландский астроном и математик-любитель, трудился профессором астрономии в Глазго. Теоремы Ферма, Эйлера и Вильсона всегда идут дружной тройкой во всех учебниках и теоретико-числовых курсах.

Теорема (Вильсон). *Сравнение* $(p-1)!+1 \equiv 0(\mathrm{mod}\, p)$ *выполняется тогда и только тогда, когда* p *— простое число.*

Доказательство. Пусть p — простое число. Если $p=2$, то, очевидно, $1!+1 \equiv 0(\mathrm{mod}\, 2)$. Если $p>2$, то рассмотрим сравнение

$$[(x-1)(x-2)\cdot\ldots\cdot(x-(p-1))]-(x^{p-1}-1)\equiv 0(\mathrm{mod}\, p).$$

Ясно, что это сравнение степени не выше $p-2$, но оно имеет $p-1$ решение: $1,2,3,\ldots,p-1$, так как при подстановке любого из этих чисел, слагаемое в квадратных скобках обращается в ноль, а $(x^{p-1}-1)$ сравнимо с нулем по теореме Ферма (x и p взаимно просты, так как. $x<p$). Это означает, по лемме 2, что все коэффициенты выписанного сравнения кратны p, в частности, на p делится его свободный член, равный $1\cdot 2\cdot 3\cdot\ldots\times$ $\times(p-1)+1$. [1])

Обратно. Если p — не простое, то найдется делитель d числа p, $1<d<p$. Тогда $(p-1)!$ делиться на d, поэтому $(p-1)!+1$ не может делится на d и, значит, не может делиться также и на p. Следовательно, сравнение $(p-1)!+1\equiv 0(\mathrm{mod}\, p)$ не выполняется. ♦

Пример. $1\cdot 2\cdot 3\cdot\ldots\cdot 10+1=3628800+1=3628801$ — делится на 11 (вспомните признак делимости на 11 — если сумма цифр в десятичной записи числа на четных позициях совпадает с суммой цифр на нечетных позициях, то число кратно 11).

Пример-задача. Доказать, что если простое число p представимо в виде $4n+1$, то существует такое число x, что x^2+1 делится на p.

Решение. Пусть $p=4n+1$ — простое число. По теореме Вильсона, $(4n)!+1$ делится на p. Заменим в выражении $1\cdot 2\cdot 3\cdot\ldots\cdot(4n)+1$ все множители большие $\dfrac{p-1}{2}=2n$ через разности числа p и чисел меньших $\dfrac{p-1}{2}=2n$. Получим

[1]) Так как коэффициенты многочлена являются значениями симметрических многочленов от его корней, то здесь наметился путь для доказательства огромного числа сравнений для симметрических многочленов. Однако я по этому пути дальше не пойду, оставляя это прекрасное развлечение читателю, которому нечем коротать долгие зимние вечера.

$$(p-1)!+1 = 1\cdot 2\cdot 3\cdot \ldots \cdot 2n\cdot (p-2n)(p-2n+1)\cdot \ldots \cdot (p-1) =$$
$$= (1\cdot 2\cdot 3\cdot \ldots \cdot 2n)\left[A\cdot p + (-1)^{2n}\cdot 2n\cdot (2n-1)\cdot \ldots \cdot 2\cdot 1\right] + 1 =$$
$$= A_1 p + (1\cdot 2\cdot 3\cdot \ldots \cdot 2n)^2 + 1.$$

Так как это число делится на p, то и сумма $(1\cdot 2\cdot 3\cdot \ldots \cdot 2n)^2+1$ делится на p, т. е. $x = (2n)! = \left(\frac{p-1}{2}\right)!$. ♦

Мелким шрифтом добавлю, что только что рассмотренный пример-задача тесно связан с проблематикой, касающейся представления натуральных чисел в виде сумм степеней (с показателями степени $n>1$) других натуральных чисел. Из нашего примера-задачи можно вывести, что натуральное число N в том и только в том случае представимо в виде суммы двух квадратов, когда в разложении N на простые множители все простые множители вида $4n+3$ входят в четных степенях. Попробуйте самостоятельно доказать это утверждение. Что касается представления чисел в виде сумм степеней, то здесь известна общая замечательная теорема:

для любого натурального k существует такое натуральное N (разумеется, зависящее от k), что каждое натуральное число представимо в виде суммы не более чем N слагаемых, являющихся k-ми степенями целых чисел.

У этой теоремы было известно несколько различных неэлементарных доказательств, но в 1942 г. ленинградский математик Ю. В. Линник придумал чисто арифметическое элементарное доказательство, которое, однако, является исключительно сложным (см., например, книжку А. Я. Хинчина «Три жемчужины теории чисел»). Что касается функции $N(k)$, то здесь в настоящее время почти ничего не ясно. Всякое натуральное число представимо в виде суммы четырех квадратов, девяти кубов (число 9 не может быть уменьшено), 21 штуки четвертых степеней (вот тут, кажется, что 21 может быть уменьшено до 19). Далее — полный туман. Всякое рациональное число представимо в виде суммы трех кубов рациональных чисел. [1]) В качестве неплохого развлечения, предлагаю читателю следующую задачу: доказать, что число 1 не может быть представлено в виде суммы двух кубов отличных от нуля рациональных чисел.

[1]) Доказательство этого утверждения впервые получено в 1825 г. Выглядит оно потрясающе: для рационального числа a непосредственно пишется его представление в виде суммы трех кубов рациональных чисел:

$$a = \left(\frac{a^3-3^6}{3^2a^2+3^4a+3^6}\right)^3 + \left(\frac{-a^3+3^5a+3^6}{3^2a^2+3^4a+3^6}\right)^3 + \left(\frac{a^2+3^4a}{3^2a^2+3^4a+3^6}\right)^3.$$

Совершенно неясно, как додуматься до такого доказательства.

Задачки

1. Какому сравнению степени ниже 7 равносильно сравнение:

$$2x^{17} + 6x^{16} + x^{14} + 5x^{12} + 3x^{11} + 2x^{10} + x^9 + 5x^8 + 2x^7 + \\ + 3x^5 + 4x^4 + 6x^3 + 4x^2 + x + 4 \equiv 0 (\mathrm{mod}\ 7)?$$

2. Используя процесс перебора всех вычетов из полной системы, решите сравнение

$$3x^{14} + 4x^{13} + 3x^{12} + 2x^{11} + x^9 + 2x^8 + 4x^7 + x^6 + 3x^4 + \\ + x^3 + 4x^2 + 2x \equiv 0 (\mathrm{mod}\ 5),$$

предварительно понизив его степень.

3. Пусть $(a_0, m) = 1$. Укажите сравнение n-й степени со старшим коэффициентом 1, равносильное сравнению

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_n \equiv 0 (\mathrm{mod}\ m).$$

4. Докажите, что сравнение $f(x) \equiv 0 (\mathrm{mod}\, p)$, где p — простое, $f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$, $n \leqslant p$, имеет n решений тогда и только тогда, когда все коэффициенты остатка от деления $x^p - x$ на $f(x)$ кратны p.

5. Перед вами крупная задачка, разделенная на несколько мелких частей. Решите их по порядку.

а) Пусть

$$\chi(k) = \begin{cases} 1, & \text{если } k \text{ — простое,} \\ 0, & \text{если } k \text{ — составное,} \end{cases}$$

— характеристическая функция множества простых чисел. Докажите, что

$$\chi(k) = ((k-1)!)^2 - k \cdot \left[\frac{((k-1)!)^2}{k} \right],$$

где, как обычно, $[x]$ — целая часть числа x.

б) Сообразите, что $\pi(m) = \sum\limits_{k=2}^{m} \chi(k)$, где $\pi(m)$ — число простых чисел, не превосходящих m («функция распределения» простых чисел).

в) Убедитесь, что

$$\mathrm{sgn}\,(n - \pi(m)) = \begin{cases} 1, & \text{если } m < p_n, \\ 0, & \text{если } m \geqslant p_n, \end{cases}$$

где $\mathrm{sgn}\,(x) = \begin{cases} 1, & \text{если } x > 0, \\ 0, & \text{если } x \leqslant 0, \end{cases}$ («сигнум», т. е. знак x).

г) Пусть p_n — n-е в порядке возрастания простое число, т. е. $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$. Докажите, что $p_n \leqslant n^2 + 1$ для всех n.

д) Докажите, что (Внимание! Перед вами формула, выражающая простое число p_n через его номер!) [1]

$$p_n = \sum_{m=0}^{n^2+1} \operatorname{sgn}\left(n - \sum_{k=2}^{m}\left(((k-1)!)^2 - k \cdot \left[\frac{((k-1)!)^2}{k}\right]\right)\right).$$

21. Сравнения любой степени по составному модулю

Переход от решения сравнений по простому модулю к *a priori* более сложной задаче — решению сравнений по составному модулю (переход от п. 20 к п. 21) — осуществляется быстро и без лишних затей с помощью следующей теоремы.

Теорема 1. *Если числа $m_1, m_2, \ldots, m_k$ попарно взаимно просты, то сравнение $f(x) \equiv 0 (\mathrm{mod}\ m_1 m_2 \cdot \ldots \cdot m_k)$ равносильно системе сравнений*

$$\begin{cases} f(x) \equiv 0 (\mathrm{mod}\ m_1), \\ f(x) \equiv 0 (\mathrm{mod}\ m_2), \\ \vdots \\ f(x) \equiv 0 (\mathrm{mod}\ m_k). \end{cases}$$

При этом если $T_1, T_2, \ldots, T_к$ — числа решений отдельных сравнений этой системы по соответствующим модулям, то число решений T исходного сравнения равно $T_1 T_2 \cdot \ldots \cdot T_к$.

Доказательство. Первое утверждение теоремы (о равносильности системы и сравнения) очевидно, так как если $a \equiv b (\mathrm{mod}\, m)$, то $a \equiv b (\mathrm{mod}\, d)$, где d делит m. Если же $a \equiv b (\mathrm{mod}\, m_1)$ и $a \equiv b (\mathrm{mod}\ m_2)$, то получаем $a \equiv b (\mathrm{mod}\, HOK(m_1, m_2))$, где НОК$(m_1,\ m_2)$ — наименьшее общее кратное m_1 и m_2. (Вспомните простейшие свойства сравнений из п. 16.)

[1] Вопреки распространенному мнению о «невозможности задать простые числа формулой», довольно легко сконструировать выражение n-го простого числа через его номер. Беда в том, что от подобных формул мало толку. Во-первых, вычисление по ним не короче вычисления при помощи решета Эратосфена, во-вторых, эти формулы отнюдь не облегчают исследование различных закономерностей, связанных с простыми числами (распределение простых чисел, наличие в множестве простых чисел арифметических прогрессий заданной длины и т. п.).

Обратимся ко второму утверждению теоремы (о числе решений сравнения). Каждое сравнение $f(x) \equiv 0(\mathrm{mod}\ m_s)$ выполняется тогда и только тогда, когда выполняется одно из T_s штук сравнений вида $x \equiv b_s(\mathrm{mod}\ m_s)$, где b_s пробегает вычеты решений сравнения $f(x) \equiv 0(\mathrm{mod}\ m_s)$. Всего различных комбинаций таких простейших сравнений

$$\begin{cases} x \equiv b_1(\mathrm{mod}\ m_1), \\ x \equiv b_2(\mathrm{mod}\ m_2), \\ \vdots \\ x \equiv b_k(\mathrm{mod}\ m_k), \end{cases}$$

$T_1T_2 \cdot \ldots \cdot T_{\mathrm{к}}$ штук. Все эти комбинации, по лемме 2 из п. 19, приводят к различным классам вычетов по $\mathrm{mod}\,(m_1m_2 \cdot \ldots \cdot m_k)$. ♦

Итак, решение сравнения $f(x) \equiv 0(\mathrm{mod}\ p_1^{\alpha_1}p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k})$ сводится к решению сравнений вида $f(x) \equiv 0(\mathrm{mod}\, p^{\alpha})$. Оказывается, что решение этого последнего сравнения, в свою очередь, сводится к решению некоторого сравнения $g(x) \equiv 0(\mathrm{mod}\, p)$ с другим многочленом в левой части, но уже с простым модулем, а это, просто напросто, приводит нас в рамки предыдущего пункта. Сейчас я расскажу процесс сведения решения сравнения $f(x) \equiv 0(\mathrm{mod}\, p^{\alpha})$ к решению сравнения $g(x) \equiv 0(\mathrm{mod}\, p)$.

Процесс сведения. Очевидно, выполнение сравнения $f(x) \equiv 0(\mathrm{mod}\, p^{\alpha})$ влечет, что x подходит в сравнение $f(x) \equiv 0(\mathrm{mod} p)$. Пусть $x \equiv x_1(\mathrm{mod} p)$ — какое-нибудь решение сравнения $f(x) \equiv 0(\mathrm{mod}\, p)$. Это означает, что

$$x = x_1 + p \cdot t_1,$$

где $t_1 \in \mathbf{Z}$.

Вставим это x в сравнение $f(x) \equiv 0(\mathrm{mod}\, p^2)$. Получим сравнение

$$f(x_1 + p \cdot t_1) \equiv 0(\mathrm{mod}\, p^2),$$

которое тоже, очевидно, выполняется.

Разложим далее (не пугайтесь!) левую часть полученного сравнения по формуле Тейлора по степеням $(x - x_1)$:

$$f(x) = f(x_1) + \frac{f'(x_1)}{1!}(x - x_1) + \frac{f''(x_1)}{2!}(x - x_1)^2 + \ldots.$$

Но, ведь, $x = x_1 + p \cdot t_1$, следовательно,

$$f(x_1 + p \cdot t_1) = f(x_1) + \frac{f'(x_1)}{1!} p \cdot t_1 + \frac{f''(x_1)}{2!} p^2 \cdot t_1^2 + \ldots .$$

Заметим, что число $\dfrac{f^{(k)}(x_1)}{k!}$ всегда целое, так как $f(x_1 + p \cdot t_1)$ — многочлен с целыми коэффициентами. Теперь в сравнении

$$f(x_1 + p \cdot t_1) \equiv 0 (\mathrm{mod}\, p^2)$$

можно слева отбросить члены, кратные p^2:

$$f(x_1) + \frac{f'(x_1)}{1!} p \cdot t_1 \equiv 0 (\mathrm{mod}\, p^2).$$

Разделим последнее сравнение и его модуль на p:

$$\frac{f(x_1)}{p} + \frac{f'(x_1)}{1!} \cdot t_1 \equiv 0 (\mathrm{mod}\, p).$$

Заметим опять, что $\dfrac{f(x_1)}{p}$ — целое число, так как $f(x_1) \equiv \equiv 0 (\mathrm{mod}\, p)$.

Далее ограничимся случаем, когда значение производной $f'(x_1)$ не делится на p. В этом случае имеется всего одно решение сравнения первой степени $\dfrac{f(x_1)}{p} + \dfrac{f'(x_1)}{1!} \cdot t_1 \equiv 0 (\mathrm{mod}\, p)$ относительно t_1:

$$t_1 \equiv t_1^{\nabla} (\mathrm{mod}\, p). \text{ [1)]}$$

Это, опять-таки, означает, что $t_1 = t_1^{\nabla} + p \cdot t_2$, где $t_2 \in \mathbf{Z}$, и

$$x = x_1 + p \cdot t_1 = \underbrace{x_1 + p \cdot t_1^{\nabla}}_{x_2} + p^2 t_2 = x_2 + p^2 t_2.$$

Снова вставим это $x = x_2 + p^2 t_2$ в сравнение $f(x) \equiv 0 (\mathrm{mod}\, p^3)$ (но теперь это сравнение уже по $\mathrm{mod}\, p^3$), разложим его левую часть

[1)] В случае, когда значение производной $f'(x_1)$ кратно p, сравнение

$$\frac{f(x_1)}{p} + \frac{f'(x_1)}{1!} \cdot t_1 \equiv 0 (\mathrm{mod}\, p)$$

может иметь несколько решений, тогда рассматриваемый процесс нужно продолжать для каждого решения в отдельности.

по формуле Тейлора по степеням $(x - x_2)$ и отбросим члены, кратные p^3:

$$f(x_2) + \frac{f'(x_2)}{1!}p^2 t_2 \equiv 0 (\mathrm{mod}\, p^3).$$

Делим это сравнение и его модуль на p^2:

$$\frac{f(x_2)}{p^2} + f'(x_2) \cdot t_2 \equiv 0 (\mathrm{mod}\, p).$$

Опять-таки $\dfrac{f(x_2)}{p^2}$ — целое число, ведь число t_1^{∇} такое, что $f(x_1 + p \cdot t_1^{\nabla}) \equiv 0 (\mathrm{mod}\, p^2)$. Кроме того, $x_2 \equiv x_1 (\mathrm{mod}\, p)$, значит, $f'(x_2) \equiv f'(x_1) (\mathrm{mod} p)$, т. е. $f'(x_2)$, как и $f'(x_1)$, не делится на p. Имеем единственное решение сравнения первой степени $\dfrac{f(x_2)}{p^2} + f'(x_2) \cdot t_2 \equiv 0 (\mathrm{mod}\, p)$ относительно t_2:

$$t_2 \equiv t_2^{\nabla} (\mathrm{mod}\, p).$$

Это, опять-таки, означает, что $t_2 = t_2^{\nabla} + p \cdot t_3$, где $t_3 \in \mathbf{Z}$, и

$$x = \underbrace{x_2 + p^2 \cdot t_2^{\nabla}}_{x_3} + p^3 t_3 = x_3 + p^3 t_3$$

и процесс продолжается дальше и дальше, аналогично предыдущим шагам, до достижения степени α, в которой стоит простое число p в модуле исходного сравнения $f(x) \equiv 0 (\mathrm{mod}\, p^{\alpha})$.

Итак:

всякое решение $x \equiv x_1 (\mathrm{mod}\, p)$ *сравнения* $f(x) \equiv 0 (\mathrm{mod}\, p)$ *при условии* p не делит $f'(x_1)$, *дает одно решение сравнения* $f(x) \equiv 0 (\mathrm{mod}\, p^{\alpha})$ *вида* $x \equiv x_{\alpha} + p^{\alpha} t_{\alpha}$, *т. е.* $x \equiv x_{\alpha} (\mathrm{mod}\, p^{\alpha})$. ♦

Пример. Решить сравнение $x^4 + 7x + 4 \equiv 0 (\mathrm{mod}\, 27)$.

Р е ш е н и е. $27 = 3^3$. Далее, можно проверить перебором полной системы вычетов по $\mathrm{mod}\, 3$, что сравнение $x^4 + 7x + 4 \equiv$ $\equiv 0 (\mathrm{mod}\, 3)$ имеет всего одно решение $x \equiv 1 (\mathrm{mod}\, 3)$. Последующий процесс решения, в идеале, должен быть таким:

$$f'(x) = (4x^3 + 7)\,|_{x \equiv 1} \equiv 2 (\mathrm{mod}\, 3),$$

т. е. не делится на $p = 3$. Далее,

$$x_1 = 1 + 3 \cdot t_1,$$
$$f(1) + f'(1) \cdot 3t_1 \equiv 0 (\mathrm{mod}\, 3^2).$$

Ищем t_1:

$$3 + 3t_1 \cdot 2 \equiv 0(\mathrm{mod}\ 9),$$

после деления на $p = 3$:

$$1 + 2t_1 \equiv 0(\mathrm{mod}\ 3),$$
$$t_1 \equiv 1(\mathrm{mod}\ 3)$$

— единственное решение. Далее:

$$t_1 = 1 + 3t_2,$$
$$x = 1 + 3t_1 = 4 + 9t_2,$$
$$f(4) + 9 \cdot t_2 \cdot f'(4) \equiv 0(\mathrm{mod}\ p^3 = 27),$$
$$18 + 9 \cdot 20 \cdot t_2 \equiv 0(\mathrm{mod}\ 27),$$

и, после деления на $p^2 = 9$, ищем t_2:

$$2 + 20t_2 \equiv 0(\mathrm{mod}\ 3),$$
$$t_2 \equiv 2(\mathrm{mod}\ 3),$$
$$t_2 = 2 + 3 \cdot t_3,$$

откуда

$$x = 4 + 9 \cdot (2 + 3t_3) = 22 + 27t_3.$$

Значит, единственным решением исходного сравнения является $x \equiv 22(\mathrm{mod}\ 27)$. ♦

Следующая теорема относится к специфическому, но весьма приятному виду сравнений.

Теорема 2. *Пусть A, m, n — натуральные числа*; $(A, m) = 1$, $x \equiv x_0(\mathrm{mod}\ m)$ *— одно из решений сравнения*

$$x^n \equiv A(\mathrm{mod}\ m).$$

Тогда все решения этого сравнения получаются умножением x_0 на вычеты решений сравнения $y^n \equiv 1(\mathrm{mod}\ m)$.

Доказательство. Перемножим сравнения:

$$\begin{array}{r} x_0^n \equiv A(\mathrm{mod}\ m) \\ \underline{y^n \equiv 1(\mathrm{mod}\ m)} \quad \times \\ (x_0 y)^n \equiv A(\mathrm{mod}\ m), \end{array}$$

откуда видно, что $x_0 y$ — решения сравнения $x^n \equiv A(\mathrm{mod}\ m)$.

Если теперь $y_1 \not\equiv y_2 (\mathrm{mod}\ m)$, то $x_0 y_1 \not\equiv x_0 y_2 (\mathrm{mod}\ m)$. Действительно, предположим, что $x_0 y_1 \equiv x_0 y_2 (\mathrm{mod}\ m)$. Очевидно, что $(x_0, m) = 1$, так как иначе было бы:

$$x_0 = d \cdot x_0^{\nabla}, m = d \cdot m^{\nabla},$$
$$x_0 = d^n (x_0^{\nabla})^n \equiv A (\mathrm{mod}\ d m^{\nabla}),$$

следовательно, d делит A и делит m, что противоречит взаимной простоте A и m. Значит, $(x_0, m) = 1$ и сравнение $x_0 y_1 \equiv x_0 y_2 (\mathrm{mod}\ m)$ можно поделить на x_0: $y_1 \equiv y_2 (\mathrm{mod}\ m)$ — а это противоречит исходному предположению. Таким образом, для разных y_1 и y_2, получаются разные решения.

Осталось убедиться, что каждое решение сравнения $x^n \equiv A (\mathrm{mod}\ m)$ получается именно таким способом. Имеем

$$x^n \equiv A (\mathrm{mod}\ m),$$
$$x_0^n \equiv A (\mathrm{mod}\ m),$$

следовательно, $x^n \equiv x_0^n (\mathrm{mod}\ m)$. Возьмем число y такое, что $x \equiv y \cdot x_0 (\mathrm{mod}\ m)$. Тогда $y^n x_0^n \equiv x_0^n (\mathrm{mod}\ m)$, т. е. $y^n \equiv 1 (\mathrm{mod}\ m)$. ♦

Пункт с номером 21 (очко!) закончен.

Задачки

1. Сколько решений имеет сравнение

$$x^5 + x + 1 \equiv 0 (\mathrm{mod}\ 105)?$$

2. Решите сравнения:

а) $7x^4 + 19x + 25 \equiv 0 (\mathrm{mod}\ 27)$;
б) $9x^2 + 29x + 62 \equiv 0 (\mathrm{mod}\ 64)$;
в) $6x^3 + 27x^2 + 17x + 20 \equiv 0 (\mathrm{mod}\ 30)$;
г) $31x^4 + 57x^3 + 96x + 191 \equiv 0 (\mathrm{mod}\ 225)$;
д) $x^3 + 2x + 2 \equiv 0 (\mathrm{mod}\ 125)$;
е) $x^4 + 4x^3 + 2x^2 + 2x + 12 \equiv 0 (\mathrm{mod}\ 625)$.

22. Сравнения второй степени. Символ Лежандра

В этом пункте мы будем подробно рассматривать простейшие двучленные сравнения второй степени вида

$$x^2 \equiv a (\mathrm{mod}\ p),$$

где a и p взаимно просты, а p — нечетное простое число. (Традиционная фраза «нечетное простое число», на мой взгляд, несколько странновата. Глядя на нее, можно подумать, что четных простых чисел — пруд пруди, а она, всего-навсего, убирает из рассмотрения только число $p = 2$.) Обратите внимание, что условие взаимной простоты $(a, p) = 1$ исключает из нашего рассмотрения случай $a = 0$.

Почему мы хотим исключить из дальнейших рассмотрений эти случаи? Нас будет интересовать вопрос, при каких a простейшее двучленное сравнение второй степени имеет решение, а при каких — не имеет. Ясно, что сравнение $x^2 \equiv a (\mathrm{mod}\, 2)$ имеет решение при любых a, так как вместо a достаточно подставлять только 0 или 1, а числа 0 и 1 являются квадратами. Именно поэтому случай $p = 2$ не представляет особого интереса и выводится из дальнейшего рассмотрения вышенаписанной странноватой фразой. [1]

Что касается сравнения $x^2 \equiv 0 (\mathrm{mod}\, p)$, то оно, очевидно, всегда имеет решение $x = 0$. Итак, интерес представляет только ситуация с нечетным простым модулем и $a \neq 0$, поэтому далее мы будем трудиться только в рамках оговоренных ограничений.

Определение. Если сравнение $x^2 \equiv a (\mathrm{mod}\, p)$ имеет решения, то число aназывается *квадратичным вычетом* по модулю p. В противном случае число a называется *квадратичным невычетом* по модулю p. [2]

Итак, если a — квадрат некоторого числа по модулю p, то a — «квадратичный вычет», если же никакое число в квадрате не сравнимо с a по модулю p, то a — «квадратичный невычет». Смиримся с этим.

Пример. Число 2 является квадратом по модулю 7, так как $4^2 \equiv 16 \equiv 2 (\mathrm{mod}\, 7)$. Значит, 2 — квадратичный вычет. (Сравнение $x^2 \equiv 2 (\mathrm{mod}\, 7)$ имеет еще и другое решение: $3^2 \equiv 9 \equiv$

[1] Искушенный алгебраист объяснил бы эту ситуацию так: «Всякий элемент любого поля характеристики 2 является квадратом, так как отображение $x \mapsto x^2$есть автоморфизм такого поля».

[2] Чтобы понять явление, надо сделать на него пародию. Всю стилистическую прелесть подобного определения (между прочим, общепринятого) и, в особенности, очарование содержащегося в нем термина «невычет» (в слитном написании), поможет прочувствовать аналогичная дефиниция: маленькое и жесткое хлебобулочное изделие тороидальной формы называется сушкой. В противном случае, оно называется несушкой. Впрочем, стилистических казусов в традиционной математической терминологии довольно много, например: нормальная подгруппа — ненормальная подгруппа, невязка — вязка и т. п.

$\equiv 2(\mathrm{mod}\,7)$.) Напротив, число 3 является квадратичным невычетом по модулю 7, так как сравнение $x^2 \equiv 3(\mathrm{mod}\,7)$ решений не имеет, в чем нетрудно убедиться последовательным перебором полной системы вычетов: $x = 0, 1, 2, 3, 4, 5, 6$.

Простое наблюдение: если a — квадратичный вычет по модулю p, то сравнение $x^2 \equiv a(\mathrm{mod}\,p)$ имеет в точности два решения. Действительно, если a — квадратичный вычет по модулю p, то у сравнения $x^2 \equiv a(\mathrm{mod}\,p)$ есть хотя бы одно решение $x \equiv x_1(\mathrm{mod}\,p)$. Тогда $x_2 = -x_1$ — тоже решение, ведь $(-x_1)^2 = x_1^2$. Эти два решения не сравнимы по модулю $p > 2$, так как из $x_1 \equiv -x_1(\mathrm{mod}\,p)$ следует $2x_1 \equiv 0(\mathrm{mod}\,p)$, т. е. (поскольку $p \neq 2$) $x_1 \equiv 0(\mathrm{mod}\,p)$, что невозможно, ибо $a \neq 0$. Поскольку сравнение $x^2 \equiv a(\mathrm{mod}\,p)$ есть сравнение второй степени по простому модулю, то больше двух решений оно иметь не может (см. п. 20, лемма 2).

Еще одно простое наблюдение: приведенная (т. е. без нуля) система вычетов

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

по модулю p состоит из $\dfrac{p-1}{2}$ квадратичных вычетов, сравнимых с числами $1^2, 2^2, \ldots, \left(\dfrac{p-1}{2}\right)^2$, и $\dfrac{p-1}{2}$ квадратичных невычетов, т. е. вычетов и невычетов поровну.

Действительно, квадратичные вычеты сравнимы с квадратами чисел

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

т. е. с числами $1^2, 2^2, \ldots, \left(\dfrac{p-1}{2}\right)^2$, при этом все эти квадраты различны по модулю p, ибо из $k^2 \equiv l^2(\mathrm{mod}\,p)$, где $0 < k < l \leqslant \dfrac{p-1}{2}$, следует, что нетривиальное сравнение $x^2 \equiv k^2(\mathrm{mod}\,p)$ имеет аж четыре решения: $l, -l, k, -k$, что невозможно (см. п. 20, лемма 2). [1)]

[1)] Искушенный алгебраист опять-таки сказал бы больше: «Квадраты (исключая 0) любого поля конечной характеристики, большей двух, образуют подгруппу индекса 2 мультипликативной группы этого поля. Эта подгруппа есть ядро эндоморфизма $x \mapsto x^{\frac{p-1}{2}}$». Если есть желание, проверьте это утверждение самостоятельно.

Согласитесь, что фраза «Число a является квадратичным вычетом (или невычетом) по модулю p» несколько длинновата, особенно если ее приходится часто употреблять при доказательстве какого-либо утверждения. В свое время божественная длиннота этой фразы тревожила и знаменитого французского математика Адриена-Мари Лежандра (того самого, который имеет прямое отношение к ортогональным полиномам и многим другим математическим открытиям). Он предложил изящный выход, введя в рассмотрение удобный символ $\left(\frac{a}{p}\right)$, заменяющий длинную фразу. Этот символ носит теперь фамилию Лежандра и читается: «символ Лежандра а по пэ».

Определение. Пусть a не кратно p. Тогда символ Лежандра определяется так:

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{если } a \text{ — квадратичный вычет по модулю } p, \\ -1, & \text{если } a \text{ — квадратичный невычет по модулю } p. \end{cases}$$

Оказывается, что символ Лежандра есть не просто удобное обозначение. Он имеет много полезных свойств и глубокий смысл, уходящий корнями в теорию конечных полей. Далее в этом пункте мы рассмотрим некоторые простейшие свойства символа Лежандра и, прежде всего, научимся его вычислять (т. е. тем самым, научимся отвечать на вопрос, проставленный в начале пункта: при каких a простейшее двучленное сравнение второй степени имеет решение, а при каких — не имеет?).

Теорема (критерий Эйлера). *Пусть a не кратно p. Тогда*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (\mathrm{mod}\, p).$$

Доказательство. По теореме Ферма, $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$, т. е.

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 (\mathrm{mod}\, p).$$

В левой части последнего сравнения в точности один сомножитель делится на p, ведь оба сомножителя на p делиться не могут, иначе их разность, равная двум, делилась бы на $p > 2$. Следовательно, имеет место одно и только одно из сравнений:

$$a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p),$$
$$a^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\, p).$$

Но всякий квадратичный вычет a удовлетворяет при некотором x сравнению $a \equiv x^2 (\mathrm{mod}\, p)$ и, следовательно, удовлетворяет также получаемому из него почленным возведением в степень $\frac{p-1}{2}$ сравнению $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 (\mathrm{mod}\, p)$ (опять теорема Ферма). При этом квадратичными вычетами и исчерпываются все решения сравнения $a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$, так как, будучи сравнением степени $\frac{p-1}{2}$, оно не может иметь более $\frac{p-1}{2}$ решений. Это означает, что квадратичные невычеты удовлетворяют сравнению $a^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\, p)$. [1] ♦

Пример. Крошка-сын к отцу пришел, и спросила кроха: «Будет ли число 5 квадратом по модулю 7?». Гигант-отец тут же сообразил:

$$5^{\frac{7-1}{2}} = 5^3 = 125 = 18 \cdot 7 - 1 \equiv -1 (\mathrm{mod}\, 7),$$

т. е. сравнение $x^2 \equiv 5 (\mathrm{mod}\, 7)$ решений не имеет и 5 — квадратичный невычет по модулю 7. Кроха-сын, расстроенный, пошел на улицу делиться с друзьями полученной информацией.

Перечислим далее, кое-где доказывая или комментируя, простейшие свойства символа Лежандра.

Свойство 1. *Если* $a \equiv b (\mathrm{mod}\, p)$, *то* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Это свойство следует из того, что числа одного и того же класса по модулю p будут все одновременно квадратичными вычетами либо квадратичными невычетами. ♦

Свойство 2. $\left(\frac{1}{p}\right) = 1$.

Доказательство очевидно, ведь единица является квадратом. ♦

Свойство 3. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

---

[1] Свойство $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (\mathrm{mod}\, p)$, даваемое критерием Эйлера, можно было бы сразу принять за определение символа Лежандра, показав, конечно, предварительно, с помощью теоремы Ферма, что $a^{\frac{p-1}{2}} \equiv \pm 1 (\mathrm{mod}\, p)$. Именно так частенько и поступают в книжках по теории конечных полей.

Доказательство этого свойства следует из критерия Эйлера при $a = -1$. Так как $\dfrac{p-1}{2}$ — четное, если p имеет вид $4n+1$, и нечетное, если p имеет вид $4n+3$, то число -1 является квадратичным вычетом по модулю p тогда и только тогда, когда p имеет вид $4n+1$. ♦

Свойство 4. $\left(\dfrac{ab}{p}\right) = \left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)$.

Действительно,

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) (\mathrm{mod}\, p). \quad ♦$$

Свойство 4, очевидно, распространяется на любое конечное число сомножителей в числителе символа Лежандра, взаимно простых с p. Кроме того, из него следует

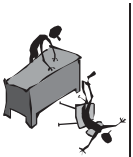
Свойство 5. $\left(\dfrac{ab^2}{p}\right) = \left(\dfrac{a}{p}\right)$, *т. е. в числителе символа Лежандра можно отбросить любой квадратный множитель.*

Действительно:

$$\left(\frac{ab^2}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right) \equiv \left(\frac{a}{p}\right) \cdot 1 \equiv \left(\frac{a}{p}\right) (\mathrm{mod}\, p). \quad ♦$$

Запомним хорошенько эти пять перечисленных простейших свойств символа Лежандра и устремимся дальше, в п. 23, где нам раскроются свойства более сложные и глубокие, поразительные и загадочные. Вперед!

Задачки



1. Среди вычетов приведенной системы по модулю 37 укажите квадратичные вычеты и квадратичные невычеты.

2. Посчитайте символ Лежандра, умело пользуясь его свойствами:
а) $\left(\dfrac{20}{7}\right)$; б) $\left(\dfrac{200}{43}\right)$; в) $\left(\dfrac{1601600}{839}\right)$.

3. С помощью критерия Эйлера установите, имеет ли решение сравнение $x^2 \equiv 5 (\mathrm{mod}\ 13)$?

4. С помощью символа Лежандра установите, имеют ли решения сравнения:
а) $x^2 \equiv 22 (\mathrm{mod}\ 13)$;
б) $x^2 \equiv 239 (\mathrm{mod}\ 661)$;
в) $x^2 \equiv 412 (\mathrm{mod}\ 421)$?

5. Решите сравнения:
а) $x^2 \equiv 7 (\mathrm{mod}\ 137)$; б) $x^2 \equiv 23 (\mathrm{mod}\ 101)$.

6. Докажите, что:
а) сравнение $x^2 + 1 \equiv 0 (\mathrm{mod}\, p)$ разрешимо тогда и только тогда, когда p — простое число вида $4m + 1$;
б) сравнение $x^2 + 2 \equiv 0 (\mathrm{mod}\, p)$ разрешимо тогда и только тогда, когда p — простое число вида $8m + 1$ или вида $8m + 3$;
в) сравнение $x^2 + 3 \equiv 0 (\mathrm{mod}\, p)$ разрешимо тогда и только тогда, когда p — простое число вида $6m + 1$.

7. Используя теорему Вильсона, докажите, что решениями сравнения $x^2 + 1 \equiv 0 (\mathrm{mod}\, p)$, где p — простое число вида $4m + 1$, являются числа $x_{1,2} \equiv \pm (2m)! (\mathrm{mod}\, p)$ и только они.

8. Докажите, что сравнение $x^2 \equiv a (\mathrm{mod}\, p^\alpha)$, где $\alpha > 1$, $p > 2$, имеет два решения или же ни одного, в зависимости от того, будет ли число a квадратичным вычетом или же невычетом по модулю p.

9. Исследуйте самостоятельно сравнение вида

$$x^2 \equiv a (\mathrm{mod}\, 2^\alpha), \quad \alpha > 1.$$

При каких условиях на числа a и α это сравнение имеет решения и сколько оно их имеет? Найдите эти решения.

10. Докажите, что решениями сравнения $x^2 \equiv a (\mathrm{mod} p^\alpha)$, где $(a, p) = 1$, $p > 2$, будут числа $x \equiv \pm P Q^\nabla (\mathrm{mod}\, p^\alpha)$, где

$$P = \frac{(z + \sqrt{a}\,)^\alpha + (z - \sqrt{a}\,)^\alpha}{2},$$

$$Q = \frac{(z + \sqrt{a}\,)^\alpha + (z - \sqrt{a}\,)^\alpha}{2\sqrt{a}},$$

$$z^2 \equiv a (\mathrm{mod}\, p), \quad Q \cdot Q^\nabla \equiv 1 (\mathrm{mod}\, p^\alpha).$$

11. Докажите, что число различных разложений натурального числа n на сумму квадратов двух целых чисел равно учетверенному избытку числа делителей n вида $4k + 1$ над числом делителей вида $4k + 3$. [1])

[1]) Порядок слагаемых в разложении учитывается, например, $25 = 3^2 + 4^2$ и $25 = 4^2 + 3^2$ — разные разложения. Иначе эту задачу можно сформулировать так: сколько целых точек лежит на окружности

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

23. Дальнейшие свойства символа Лежандра. Закон взаимности Гаусса

Какая песня без баяна, какой курс теории чисел без удивительного закона взаимности Гаусса! В этом пункте я расскажу об этом законе, ибо без него традиционный курс теории чисел как дом без дверей, как машина без руля.

Историческое отступление про Гаусса

Карл Фридрих Гаусс (1777–1855) — величественная фигура математики рубежа восемнадцатого — девятнадцатого столетий. Он родился в немецком городке Брауншвейге, был сыном поденщика. Математические способности Гаусса проявились очень рано, а, согласно его дневникам, в 17 лет Карл Фридрих уже начал делать выдающиеся математические открытия. Дебютом Гаусса явилось доказательство возможности построения правильного семнадцатиугольника циркулем и линейкой (записью об этом открывается дневник Гаусса — удивительная летопись гениальных открытий. Запись датирована 30 марта 1796 г.). Отдадим должное герцогу Брауншвейгскому, который обратил внимание на вундеркинда Гаусса и позаботился о его обучении. В 1795–1798 годах юный гений учился в Геттингенском университете, в 1799 г. он получил степень доктора, а с 1807 г. до самой смерти он спокойно работал в качестве директора астрономической обсерватории и профессора математики Гёттингенского университета. Как и его великие современники Кант, Гёте, Бетховен и Гегель, Гаусс не вмешивался в яростные политические события той эпохи («Буря и натиск», наполеоновские войны, Великая Французская революция и т. п.), но в области математики он очень ярко выразил новые идеи своего века.

Обладая феноменальными вычислительными способностями, Гаусс составил огромные таблицы простых чисел (ему были известны все простые числа, меньшие пяти миллионов) и самостоятельно, путем внимательного их разглядывания, открыл квадратичный закон взаимности (до Гаусса этот закон впервые подметил Эйлер, но не смог его доказать): если p и q — два нечетных простых числа, то

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Сам Гаусс не пользовался для записи этого закона символом Лежандра, хотя знал этот формализм (Лежандр был на 20 лет старше Гаусса), да и выражения «квадратичная взаимность» у Гаусса нет (его потом придумал Дирихле). В знаменитой книге Гаусса «Арифметические исследования», которая считается родоначальницей современной теории чисел (издана в Лейпциге, в 1801 г.), отмечается, что сам закон квадратичной взаимности впервые сформулировал Эйлер, подробно обсуждал

Лежандр, но до 1801 г. не было опубликовано ни одного строгого доказательства этого закона. Свое первое доказательство закона взаимности Гаусс (а он, впоследствии, придумал их аж шесть штук!) получил в 1796 г. [1]), в девятнадцатилетнем возрасте, ценой невероятного напряжения. На отыскание первого доказательства у Гаусса ушло более года работы, которая, по меткому выражению Кроннекера, явилась серьезной «пробой гауссовского гения». Столь выдающийся результат Гаусса был назван современниками (конечно, не всеми, а только смыслящими в математике) «золотая теорема» («theorema aurum»). Давайте и мы познакомимся с этой золотой теоремой.

Нам понадобится несколько дополнительных свойств символа Лежандра $\left(\frac{a}{p}\right)$, которые я сформулирую в виде лемм.

Пусть p — нечетное простое число, $S = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ — множество всех положительных чисел из приведенной системы вычетов по модулю p. Рассмотрим сравнение $a \cdot s \equiv \varepsilon_s r_s (\mathrm{mod}\, p)$, где a — числитель исследуемого символа Лежандра, $s \in S$, $\varepsilon_s r_s$ — абсолютно наименьший вычет числа as по модулю p (т. е. вычет, абсолютная величина которого наименьшая), r_s — абсолютная величина этого вычета, а ε_s, стало быть, его знак. Таким образом, $r_s \in S$, а $\varepsilon_s = \pm 1$.

Лемма 1 (Гаусс). $\left(\frac{a}{p}\right) = \prod_{s \in S} \varepsilon_s$.

Доказательство. Рассмотрим сравнения

$$\left\{\begin{array}{c} a \cdot 1 \equiv \varepsilon_1 r_1 (\mathrm{mod}\, p) \\ a \cdot 2 \equiv \varepsilon_2 r_2 (\mathrm{mod}\, p) \\ \vdots \\ a \cdot \frac{p-1}{2} \equiv \varepsilon_{\frac{p-1}{2}} p_{\frac{p-1}{2}} (\mathrm{mod}\, p). \end{array}\right. \qquad (*)$$

Множество чисел

$$\{\pm as | s \in S\} = \left\{a \cdot 1, -a \cdot 1, a \cdot 2, -a \cdot 2, \ldots, a \cdot \frac{p-1}{2}, -a \cdot \frac{p-1}{2}\right\}$$

[1]) Вторая запись в дневнике Гаусса имеет дату 8 апреля 1796 г. В этой записи Гаусс отмечает, что им наконец-то найдено строгое доказательство «золотой» гипотезы Эйлера.

является приведенной системой вычетов по модулю p (см. п. 17, лемма 2). Их абсолютно наименьшие вычеты соответственно суть

$$\{\pm\varepsilon_s r_s | s \in S\} = \left\{\varepsilon_1 r_1, -\varepsilon_1 r, \varepsilon_2 r_2, -\varepsilon_2 r_2, \ldots, \varepsilon_{\frac{p-1}{2}} r_{\frac{p-1}{2}}, -\varepsilon_{\frac{p-1}{2}} r_{\frac{p-1}{2}}\right\},$$

положительные же из них, т. е. $r_1, r_2, \ldots, r_{\frac{p-1}{2}}$, совпадают с числами $1, 2, \ldots, \dfrac{p-1}{2}$, т. е. образуют множество S. Перемножим теперь почленно сравнения $(*)$ и сократим произведение на

$$1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} = r_1 \cdot r_2 \cdot \ldots \cdot r_{\frac{p-1}{2}} = \prod_{s \in S} s.$$

Получим

$$a^{\frac{p-1}{2}} \equiv \varepsilon_1 \varepsilon_2 \ldots \varepsilon_{\frac{p-1}{2}} (\mathrm{mod}\, p).$$

Согласно критерию Эйлера из предыдущего пункта, $a^{\frac{p-1}{2}} \equiv \left(\dfrac{a}{p}\right) (\mathrm{mod}\, p)$, т. е. $\left(\dfrac{a}{p}\right) = \prod\limits_{s \in S} \varepsilon_s$, что и требовалось. ♦

Лемма 2. *При нечетном a верно*

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\frac{p^2-1}{8} + \sum\limits_{s \in S} \left[\frac{as}{p}\right]},$$

где $\left[\dfrac{as}{p}\right]$ — целая часть числа $\dfrac{as}{p}$.

Доказательство. Имеем

$$\left[\frac{2as}{p}\right] = \left[2 \cdot \left[\frac{as}{p}\right] + 2\left\{\frac{as}{p}\right\}\right] = 2 \cdot \left[\frac{as}{p}\right] + \left[2\left\{\frac{as}{p}\right\}\right],$$

что будет четным или нечетным, в зависимости от того, будет ли наименьший неотрицательный вычет числа as меньше или больше числа $\dfrac{p}{2}$, т. е. будет ли $\varepsilon_s = 1$ или $\varepsilon_s = -1$. Отсюда, очевидно,

$$\varepsilon_s = (-1)^{\left[\frac{2as}{p}\right]},$$

поэтому, в силу леммы Гаусса,

$$\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{s \in S} \left[\frac{2as}{p}\right]}.$$

Преобразуем это равенство (помним, что $a+p$ — четное, а квадратичный множитель из числителя символа Лежандра можно отбрасывать):

$$\left(\frac{2a}{p}\right)=\left(\frac{2a+2p}{p}\right)=\left(\frac{4\dfrac{a+p}{2}}{p}\right)=\left(\frac{\dfrac{a+p}{2}}{p}\right)=$$

$$=(-1)^{\sum\limits_{s\in S}\left[\frac{(a+p)s}{p}\right]}=(-1)^{\sum\limits_{s\in S}\left[\frac{as}{p}\right]+\sum\limits_{s\in S}s}.$$

Поскольку $\left(\dfrac{2a}{p}\right)=\left(\dfrac{2}{p}\right)\left(\dfrac{a}{p}\right)$, а

$$\sum_{s\in S}s=1+2+\ldots+\frac{p-1}{2}=\frac{p^2-1}{8},$$

то лемма 2 доказана. ♦

Лемма 3. $\left(\dfrac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$.

Доказательство непосредственно следует из леммы 2 при $a=1$. ♦

Ни у кого не должно возникать недоумения по поводу возможности деления числа $p^2-1=(p-1)(p+1)$ на 8 нацело, так как из двух последовательных четных чисел одно обязательно делится на 4. Кроме того, простое число p можно представить в виде $p=8n+k$, где k — одно из чисел 1, 3, 5, 7. Так как число

$$\frac{(8n+k)^2-1}{8}=8n^2+2nk+\frac{k^2-1}{8}$$

будет четным при $k=1$ и $k=7$, то 2 будет квадратичным вычетом по модулю p, если p имеет вид $8n+1$ или $8n+7$. Если же p имеет вид $8n+3$ или $8n+5$, то 2 будет квадратичным невычетом.

Теорема (закон взаимности квадратичных вычетов). *Если p и q — нечетные простые числа, то*

$$\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right).$$

Другими словами, *если хоть одно из чисел p или q имеет вид $4n+1$, то p — квадрат по модулю q тогда и только тогда,*

когда q — квадрат по модулю p. Если же оба числа p и q имеют вид $4n+3$, то p — квадрат по модулю q тогда и только тогда, когда q не является квадратом по модулю p.

Доказательство. Поскольку $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, то формула из леммы 2 принимает вид

$$\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{s=1}^{\frac{p-1}{2}} \left[\frac{as}{p}\right]}.$$

Рассмотрим два множества:

$$S = \left\{1, 2, \ldots, \frac{p-1}{2}\right\} \quad \text{и} \quad K = \left\{1, 2, \ldots, \frac{q-1}{2}\right\}.$$

Образуем $\frac{p-1}{2} \cdot \frac{q-1}{2}$ пар чисел (qx, py), где x пробегает множество S, а y пробегает множество K. Первая и вторая компонента одной пары никогда не совпадают, ибо из $py = qx$ следует, что py кратно q. Но ведь это невозможно, так как $(p, q) = 1$ и, поскольку $0 < y < q$, то $(y, q) = 1$. Положим, поэтому, $\frac{p-1}{2} \cdot \frac{q-1}{2} = V_1 + V_2$, где V_1 — число пар, в которых первая компонента меньше второй $(qx < py)$, V_2 — число пар, в которых вторая компонента меньше первой $(qx > py)$.

Очевидно, что V_1 есть число пар, в которых $x < \frac{p}{q}y$. (Вообще-то, $x \leqslant \frac{p-1}{2}$, но $\frac{p}{q}y < \frac{p}{2}$ так как $\frac{y}{q} < \frac{1}{2}$, следовательно, $\left[\frac{p}{q}y\right] \leqslant \left[\frac{p}{2}\right] = \frac{p-1}{2}$ и неравенство $x < \frac{p}{q}y$ не противоречит неравенству $x \leqslant \frac{p-1}{2}$.) Поэтому

$$V_1 = \sum_{y \in K} \left[\frac{p}{q}y\right].$$

Аналогично,

$$V_2 = \sum_{x \in S} \left[\frac{q}{p}x\right].$$

Тогда равенство из леммы 2, отмеченное в начале этого доказательства, дает

$$\left(\frac{p}{q}\right) = (-1)^{V_1}, \left(\frac{q}{p}\right) = (-1)^{V_2}.$$

Это означает, что

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{V_1+V_2} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

а это, собственно, и требовалось. ♦

Справедливости ради следует отметить мелким шрифтом, что мы могли бы доказать закон взаимности в этом пункте сразу после леммы 1, но при этом упустили бы из виду важные свойства символа Лежандра, которые спрашивают на кандидатском экзамене по специальности «Алгебра, математическая логика и теория чисел». Кроме того, «быстрое» доказательство закона взаимности страдает существенным недостатком — совершенно непонятно, как до него додуматься. А додумался до него немецкий математик Фердинанд Готхольд Эйзенштейн (1823–1852). Это доказательство, дословно почерпнутое из замечательной книжки Ж. П. Серра «Курс арифметики», — перед вами.

Тригонометрическая лемма. Пусть m — нечетное натуральное число. Тогда

$$\frac{\sin mx}{\sin x} = (-4)^{\frac{m-1}{2}} \prod_{1\leqslant j\leqslant\frac{m-1}{2}} \left(\sin^2 x - \sin^2\frac{2\pi j}{m}\right).$$

Доказательство получается непосредственной проверкой. Например, с помощью формулы Муавра убеждаемся, что левая часть есть полином степени $\dfrac{m-1}{2}$ от $\sin^2 x$, корни которого есть $\sin^2(2\pi j/m)$, где $1 \leqslant j \leqslant \dfrac{m-1}{2}$. Множитель $(-4)^{\frac{m-1}{2}}$ получается сравнением коэффициентов в левой и правой частях.

Доказательство закона взаимности. Пусть p и q — два различных нечетных простых числа. По лемме Гаусса, $\left(\dfrac{q}{p}\right) = \prod\limits_{s\in S} \varepsilon_s$. В силу равенства $qs = \varepsilon_s r_s$ (обозначения леммы 1 сохранены), имеем

$$\sin\frac{2\pi}{p}qs = \varepsilon_s \sin\frac{2\pi}{p}r_s.$$

(Синус-то — функция нечетная, и знак можно вынести вперед.)

Перемножая эти равенства и учитывая, что отображение $s \mapsto r_s$ биективно, получаем

$$\left(\frac{q}{p}\right) = \prod_{s\in S}\varepsilon_s = \prod_{s\in S}\left(\sin\frac{2\pi qs}{p} \Big/ \sin\frac{2\pi s}{p}\right).$$

Применим теперь тригонометрическую лемму при $m = q$:

$$\left(\frac{q}{p}\right) = \prod_{s\in S}(-4)^{\frac{q-1}{2}} \prod_{t\in K}\left(\sin^2\frac{2\pi s}{p} - \sin^2\frac{2\pi t}{q}\right) =$$

$$= (-4)^{\frac{(q-1)(p-1)}{4}} \prod_{s\in S,t\in K}\left(\sin^2\frac{2\pi s}{p} - \sin^2\frac{2\pi t}{q}\right),$$

где $K = \left\{1, 2, \ldots, \dfrac{q-1}{2}\right\}$. Меняя роли q и p, точно так же получим

$$\left(\frac{p}{q}\right) = (-4)^{\frac{(q-1)(p-1)}{4}} \prod_{s\in S,t\in K}\left(\sin^2\frac{2\pi t}{q} - \sin^2\frac{2\pi s}{p}\right).$$

Множители в формулах для $\left(\dfrac{q}{p}\right)$ и $\left(\dfrac{p}{q}\right)$ одинаковы с точностью до знака. Число же противоположных знаков равно $\dfrac{(p-1)(q-1)}{4}$, поэтому $\left(\dfrac{q}{p}\right) = \left(\dfrac{p}{q}\right)(-1)^{\frac{(p-1)(q-1)}{4}}$. ♦

На этом п. 23 и с ним весь параграф, посвященный теории сравнений закончим. С удовлетворением отмечу, что если мы и не все познали в сравнении, то весьма немало. Примите мои сердечные поздравления.

Задачки

1. Используя закон взаимности для «переворачивания» символа Лежандра, посчитайте:
а) $\left(\dfrac{59}{269}\right)$; б) $\left(\dfrac{37}{557}\right)$; в) $\left(\dfrac{43}{991}\right)$.

2. Докажите, что число a одновременно является или квадратичным вычетом или квадратичным невычетом для всех простых чисел, входящих в арифметическую прогрессию $4at + r, t = 0, 1, 2, \ldots$, где r — произвольное натуральное число, меньшее $4a$. [1])

3. Пусть p и q — простые числа и $p + q = 4a$. Докажите, что тогда число a является одновременно или квадратичным вычетом по модулям p и q или кадратичным невычетом.

[1]) В 1847 г. Л. Эйлер подметил закон взаимности именно в такой формулировке.

§ 5. ТРАНСЦЕНДЕНТНЫЕ ЧИСЛА

В этом параграфе мы снова покинем прекрасное и уютное царство целых чисел, по которому разгуливали, изучая теорию сравнений. Если проследить историю возникновения и развития знаний человечества о числах, то выявится довольно парадоксальный факт — на протяжении почти всей своей многовековой истории человечество использовало на практике и пристально изучало исключительно малую долю всего множества живущих в природе чисел. Люди долгое время совершенно не подозревали о существовании, как выяснилось впоследствии, подавляющего большинства действительных чисел, наделенных удивительными и загадочными свойствами и называемых теперь трансцендентными. Судите сами (перечисляю ориентировочные этапы развития понятия действительного числа):

1. Идущая из глубины тысячелетий гениальная математическая абстракция натурального числа.

Гениальность этой абстракции поражает, а ее значение для развития человечества превосходит, наверное, даже изобретение колеса. Мы привыкли к ней настолько, что перестали восхищаться этим самым выдающимся достижением человеческого разума. Однако попробуйте, для пущей достоверности представив себя не студентом-математиком, а первобытным человеком, или, скажем, студентом-филологом, сформулировать точно, что общего имеется между тремя хижинами, тремя быками, тремя бананами и тремя ультразвуковыми томографами. Объяснять нематематику, что такое натуральное число «три» — почти безнадежная затея, однако уже пятилетний человеческий детеныш внутренне ощущает эту абстракцию и в состоянии разумно оперировать с ней, выпрашивая у мамы три конфеты вместо двух.

2. Дроби, т. е. положительные рациональные числа.

Дроби естественно возникли при решении задач о разделе имущества, измерении земельных участков, исчислении времени

и т. п. В древней Греции рациональные числа вообще являлись символом гармонии окружающего мира и проявлением божественного начала, а все отрезки, до некоторого времени, считались соизмеримыми, т. е. отношение их длин обязано было выражаться рациональным числом, иначе — труба (а боги этого допустить не могут).

3. Отрицательные числа и ноль.

Отрицательные числа первоначально трактовались как долг при финансовых и бартерных расчетах, однако потом выяснилось, что без отрицательных чисел и в других областях человеческой деятельности никуда не денешься (кто не верит, пусть посмотрит зимой на градусник за окном). Число ноль, на мой взгляд, первоначально служило скорее не символом пустого места и отсутствием всякого количества, а символом равенства и завершенности процесса расчетов (сколько был должен соседу, столько ему и отдал, и вот теперь — ноль).

4. Иррациональные алгебраические числа.

Иррациональные числа открыли в пифагорейской школе при попытке соизмерить диагональ квадрата с его стороной, но хранили это открытие в страшной тайне — как бы смуты не вышло! В это открытие посвящались только наиболее психически устойчивые и проверенные ученики, а истолковывалось оно как отвратительное явление, нарушающее гармонию мира. Но нужда и война заставили человечество учиться решать алгебраические уравнения не только первой степени с целыми коэффициентами. После Галилея снаряды стали летать по параболам, после Кеплера планеты полетели по эллипсам, механика и баллистика стали точными науками и везде нужно было решать и решать уравнения, корнями которых являлись иррациональные числа. Поэтому с существованием иррациональных корней алгебраических уравнений пришлось смириться, какими бы отвратительными они не казались. Более того, методы решения кубических уравнений и уравнений четвертой степени, открытые в XVI в. итальянскими математиками Сципионом дель Ферро, Никколо Тартальей (Тарталья — это прозвище, означающее в переводе — заика, настоящей его фамилии я не знаю), Людовиком Феррари и Рафаэлем Бомбелли привели к изобретению совсем уж «сверхъестественных» комплексных чисел, которым суждено было получить полное признание только в XIX в. Алгебраические иррациональности прочно вошли в человеческую практику уже с XVI в.

В этой истории развития понятия числа не нашлось места для трансцендентных чисел, т. е. чисел не являющихся корнями никакого алгебраического уравнения с рациональными или, что равносильно (после приведения к общему знаменателю), целыми коэффициентами. Правда, еще древние греки знали замечательное число π, которое, как выяснилось впоследствии, трансцендентно, но они знали его только как отношение длины окружности к ее диаметру. Вопрос об истинной природе этого числа вообще мало кого интересовал до тех пор, пока люди вдоволь и безуспешно не нарешались древнегреческой задачей о квадратуре круга, а само число π каким-то загадочным образом повылезало в разных разделах математики и естествознания.

Лишь только в 1844 г. Лиувилль построил исторически первый пример трансцендентного числа, а математический мир удивился самому факту существования таких чисел. Лишь только в XIX в. гениальный Георг Кантор понял, используя понятие мощности множества, что на числовой прямой трансцендентных чисел подавляющее большинство. Лишь только в пятом параграфе этой небольшой книжки мы, наконец-то, обратим на трансцендентные числа свое внимание.

24. Мера и категория на прямой

В этом пункте я приведу некоторые предварительные сведения из математического анализа, необходимые для понимания дальнейшего изложения. В математике придумано довольно много различных формализаций понятия «малости» множества. Нам понадобятся два из них — множества меры нуль и множества первой категории по Бэру. Оба эти понятия опираются на понятие счетности множества. Известно, что множество рациональных чисел счетно ($|\mathbf{Q}| = \aleph_0$), и что любое бесконечное множество содержит счетное подмножество, т. е. счетные множества самые «маленькие» из бесконечных. Между любым счетным множеством и множеством натуральных чисел $\mathbf{N}$ существует биективное отображение, т. е. элементы любого счетного множества можно перенумеровать, или, другими словами, любое счетное множество можно выстроить в последовательность. Ни один интервал на прямой не является счетным множеством. Это, очевидно, вытекает из следующей теоремы.

Теорема 1 (Кантор). *Для любой последовательности $\{a_n\}$ действительных чисел и для любого интервала I существует точка $p \in I$ такая, что $p \neq a_n$ для любого $n \in \mathbf{N}$.*

Доказательство. Процесс. Берем отрезок (именно отрезок, вместе с концами) $I_1 \subset I$ такой, что $a_1 \notin I_1$. Из отрезка I_1 берем отрезок $I_2 \subset I_1$ такой, что $a_2 \notin I_2$ и т. д. Продолжая процесс, из отрезка I_{n-1} берем отрезок $I_n \subset I_{n-1}$ такой, что $a_n \notin I_n$. В результате этого процесса получаем последовательность вложенных отрезков $I_1 \supset I_2 \supset \ldots \supset I_n \supset \ldots$, пересечение $\bigcap\limits_{n=1}^{\infty} I_n$ которых, как известно с первого курса, непусто, т. е. содержит некоторую точку $p \in \bigcap\limits_{n} I_n$. Очевидно, что $p \neq a_n$ при всех $n \in \mathbf{N}$.

♦

Я не думаю, что читатели ранее не встречались с этим изящным доказательством, просто идея этого доказательства далее будет использована при доказательстве теоремы Бэра и поэтому ее полезно напомнить заранее.

Определение. Множество A *плотно в интервале* I, если оно имеет непустое пересечение с каждым подынтервалом из I. Множество A плотно, если оно плотно в $\mathbf{R}$. Множество A *нигде не плотно*, если оно не плотно ни в каком интервале на действительной прямой, т. е. каждый интервал на прямой содержит подынтервал, целиком лежащий в дополнении к A.

Легко понять, что множество A нигде не плотно тогда и только тогда, когда его дополнение A' содержит плотное открытое множество. Легко понять, что множество A нигде не плотно тогда и только тогда, когда его замыкание $\overline{A}$ не имеет ни одной внутренней точки.

Нигде не плотные множества на прямой интуитивно ощущаются маленькими в том смысле, что в них полным полно дыр и точки такого множества расположены на прямой довольно редко. Некоторые свойства нигде не плотных множеств сформулируем скопом в виде теоремы.

Теорема 2. 1) *Любое подмножество нигде не плотного множества нигде не плотно.*

2) *Объединение двух* (*или любого конечного числа*) *нигде не плотных множеств нигде не плотно.*

3) *Замыкание нигде не плотного множества нигде не плотно.*

Доказательство. 1) Очевидно.

2) Если A_1 и A_2 нигде не плотны, то для каждого интервала I найдутся интервалы $I_1 \subset (I \backslash A_1)$ и $I_2 \subset (I_1 \backslash A_2)$. Значит, $I_2 \subset I \backslash (A_1 \cup A_2)$, а это означает, что $A_1 \cup A_2$ нигде не плотно.

3) Очевидно, что любой открытый интервал, содержащийся в A', содержится также и в $\left(\overline{A}\right)'$. ♦

Таким образом, класс нигде не плотных множеств замкнут относительно операции взятия подмножеств, операции замыкания и конечных объединений. Счетное объединение нигде не плотных множеств, вообще говоря, не обязано быть нигде не плотным множеством. Пример тому — множество рациональных чисел, которое всюду плотно, но является счетным объединением отдельных точек, каждая из которых образует одноэлементное нигде не плотное множество в $\mathbf{R}$.

Определение. Множество, которое можно представить в виде конечного или счетного объединения нигде не плотных множеств, называется *множеством первой категории* (по Бэру). Множество, которое нельзя представить в таком виде, называется *множеством второй категории*.

Теорема 3. 1) *Дополнение любого множества первой категории на прямой является плотным.*

2) *Никакой интервал в* $\mathbf{R}$ *не является множеством первой категории.*

3) *Пересечение любой последовательности плотных открытых множеств является плотным множеством.*

Доказательство. Три сформулированных в теореме свойства являются по существу эквивалентными. Докажем первое.

Пусть $A = \bigcup\limits_n A_n$ — представление множества A первой категории в виде счетного объединения нигде не плотных множеств, I — произвольный интервал. Далее — такой же процесс, как в доказательстве теоремы Кантора. Выберем отрезок (именно отрезок, вместе с концами) $I_1 \subset (I \backslash A_1)$. Это возможно сделать, так как в дополнении к нигде не плотному множеству A_1 внутри интервала I всегда найдется целый подынтервал, а он, в свою очередь, содержит внутри себя целый отрезок. Выберем отрезок $I_2 \subset (I_1 \backslash A_2)$. Выберем отрезок $I_3 \subset (I_2 \backslash A_3)$ и т. д. Пересечение вложенных отрезков $\bigcap\limits_n I_n$ не пусто, следовательно, дополнение $I \backslash A$ не пусто, а это означает, что дополнение A' плотно.

Второе утверждение теоремы непосредственно следует из первого, третье утверждение также следует из первого, если только сделать над собой усилие и перейти к дополнениям последовательности плотных открытых множеств. ♦

Определение. Класс множеств, содержащий всевозможные конечные или счетные объединения своих членов и любые подмножества своих членов, называется *σ-идеалом.*

Очевидно, что класс всех не более чем счетных множеств является σ-идеалом. После небольших размышлений легко понять, что класс всех множеств первой категории на прямой также является σ-идеалом. Еще один интересный пример σ-идеала дает класс так называемых нуль-множеств (или множеств меры нуль).

Определение. Множество $A \subset \mathbf{R}$ называется *множеством меры нуль* (*нуль-множеством*), если A можно покрыть не более чем счетной совокупностью интервалов, суммарная длина которых меньше любого наперед заданного числа $\varepsilon > 0$, т. е. для любого $\varepsilon > 0$ существует такая последовательность интервалов I_n, что $A \subset \bigcup\limits_n I_n$ и $\sum |I_n| < \varepsilon$.

Понятие нуль-множества является другой формализацией интуитивного понятия «малости» множества: нуль-множества — это множества маленькие по длине. Очевидно, что отдельная точка является нуль-множеством и что любое подмножество нуль-множества само является нуль-множеством. Поэтому тот факт, что нуль-множества образуют σ-идеал вытекает из следующей теоремы.

Теорема 4 (Лебег). *Пусть $A = \cup A_i$ и A_i — нуль-множество, $i = 1, 2, \ldots$. Любое счетное объединение нуль-множеств является нуль-множеством.*

Доказательство. Пусть A_i — нуль-множества, $i = 1, 2, \ldots$. Тогда для каждого i существует последовательность интервалов I_{ij} $(j = 1, 2, \ldots)$ такая, что $A_i \subset \bigcup\limits_j I_{ij}$ и $\sum\limits_j |I_{ij}| < \dfrac{\varepsilon}{2^i}$. Множество всех интервалов I_{ij} покрывает A и сумма их длин меньше ε, так как $\sum\limits_{i,j} |I_{ij}| < \sum\limits_i \dfrac{\varepsilon}{2^i} = \varepsilon$. Значит, A — нуль-множество. ♦

Никакой интервал или отрезок не является нуль-множеством, так как справедлива

Теорема 5 (Гейне–Борель). *Если конечная или бесконечная последовательность интервалов I_n покрывает интервал I, то*

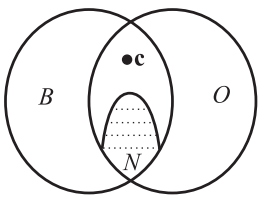
$$\sum |I_n| \geqslant |I|\,. \qquad \blacklozenge$$

Я не буду приводить здесь доказательство этой интуитивно очевидной теоремы, ибо его можно найти в любом мало-мальски серьезном курсе математического анализа.

Из теоремы Гейне-Бореля следует, что σ-идеал нуль-множеств, подобно σ-идеалам не более чем счетных множеств и множеств первой категории, не содержит интервалов и отрезков. Общим между этими тремя σ-идеалами является также то, что они включают в себя все конечные и счетные множества. Кроме того, существуют несчетные множества первой категории меры нуль. Наиболее знакомый пример такого множества — канторово совершенное [1]) множество $\mathbf{c} \subset [0;1]$, состоящее из чисел, в троичной записи которых нет единицы. Вспомните процесс построения канторова совершенного множества: отрезок $[0;1]$ делится на три равные части и средний открытый интервал выкидывается. Каждая из двух оставшихся третей отрезка снова делится на три равные части и средние открытые интервалы из них выкидываются и т. д. Очевидно, что оставшееся после этого процесса множество нигде не плотно, т. е. первой категории. Легко подсчитать, что суммарная длина выкинутых средних частей равна единице, т. е. $\mathbf{c}$ имеет меру нуль. Известно, что $\mathbf{c}$ несчетно, так как несчетно множество бесконечных последовательностей, состоящих из нулей и двоек (каждый элемент $\mathbf{c}$ представляется троичной дробью, в которой после запятой идет именно последовательность из нулей и двоек).

Предлагаю читателям самостоятельно проверить, что существуют множества первой категории, не являющиеся нуль-множествами, и существуют нуль-множества, не являющиеся множествами первой категории (впрочем, если вас затруднит придумывание соответствующих примеров, не отчаивайтесь, а просто дочитайте этот пункт до теоремы 6).

Таким образом, картинка соотношений между рассматриваемыми тремя σ-идеалами такова:



N — не более чем счетные множества
B — множества первой категории
O — множества меры нуль

Итак, мы ввели два понятия малости множеств. Нет ничего парадоксального, что множество, малое в одном смысле, может в другом смысле оказаться большим. Следующая теорема

[1]) Множество называется совершенным, если оно замкнуто и не содержит изолированных точек.

неплохо иллюстрирует эту мысль и показывает, что в некоторых случаях введенные нами понятия малости могут оказаться диаметрально противоположными.

Теорема 6. *Числовую прямую можно разбить на два дополняющих друг друга множества A и B так, что A есть множество первой категории, а B имеет меру нуль.*

Доказательство. Пусть $a_1, a_2, \dots, a_n, \dots$ — занумерованное множество рациональных чисел (или любое другое счетное всюду плотное подмножество $\mathbf{R}$). Пусть I_{ij} — открытый интервал длины $1/2^{i+j}$ с центром в точке a_i. Рассмотрим множества

$$G_j = \bigcup_{i=1}^{\infty} I_{ij}, \quad j = 1, 2, \dots; \quad B = \bigcap_{j=1}^{\infty} G_j; \quad A = R \backslash B = B'.$$

Очевидно, что для любого $\varepsilon > 0$ можно выбрать j так, что $1/2^j < \varepsilon$. Тогда

$$B \subset \bigcup_i I_{ij},$$

$$\sum_i |I_{ij}| = \sum_i \frac{1}{2^{i+j}} = \frac{1}{2^j} < \varepsilon,$$

следовательно, B — нуль-множество.

Далее, $G_j = \bigcup\limits_{i=1}^{\infty} I_{ij}$ — плотное открытое подмножество $\mathbf{R}$, так как оно есть объединение последовательности открытых интервалов и содержит все рациональные точки. Это означает, что его дополнение G_j' нигде не плотно, следовательно $A = B' = \bigcup\limits_j G_j'$ — множество первой категории. ♦

Не правда ли, удивительный результат! Из доказанной теоремы следует, что каждое подмножество прямой, оказывается, можно представить в виде объединения нуль-множества и множества первой категории. В следующем пункте мы рассмотрим конкретное разбиение $\mathbf{R}$ на два подмножества, одно из которых — трансцендентные числа Лиувилля — меры нуль, но второй категории по Бэру. Скорей в следующий пункт!

Задачки

1. Приведите пример двух всюду плотных множеств, пересечение которых не является всюду плотным. Приведите пример всюду плотного множества, дополнение до которого также всюду плотно.

2. Существует ли несчетное множество меры нуль, плотное на отрезке $[0;1]$?

3. Какова мера и категория множества тех точек отрезка $[0;1]$, которые допускают разложение в десятичную дробь без использования цифры 7?

4. Какова мера и категория множества тех точек отрезка $[0;1]$, в записи которых в виде бесконечной двоичной дроби на всех четных местах стоят нули? Является ли это множество совершенным?

5. Пусть множество E на отрезке $[0;1]$ имеет меру нуль. Является ли его замыкание множеством меры нуль?

6. Пусть множество E нигде не плотно на отрезке $[0;1]$ и имеет меру нуль. Является ли его замыкание множеством меры нуль?

7. Существуют ли такие два всюду плотные несчетные множества на прямой, пересечение которых пусто?

8. Постройте на отрезке $[0;1]$ совершенное нигде не плотное множество ненулевой меры.

9. Пусть $s>0$, $A\subseteq\mathbf{R}$. Говорят, что множество A имеет нулевую s-мерную меру Хаусдорфа, если для любого $\varepsilon>0$ существует последовательность интервалов I_n такая, что $A\subseteq\bigcup\limits_{n=1}^{\infty}I_n$, $\sum\limits_{n=1}^{\infty}|I_n|^s<\varepsilon$ и $|I_n|<\varepsilon$ при всех n. Докажите, что семейство всех множеств нулевой s-мерной меры Хаусдорфа образует σ-идеал; при $s=1$ он совпадает с классом нуль-множеств, а при $0<s<1$ является его собственным подклассом.

10. Пусть последовательность $f_n(x)$ непрерывных функций поточечно сходится к функции $f(x)$ на отрезке $[0;1]$. Докажите, что множество точек разрыва функции $f(x)$ на этом отрезке является множеством первой категории. [1)]

25. Числа Лиувилля

Определение 1. Число $z\in\mathbf{C}$ называется *алгебраическим*, если оно является корнем некоторого алгебраического уравнения

$$a_nz^n+\ldots+a_2z^2+a_1z^1+a_0=0,$$

все коэффициенты $a_0,a_1,\ldots,a_n$ которого суть целые числа, не равные одновременно нулю.

[1)] Именно для выяснения, сколь большим может быть множество точек разрыва поточечного предела последовательности непрерывных функций, Бэр и придумал понятие категории.

Безусловно, множество алгебраических чисел не изменится, если в определении 1 коэффициентам алгебраического уравнения позволить быть произвольными рациональными числами, но нам удобнее пока считать эти коэффициенты целыми.

Определение 2. *Степенью алгебраического числа* называется наименьшая степень уравнения с целыми коэффициентами, которому это число удовлетворяет.

Пример. Число $\sqrt{2}$ — алгебраическое степени 2, так как оно есть корень уравнения $x^2 - 2 = 0$, но не является корнем никакого уравнения степени 1 с целыми коэффициентами. Действительно, если $a\sqrt{2} + b = 0$, то $\sqrt{2} = \dfrac{-b}{a} = \dfrac{m}{n}$ и пусть $\dfrac{m}{n}$ — несократимая дробь. Следовательно, $2n^2 = m^2$, т. е. m — четно, $m = 2k$, $2n^2 = 4k^2$, $n^2 = 2k^2$, значит, n — четно, что противоречит несократимости дроби $\dfrac{m}{n}$.

Теорема 1. *Множество A всех алгебраических чисел счетно.*

Доказательство. Для любого многочлена с целыми коэффициентами $a_n z^n + \ldots + a_2 z^2 + a_1 z^1 + a_0$, $a_n \neq 0$, определим натуральное число $p = n + \sum\limits_{k=0}^{n} |a_k|$ — вес этого многочлена. Очевидно, что для любого заданного веса p существует лишь конечное число многочленов, имеющих такой вес. Следовательно, многочленов с целыми коэффициентами счетное число, и, поскольку каждый многочлен имеет лишь конечное число корней, множество A всех алгебраических чисел счетно. ♦

Из этой простенькой теоремы, открытой Георгом Кантором, вытекает

Следствие. *Существует целый континуум неалгебраических чисел*!

Определение 3. Число $\alpha \in \mathbf{R}$, не являющееся алгебраическим, называется *трансцендентным*.

Теорема 1 эффектна, изящна и проста, поэтому трудно ожидать от нее каких-то реальных конструктивных следствий. Она лишь утверждает существование трансцендентных чисел, но не дает ни одного конкретного примера. Исторически первый пример трансцендентного числа построил, как уже отмечалось,

в 1844 г. некто Лиувилль, и мы сейчас приступаем к воспроизведению произведения этого выдающегося француского некто.

Лемма (Лиувилль). *Для любого действительного алгебраического числа z степени $n > 1$ (т. е. иррационального) найдется натуральное число M такое, что*

$$\left|z - \frac{p}{q}\right| > \frac{1}{Mq^n}$$

при всех целых p и q, $q > 0$.

Доказательство. Пусть $f(x)$ — тот самый многочлен степени n с целыми коэффициентами, для которого $f(z) = 0$. Поскольку производная $f'(x)$ многочлена $f(x)$ есть функция, ограниченная на отрезке $|z - x| \leqslant 1$, то найдется такое натуральное число M, что $|f'(x)| \leqslant M$ для всех x из отрезка $\|z - x| \leqslant 1$. По теореме о среднем значении:

$$|f(x)| = |f(z) - f(x)| \leqslant M \cdot |z - x|\,.$$

Возьмем теперь любые два целых числа p и q, $q > 0$, и вспомним, что нужно показать $\left|z - \frac{p}{q}\right| > \frac{1}{Mq^n}$. Очевидно, что это верно при $\left|z - \frac{p}{q}\right| > 1$, так как $M \geqslant 1$, $q \geqslant 1$. Пусть $\left|z - \frac{p}{q}\right| \leqslant 1$. Тогда

$$\left|f\left(\frac{p}{q}\right)\right| \leqslant M \cdot \left|z - \frac{p}{q}\right|.$$

Умножим полученное неравенство на q^n:

$$\left|q^n f\left(\frac{p}{q}\right)\right| \leqslant M \cdot q^n \cdot \left|z - \frac{p}{q}\right|.$$

Ясно, что уравнение $f(x) = 0$ не имеет рациональных корней, иначе число z имело бы меньшую степень (многочлен $f(x)$ разложился бы на множители, один из которых есть $\left(x - \frac{p}{q}\right)$, а иррациональное z оказалось бы корнем второго множителя меньшей степени). Таким образом, $f\left(\frac{p}{q}\right) \neq 0$, а $q^n f\left(\frac{p}{q}\right)$ — целое и не равное нулю число. Значит, $\left|q^n f\left(\frac{p}{q}\right)\right| \geqslant 1$, следовательно,

$$1 \leqslant M \cdot q^n \cdot \left|z - \frac{p}{q}\right|,$$

т. е.

$$\left|z-\frac{p}{q}\right| \geqslant \frac{1}{Mq^n}.$$

Равенство невозможно, так как z иррационально. [1)] ♦

В § 2, посвященном цепным дробям, мы немножечко поговорили о приближении действительных чисел рациональными дробями, отметив, в частности, что подходящая дробь — наилучшее приближение данного числа среди всех дробей, знаменатели которых не превосходят знаменатель подходящей дроби. Лемма Лиувилля тоже, фактически, относится к теории приближения действительных чисел рациональными, так как она говорит нам, что алгебраические числа весьма плохо приближаются рациональными дробями с заданным знаменателем. Возникает мысль, что именно этим своим свойством алгебраические числа вполне могут отличаться (и отличаться разительно) от других иррациональных чисел, если, конечно, таковые существуют. Идея, ударившая Лиувилля, как раз и заключалась в том, чтобы рассмотреть утверждение леммы как отличительное характеристическое свойство алгебраических иррациональностей. После этой простой, но сильной мысли, Лиувиллю для изобретения трансцендентных чисел оставалось совсем немного — придумать иррациональное число, которое очень хорошо приближается рациональными дробями, и проверить, что такое число обязано быть трансцендентным.

Определение 3. Действительное число z называется *числом Лиувилля*, если z иррационально и для каждого натурального n существуют целые p и q такие, что $q>1$ и

$$\left|z-\frac{p}{q}\right| < \frac{1}{q^n}.$$

Пример 1 (с помощью ряда). Рассмотрим число

$$z=\sum_{k=1}^{\infty}\frac{1}{10^{k!}} = 0,1+0,01+0,000001+\ldots = \\ = 0,11000100000000000000000100\ldots$$

[1)] Трудно объяснить, но меня почему-то приводит в восхищение последняя фраза из доказательства леммы Лиувилля: «Равенство невозможно, так как z иррационально» — кратко, просто и неоспоримо. Сказал — как отрезал. Кроме того, к моменту произнесения этой фразы читатели уже наверняка забыли (во всяком случае, студенты на лекции напрочь забывают), что нужно доказывать строгое неравенство, поэтому «нежданной шуткой огорошить» вдвойне приятно.

— в десятичной дроби единички стоят на месте с номером $k!$, остальные позиции заняты нулями. Число z иррационально, так как данная десятичная дробь не периодическая (действительно, пусть ее период имеет длину a; он должен содержать хоть одну единичку, но в записи этой дроби есть промежутки, состоящие из a нулей подряд.)

Пусть $n \in \mathbf{N}$. Возьмем $q = 10^{n!}$, $p = \sum\limits_{k=1}^{n} 10^{n!-k!}$. Тогда

$$\frac{p}{q} = 0,\underbrace{1100010\ldots01}_{n!\text{ знаков}} \text{ — рациональное число,}$$

$$\left|\sum_{k=1}^{\infty}\frac{1}{10^{k!}} - \frac{p}{10^{n!}}\right| = \left|0{,}00\ldots\underset{\substack{\uparrow\\ \text{позиция } (n+1)!}}{010}\ldots\right| < \frac{1}{q^n} = \frac{1}{10^{n!\cdot n}} =$$

$$= 0{,}00\ldots\underset{\substack{\uparrow\\ \text{позиция } n\cdot n!}}{010}\ldots,$$

так как $n \cdot n! < (n+1)! = (n+1) \cdot n!$. Итак, z — число Лиувилля.

Пример 2 (с помощью цепной дроби). Пусть

$$z = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cfrac{1}{\ddots\,\cfrac{}{q_s + \cfrac{1}{\ddots}}}}}},$$

где последовательность неполных частных $q_1 < q_2 < \ldots < q_s < \ldots$ возрастает так, что $q_{s+1} \geqslant Q_s^{s-2}$ (Q_s — знаменатель s-й подходящей дроби числа z). Тогда для произвольного натурального n возьмем в определении чисел Лиувилля $p = P_n$, $q = Q_n$ и вспомним свойства подходящих дробей:

$$\left|z - \frac{P_n}{Q_n}\right| < \left|\frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n}\right| = \frac{1}{Q_nQ_{n+1}} = \frac{1}{Q_n(q_{n+1}Q_n + Q_{n-1})} =$$

$$= \frac{1}{q_{n+1}Q_n^2 + Q_nQ_{n-1}} < \frac{1}{q_{n+1}Q_n^2} \leqslant \frac{1}{Q_n^n}.$$

Итак, z опять-таки окажется числом Лиувилля, как только я приведу пример достаточно быстро возрастающей последовательности $q_1 < q_2 < \ldots < q_s < \ldots$ неполных частных. Нужно, чтобы $q_{s+1} \geqslant Q_s^{s-2}$. Положим $q_1 = 0$, $q_2 = 1$ и начнем заполнять стандартную таблицу, вычисляя Q_s через уже вычисленные qs и q_{s-1}, а затем ставя на место q_{s+1} число Q_s^{s-2}:

n		1	2	3	4	5	6	7	…
q_s		0	1	1	$Q_3^1 = 2$	$Q_4^2 = 25$	$Q_5^3 = 2048388$	$Q_6^4 = \ldots$	…
Q_s	0	1	1	2	5	127	260145281	…	…

Вторая строчка получающейся таблицы как раз и содержит требуемую последовательность.

Используя известную формулу Стирлинга для факториалов больших чисел $n! \approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$, можно доказать, что скорость роста построенной последовательности $\sim n^n$, т. е. очень большая. Обратите внимание, что в примере 1 скорость роста знаменателей была того же порядка.

Теорема 2. *Любое число Лиувилля трансцендентно.*

Доказательство. Пусть некоторое число Лиувилля z оказалось алгебраическим степени n. Тогда $n > 1$, так как z — иррационально. По лемме Лиувилля найдется такое натуральное M, что

$$\left|z - \frac{p}{q}\right| > \frac{1}{Mq^n}$$

для всех целых p, q и $q > 0$. Пусть $k \in \mathbf{N}$ таково, что $2^k > 2^n M$. Так как z — число Лиувилля, то для этого k найдутся p и q, $q \geqslant 2$,

(тонкий момент! Целое число q — не ноль! И не единица! Значит, — не меньше двух!)

такие, что

$$\left|z - \frac{p}{q}\right| < \frac{1}{q^k},$$

следовательно,

$$\frac{1}{q^k} > \frac{1}{Mq^n}, \quad Mq^n > q^k,$$

и, после деления на q^n,

$$M > q^{k-n} \geqslant 2^{k-n} > M$$

— противоречие. ♦

Вот так, дорогие товарищи, получается, что числа из примеров 1 и 2 — самые что ни на есть трансцендентные. Посмотрите на них внимательно: ни один многочлен с целыми коэффициентами не может обратить их в ноль. Из примера 2 видно, что цепная дробь представляет собой число Лиувилля, если последовательность неполных частных растет очень быстро. Однако это лишь достаточное условие трансцендентности цепной дроби, но вовсе не необходимое. Зияющая пустота наших знаний о природе-матушке в этом круге вопросов состоит в том, что до сих пор никто не может доказать необходимость быстрого возрастания неполных частных, и, напротив, не известно ни одного примера трансцендентного числа, цепная дробь которого имела бы, например, ограниченную последовательность неполных частных.

Перейдем теперь к вопросу о величии множества E всех чисел Лиувилля. Ясно, что

$$E = Q' \cap \left(\bigcap_{n=1}^{\infty} G_n \right),$$

где Q' — дополнение до множества рациональных чисел, а

$$G_n = \bigcup_{q=2}^{\infty} \bigcup_{p=-\infty}^{\infty} \left(\frac{p}{q} - \frac{1}{q^n}; \frac{p}{q} + \frac{1}{q^n} \right)$$

— объединение интервалов.

Теорема 3. *E — нуль-множество второй категории, а E' — множество первой категории.*

Доказательство. Сначала категория. G_n — объединение интервалов, все числа вида $\frac{p}{q}$, $q \geqslant 2$, входят в G_n, следовательно, $Q \subset G_n$ и G_n — плотное и открытое. Значит, дополнение G'_n нигде не плотно и

$$E' = Q \cup \left(\bigcup_{n=1}^{\infty} G'_n \right)$$

— множество первой категории. Следовательно, E — всюду плотно (как дополнение множества первой категории) и само второй категории.

Теперь мера. Для любого натурального n

$$E \subseteq G_n.$$

Рассмотрим множества

$$G_{n,q} = \bigcup_{p=-\infty}^{\infty} \left(\frac{p}{q} - \frac{1}{q^n}; \frac{p}{q} + \frac{1}{q^n} \right),$$

где $q = 2, 3, \ldots$.

Фиксируем натуральные m и n. Имеем

$$E \cap (-m; m) \subset G_n \cap (-m; m) = \bigcup_{q=2}^{\infty} [G_{n,q} \cap (-m; m)] \subset$$

$$\subset \bigcup_{q=2}^{\infty} \bigcup_{p=-mq}^{mq} \left(\frac{p}{q} - \frac{1}{q^n}; \frac{p}{q} + \frac{1}{q^n} \right).$$

Это означает, что $E \cap (-m; m)$ можно покрыть интервалами, суммарная длина которых есть

$$\sum_{q=2}^{\infty} \sum_{p=-mq}^{mq} \frac{2}{q^n} = \sum_{q=2}^{\infty} (2mq + 1) \frac{2}{q^n} \leqslant \sum_{q=2}^{\infty} (4mq + q) \frac{1}{q^n} =$$

$$= (4m + 1) \sum_{q=2}^{\infty} \frac{1}{q^{n-1}} \leqslant \text{ вспоминаем интегральный признак! } \leqslant$$

$$\leqslant (4m + 1) \int_1^{\infty} \frac{dx}{x^{n-1}} = \text{берем интеграл самостоятельно! } =$$

$$= \frac{4m + 1}{n - 2} \underset{n \to \infty}{\longrightarrow} 0.$$

Таким образом, $E \cap (-m; m)$ — нуль-множество, значит, и

$$E = \bigcup_{m=1}^{\infty} [E \cap (-m; m)]$$

— нуль-множество. ♦

Теорема 3, дорогие читатели, как раз и дает обещанный в предыдущем пункте конкретный пример разбиения числовой прямой на два множества $\mathbf{R} = E \cup E'$, первое из которых — меры нуль, но второй категории, а второе — первой категории. Считаю краткую экскурсию в мир чисел Лиувилля законченой.

Задачки

1. Выпишите все многочлены с целыми коэффициентами веса 4. Сколько их?

2. Докажите иррациональность числа $\sqrt{3}$.

3. Докажите самостоятельно, что число $\sqrt{2}+\sqrt{3}$ — алгебраическое степени 4.

4. Докажите, что корни уравнения $x^3+2\sqrt{2}\,x^2+2=0$ являются алгебраическими числами. Найдите их степень.

5. Докажите, что все корни многочлена $f(x)=x^5-3x^2+12x-6$ — алгебраические числа пятой степени. [1]

6. Для числа $z=\dfrac{1+\sqrt{5}}{2}$ найдите натуральное M такое, что

$$\left|z-\frac{p}{q}\right|>\frac{1}{Mq^n}$$

при всех целых p и q, $q>0$.

7. Докажите, что число $z=\sum\limits_{k=1}^{\infty}\dfrac{1}{k\cdot 10^{(k+1)!}}$ является числом Лиувилля.

8. Докажите, что число

$$z=1+\cfrac{1}{(10)!+\cfrac{1}{(10^2)!+\cfrac{1}{(10^3)!+\cfrac{1}{\ddots}}}}$$

является числом Лиувилля.

9. Докажите, что множество E всех чисел Лиувилля имеет нулевую s-мерную меру Хаусдорфа при любом $s>0$. [2]

26. Число $e \approx 2{,}718281828459045\ldots$

Матушка-природа подарила нам несколько замечательных констант, весьма неожиданно появляющихся при попытках математического выражения и записи законов разных наук. С одной

[1] Рекомендую воспользоваться критерием Эйзенштейна неприводимости многочлена над полем рациональных чисел.

[2] Определение меры Хаусдорфа смотри в задаче 9 предыдущего пункта. Очевидно, что утверждение настоящей задачи 9 является усилением утверждения теоремы 3 этого пункта о том, что E является нуль-множеством.

из таких констант — «основанием натуральных логарифмов» — мы познакомимся поближе в этом пункте.

Когда-то давно я учился в средней школе № 110 г. Свердловска. В школе нам страшно повезло — судьба послала нам великого учителя, сухощавого математика на железной ноге Николая Ивановича Слободчикова, по прозвищу «Колываныч». Самым загадочным образом хулиганы и двоечники становились у него отличниками, а математика — любимым предметом. Еще в восьмом классе Колываныч говорил нам: «Дети! Запомните, что основание натуральных логарифмов обозначается буквой e в честь Леонарда Ейлера, а запомнить его десятичные знаки очень просто. Два и семь — помнят все. Дальше — 1828 — год рождения Льва Николаевича Толстого. Дальше — снова 1828 — год рождения Жюль Верна, а если вы тупые, то — опять год рождения Толстого. Потом идут углы равнобедренного прямоугольного треугольника — 45, 90, 45. А что идет потом — я сам не знаю...». Потом Николай Иванович доказал нам, что $2 < e < 3$ и загробным голосом сказал: «Число e — трансцендентно!». Этим словом мы потом обзывались на переменках. Когда я поступил в университет, я узнал, что

$$e = \lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n;$$

$$e = \sum_{n=0}^{\infty} \frac{1}{n!};$$

e — основание показательной функции, являющейся решением задачи Коши: $y' = y, y(0) = 1$;

и многое многое другое. Вразумительный ответ на вопрос, почему именно число e наиболее естественно взять за основание логарифмов, которые с таким основанием сразу становятся натуральными и пригодными к употреблению, я нашел в книжке Ф. Клейна «Элементарная математика с точки зрения высшей», том 1, «Арифметика, алгебра, анализ». Настоятельно советую ее прочитать, так как считаю, что с подобными книжками должен быть знаком каждый мало-мальски грамотный математик, ибо такие книжки составляют золотой фонд литературы о любимой нами науке.

Ряд $\sum_{n=0}^{\infty} \frac{1}{n!}$ сходится быстро (чего нельзя сказать про известные ряды, например, для числа π). Это значит, что частич-

ные суммы ряда $\sum\limits_{n=0}^{\infty} \frac{1}{n!}$, будучи рациональными числами, очень хорошо приближают число e, поэтому естественно ожидать, что трансцендентность e удастся доказать относительно легко (а исследование природы числа π потребует гораздо больших усилий). Эти эвристические соображения действительно находят свое подтверждение на практике, но не будем торопить события и начнем по порядку.

Теорема 1. *Число e иррационально.*

Доказательство. Рассмотрим числа

$$A_n = n! \sum_{k=0}^{n} \frac{1}{k!}$$

и

$$a_n = n! \sum_{k=n+1}^{\infty} \frac{1}{k!}.$$

Очевидно, что $A_n \in \mathbf{N}$, $a_n > 0$. Оценим a_n сверху:

$$a_n = \frac{n!}{(n+1)!} + \frac{n!}{(n+2)!} + \frac{n!}{(n+3)!} + \ldots = \frac{1}{(n+1)} \times$$

$$\times \left(1 + \frac{1}{(n+2)} + \frac{1}{(n+2)(n+3)} + \frac{1}{(n+2)(n+3)(n+4)} + \ldots\right) <$$

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

Итак, $0 < a_n < 1$, т. е. a_n — всегда дробное число. Это означает, что при любом натуральном n, число $n!\, e = A_n + a_n$ не является целым.

Пусть теперь $e = \frac{p}{q}$ — рациональное число, p, $q \in \mathbf{N}$. Тогда $q!\, e = q!\, \frac{p}{q} = (q-1)!\, p$ — целое число, что вопиюще противоречит факту, установленному тремя строчками выше. ♦

Для доказательства трансцендентности героя этого пункта потребуются две леммы.

Лемма 1. *Если $g(x)$ — многочлен с целыми коэффициентами, то для любого $k \in \mathbf{N}$ все коэффициенты его k-й производной $g^{(k)}(x)$ делятся на $k!$.*

Доказательство. Так как оператор $\dfrac{d}{dx}$ линейный, то утверждение леммы достаточно проверить только для многочленов вида $g(x) = x^s$, $s \geqslant 0$.

Если $k > s$, то $g^{(k)}(x) \equiv 0$ и $k! \,|\, 0$.

Если $k \leqslant s$, то

$$g^{(k)}(x) = s(s-1)(s-2)\cdot\ldots\cdot(s-k+1)x^{s-k} = \\ = \frac{s!}{(s-k)!}x^{s-k} = \frac{s!\,k!}{(s-k)!\,k!}x^{s-k} = k!\begin{pmatrix} s \\ k \end{pmatrix}x^{s-k},$$

биномиальный коэффициент $\begin{pmatrix} s \\ k \end{pmatrix}$ является целым числом и $g^{(k)}(x)$ опять-таки делится на $k!$ нацело. ♦

Ключевая идея доказательства трансцендентности числа e принадлежит Шарлю Эрмиту. Впрочем, идея Эрмита сработала и при доказательстве трансцендентности числа π, а также некоторых других чисел специального вида, но это уже заслуга других математиков. А трансцендентность непосредственно числа e доказал Эрмит в 1873 г. и это был исторически первый решительный прорыв в познание природы замечательных констант.

Лемма 2 (тождество Эрмита). *Пусть $f(x)$ — произвольный многочлен степени k с действительными коэффициентами,*

$$F(x) = f(x) + f'(x) + f''(x) + \ldots + f^{(k)}(x)$$

— сумма всех его производных. Тогда для любого действительного (*и даже комплексного, но нам это пока не понадобится*) *x выполнено*

$$e^x \int_0^x f(t)e^{-t}dt = F(0)e^x - F(x). \qquad (\spadesuit)$$

Доказательство. Интегрируем по частям:

$$\int_0^x f(t)e^{-t}dt = \left| \begin{array}{cc} U = f(t) & dU = f'(t)dt \\ dV = e^{-t}dt & V = -e^{-t} \end{array} \right| =$$

$$= -f(t)e^{-t}\Big|_0^x + \int_0^x f'(t)e^{-t}dt = f(0) - f(x)e^{-x} + \int_0^x f'(t)e^{-t}dt.$$

Интеграл $\int\limits_0^x f'(t)e^{-t}dt$ снова подвергнем процедуре интегрирования по частям, потом этой прцедуре подвергнем интеграл $\int\limits_0^x f''(t)e^{-t}dt$ и так далее. Терпеливо повторив эту процедуру всего $k+1$ раз, получим

$$\int\limits_0^x f(t)e^{-t}dt = F(0) - F(x)e^{-x}. \qquad \blacklozenge$$

Теорема 2 (Эрмит, 1873). *Число e трансцендентно.*

Доказательство. От противного. Пусть e — алгебраическое, степени m. Тогда

$$a_m e^m + \ldots + a_1 e + a_0 = 0$$

для некоторого натурального m и некоторых целых $a_m, \ldots, a_1, a_0$, причем, очевидно, $a_m \neq 0$ и $a_0 \neq 0$. Подставим в тождество Эрмита ($\spadesuit$) вместо x целое число k, попросим k принимать по очереди значения $0, 1, \ldots, m$; умножим каждое равенство

$$e^k \int\limits_0^k f(t)e^{-t}dt = F(0)e^k - F(k)$$

соответственно на a_k, а затем все их сложим, получим

$$F(0)\sum_{k=0}^{m} a_k e^k - \sum_{k=0}^{m} a_k F(k) = \sum_{k=0}^{m}\left(a_k e^k \int\limits_0^k f(t)e^{-t}dt\right).$$

Так как $\sum\limits_{k=0}^{m} a_k e^k = 0$ (это наше противное предположение), то выходит, что для любого многочлена $f(x)$ должно быть выполнено равенство

$$-\sum_{k=0}^{m} a_k F(k) = \sum_{k=0}^{m}\left(a_k e^k \int\limits_0^k f(t)e^{-t}dt\right). \qquad (\spadesuit\spadesuit)$$

Противоречие, которое углядел Эрмит в этом равенстве, сразу и не заметишь: за счет подходящего выбора многочлена $f(x)$

можно сделать левую часть (♠♠) ненулевым целым числом, а правая часть при этом окажется между нулем и единицей.

Возьмем многочлен $f(x) = \dfrac{1}{(n-1)!}x^{n-1}(x-1)^n(x-2)^n \times \times \ldots \times (x-m)^n$, где n определим позже ($n \in \mathbf{N}$, и n будет очень большое).

Число 0 — корень кратности $n-1$ многочлена $f(x)$, числа $1, 2, \ldots, m$ — корни кратности n, следовательно:

$$f^{(l)}(0) = 0, \quad l = 1, 2, \ldots, n-2,$$

$$f^{(n-1)}(0) = (-1)^{mn}(m!)^n,$$

$$f^{(l)}(k) = 0, l = 0, 1, \ldots, n-1; \quad k = 1, 2, \ldots, m.$$

Рассмотрим $\varphi(x) = x^{n-1}(x-1)^n(x-2)^n \cdot \ldots \cdot (x-m)^n$ — многочлен, ужасно похожий на $f(x)$, но с целыми коэффициентами. По лемме 1, коэффициенты $\varphi^{(l)}(x)$ — целые числа, делящиеся на $l!$, следовательно, при $l \geqslant n$ у производной $f^{(l)}(x)$ все коэффициенты — целые числа, делящиеся на n, так как $f^{(l)}(x)$ получается из $\varphi^{(l)}(x)$ делением только на $(n-1)!$. Именно поэтому

$$F(0) = \sum_{l=n-1}^{(m+1)n-1} f^{(l)}(0) = (-1)^{mn}(m!)^n + nA,$$

где A — подходящее целое число, а над знаком суммы стоит число $(m+1)n-1$ — степень многочлена $f(x)$ и, хоть суммировать можно и до бесконечности, ненулевых производных у $f(x)$ именно столько.

Аналогично,

$$F(k) = \sum_{l=n-1}^{(m+1)n-1} f^{(l)}(k) = nB_k,$$

где B_k — подходящие целые числа, $k = 1, 2, \ldots, m$.

Пусть теперь $n \in \mathbf{N}$ — любое целое число, удовлетворяющее условиям

$$\begin{cases} (n; m!) = 1, \\ |a_0| < n. \end{cases}$$

Снова рассмотрим равенство (♠♠):

$$-\sum_{k=0}^{m} a_k F(k) = \sum_{k=0}^{m} \left(a_k e^k \int_0^k f(t)e^{-t}dt \right).$$

В сумме слева все слагаемые — суть целые числа, причем $a_kF(k)$ при $k = 1, 2, \ldots, m$ **делится на** n, а $a_0F(0)$ **на** n **не делится**. Это означает, что вся сумма, будучи целым числом, **на** n **не делится**, т. е. не является нулем. Следовательно,

$$\left|\sum_{k=0}^{m} a_kF(k)\right| \geqslant 1.$$

Оценим теперь правую часть равенства (♠♠). Ясно, что $|x-k| \leqslant m$ на отрезке $[0; m]$. Поэтому на этом отрезке

$$|f(x)| \leqslant \frac{m^{(m+1)n-1}}{(n-1)!}.$$

Тогда

$$\left|\sum_{k=0}^{m} a_k e^k \int_0^k f(t)e^{-t}dt\right| = \left|\sum_{k=0}^{m} a_k \int_0^k f(t)e^{k-t}dt\right| \leqslant$$

$$\leqslant \frac{m^{(m+1)n-1}}{(n-1)!} \sum_{k=0}^{m} |a_k| \int_0^k e^{k-t}dt <$$

берем и оцениваем интеграл самостоятельно

$$< \frac{m^{(m+1)n-1}}{(n-1)!} e^m \sum_{k=0}^{m} |a_k| = C_0 \frac{C_1^n}{(n-1)!},$$

где константы C_0 и C_1 не зависят от n . Известно, что

$$\frac{C^n}{(n-1)!} \underset{n\to\infty}{\longrightarrow} 0,$$

поэтому при достаточно больших n правая часть (♠♠) меньше единицы и равенство (♠♠) невозможно. ♦

После прочтения такого серьезного доказательства я советую вам отдохнуть. Впереди предстоят еще более серьезные испытания.

Задачки

1. Докажите самостоятельно, что число e не является квадратичной иррациональностью (т. е не является алгебраическим числом степени 2). Подсказка: используйте тот факт, что $e^{-1} = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!}$, и попытайтесь показать, что

равенство $ae^2 + be + c = 0$ (т. е. $ae + b + ce^{-1} = 0$) невозможно при любых целых a, b, c.

2. Докажите иррациональность числа $\sum\limits_{n=1}^{\infty} \frac{1}{(n!)^2}$.

3. Выпишите тождество Эрмита для многочлена
$$f(x) = x^3 + 2x^2 - 7x + 1.$$

4. Докажите трансцендентность числа e^2.

27. Число $\pi \approx 3{,}141592653589793\ldots$

В этом пункте я расскажу вам правдивую историю про отношение длины окружности к ее диаметру, которое Эйлер обозначил греческой буквой π, а еще Архимед, почти тысячу триста лет назад, вычислил, дойдя в приближении длины окружности правильными многоугольниками аж до 96 сторон, что

$$3\frac{10}{71} < 3\frac{284\frac{1}{4}}{2018\frac{7}{40}} < 3\frac{284\frac{1}{4}}{2017\frac{1}{4}} < \pi < 3\frac{667\frac{1}{2}}{4673\frac{1}{2}} < 3\frac{667\frac{1}{2}}{4672\frac{1}{2}} = 3\frac{1}{7},$$

т. е. $3{,}1409 < \pi < 3{,}1429$. Среднее арифметическое верхней и нижней границ, найденных Архимедом, дает $\pi = 3{,}14159\ldots$ Очень неплохо для древнего грека!

Истинную природу числа π долгое время не удавалось распознать. Эйлер, занимаясь знаменитой древнегреческой задачей о квадратуре круга (или, что эквивалентно, задачей построения циркулем и линейкой отрезка длины π), впервые высказал предположение, что число π не удовлетворяет никакому алгебраическому уравнению с целыми коэффициентами, но доказать этого он не смог. Лишь в 1882 г. после работ Лиувилля и Эрмита немецкий математик Фердинанд Линдеман (1852–1939) весьма изощренными методами доказал трансцендентность π, показав, тем самым, неразрешимость задачи о квадратуре круга. Но давайте не будем забегать вперед и пойдем, как и в предыдущем пункте, по порядку.

Теорема 1. *Число π иррационально.*

Доказательство. Сначала докажем аналог тождества Эрмита из леммы 2 предыдущего пункта.

Пусть $f(x)$ — произвольный многочлен с действительными коэффициентами,

$$F(x) = f(x) - f''(x) + f^{(4)}(x) - f^{(6)}(x) + \ldots$$

— многочлен из производных $f(x)$ четного порядка (очевидно, ряд для $F(x)$ содержит лишь конечное число ненулевых членов). Очевидно:

$$\frac{d}{dx}\left(F'(x)\sin x - F(x)\cos x\right) = \left(F''(x) + F(x)\right)\sin x = f(x)\sin x.$$

Проинтегрируем последнее тождество:

$$\int_0^\pi f(x)\sin x\,dx = F(0) + F(\pi). \qquad (\spadesuit)$$

Это и есть тождество Эрмита с функцией $\sin x$, справедливое для любого многочлена $f(x)$.

Предположим, что $\pi = \dfrac{a}{b}$; $a, b \in \mathbf{N}$; $(a, b) = 1$. Положим в тождестве Эрмита ($\spadesuit$)

$$f(x) = \frac{b^n}{n!}x^n(\pi - x)^n = \frac{1}{n!}x^n(a - bx)^n,$$

где $n \in \mathbf{N}$ — достаточно большое число, которое определим несколько позже. Утверждается, что при таком выборе многочлена $f(x)$ мы, как и в теореме 2 предыдущего пункта, снова придем к противоречию. Именно: покажем, что интеграл в ($\spadesuit$) будет по модулю меньше единицы, а сумма $F(0) + F(\pi)$ окажется прекрасным целым числом.

Возьмемся сначала за интеграл. Очевидно, что $f(x)\sin x > 0$ на интервале $(0,\ \pi)$, поэтому $\displaystyle\int_0^\pi f(x)\sin x\,dx > 0$. Далее, на этом же интервале, $x^n(\pi - x)^n \leqslant \pi^{2n}$, следовательно,

$$\int_0^\pi f(x)\sin x dx \leqslant \frac{b^n\pi^{2n}}{n!}\int_0^\pi \sin x dx =$$

$$\left(\text{выше договаривались будто-бы } \pi = \frac{a}{b}\right)$$

$$= 2\frac{\left(a^2/b\right)^n}{n!} = 2\frac{C^n}{n!} \underset{n\to\infty}{\longrightarrow} 0.$$

Ясно, что можно взять $n \in \mathbf{N}$ настолько большим, что наш интеграл станет меньше единицы.

Обратим теперь свой взор на правую часть тождества (♠). Многочлен $f(x)$ имеет число 0 корнем кратности n, следовательно,

$$f(0) = f'(0) = f''(0) = \ldots = f^{(n-1)}(0) = 0.$$

Рассмотрим похожий на $f(x)$ многочлен $\varphi(x) = b^n x^n (\pi - x)^n$ с целыми коэффициентами. По лемме 1 из предыдущего пункта, все коэффициенты l-й производной $\varphi^{(l)}(x)$ делятся на $l!$, следовательно, все производные многочлена $f(x)$ порядка $l \geqslant n$ имеют целые коэффициенты. Это значит, что $f^{(n)}(0), f^{(n+1)}(0), \ldots, f^{(2n)}(0)$ — целые числа. Итак, $f^{(l)}(0)$ — целое число для любого $l = 0, 1, 2, \ldots$. Очевидно, что $f(x) = f(\pi - x)$. Поэтому $f^{(l)}(x) = (-1)^l f^{(l)}(\pi - x)$, т. е. $f^{(l)}(\pi) = (-1)^l f^{(l)}(0)$ — тоже целое число для любого $l = 0, 1, 2, \ldots$.

Итак, $F(0) + F(\pi)$ является целым числом, поэтому равенство

$$\int_0^\pi f(x) \sin x \, dx = F(0) + F(\pi)$$

невозможно, что и завершает доказательство теоремы. ♦

Смотрите, мы затратили на доказательство только иррациональности числа π почти столько же усилий, сколько на доказательство трансцендентности числа e. Это обстоятельство не должно вызывать удивления, особенно если вспомнить мои досужие рассуждения из предыдущего пункта о скорости приближения чисел π и e рациональными частичными суммами.

Теорема 2 (Линдеман, 1882). *Число π трансцендентно.*

Доказательство. Приводимое здесь доказательство потребует некоторых сведений из теории функций комплексного переменного, одного дополнительного определения и весьма серьезных усилий для понимания. Но волка бояться — в лес не ходить.

Мы знаем, что $e^{\pi i} = -1$ и помним тождество Эрмита

$$e^x \int_0^x f(t) e^{-t} dt = F(0) e^x - F(x),$$

выполненное для любого многочлена $f(x)$, при этом,

$$F(x) = f(x) + f'(x) + f''(x) + \ldots + f^{(k)}(x).$$

Определение. Пусть α — алгебраическое число. Тогда существует единственный неприводимый многочлен $f(x)$ с рациональными коэффициентами и старшим коэффициентом, равным единице, такой, что $f(\alpha) = 0$. Такой многочлен называется *минимальным многочленом числа* α, степень $f(x)$ называется *степенью числа* α (обозначение: $\deg \alpha$), все корни минимального многочлена числа α называются *числами*, *сопряженными* с α .

Пример. i — мнимое алгебраическое число, $\deg i = 2$, $f(x) = x^2 + 1$ — минимальный многочлен, $\{-i; i\}$ — числа, сопряженные с числом i.

Нетрудно доказать, что произведение двух алгебраических чисел снова будет алгебраическим числом. Действительно, пусть α_1, β_1 — алгебраические числа, $\deg \alpha_1 = n, \deg \beta_1 = m; \alpha_1, \alpha_2, \ldots, \alpha_n; \beta_1, \beta_2, \ldots, \beta_m$ — сопряженные числа к α_1 и β_1 соответственно. Рассмотрим многочлен

$$\prod_{i,j} (x - \alpha_i \beta_j).$$

Его коэффициенты суть основные симметрические многочлены от корней $\alpha_i \beta_j$ (теорема Виета). Значит, они являются симметрическими многочленами от $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_m$ (но уже не обязательно основными). Каждый симметрический многочлен от $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_m$ является комбинацией основных симметрических многочленов от $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_m$ (основная теорема о симметрических многочленах). Каждый основной симметрический многочлен от $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_m$ является комбинацией симметрических многочленов отдельно от $\alpha_1, \alpha_2, \ldots, \alpha_n$ и многочленов от $\beta_1, \beta_2, \ldots, \beta_m$. Последние, в свою очередь, построены из основных симметрических многочленов от $\alpha_1, \alpha_2, \ldots, \alpha_n$ и от $\beta_1, \beta_2, \ldots, \beta_m$, которые являются рациональными числами — коэффициентами минимальных многочленов чисел α_1 и β_1 соответственно. Это значит, что коэффициенты многочлена $\prod\limits_{i,j} (x - \alpha_i \beta_j)$, корнем которого является $\alpha_1 \beta_1$, суть рациональные числа, и $\alpha_1 \beta_1$ — алгебраическое число степени не выше mn.

Доказательство теоремы Линдемана в математическом мире принято вести от противного. Пусть π — алгебраическое число.

Тогда число $\gamma = \pi \cdot i$ — тоже алгебраическое как произведение двух алгебраических чисел. Пусть $\deg \gamma = \nu; \gamma = \gamma_1, \gamma_2, \ldots, \gamma_\nu$ — сопряженные числа. Имеем $e^\gamma + 1 = 0$, следовательно:

$$\prod_{i=1}^{\nu} (1 + e^{\gamma_i}) = 0.$$

В этом произведении раскрою скобки:

$$\prod_{i=1}^{\nu} (1 + e^{\gamma_i}) = \sum_{\varepsilon_1=0}^{1} \sum_{\varepsilon_2=0}^{1} \ldots \sum_{\varepsilon_\nu=0}^{1} e^{\varepsilon_1\gamma_1 + \varepsilon_2\gamma_2 + \ldots + \varepsilon_\nu\gamma_\nu} = 0.$$

Показатели над буквой e справа бывают отличными от нуля (например, при $\varepsilon_1 = 1, \varepsilon_2 = \varepsilon_3 = \ldots = \varepsilon_\nu = 0$) и равными нулю (например, при $\varepsilon_1 = \varepsilon_2 = \varepsilon_3 = \ldots = \varepsilon_\nu = 0$). Пусть среди этих показателей ровно m штук отлично от нуля, а остальные $a = 2^\nu - m$ равны нулю, $a \geqslant 1$. Обозначим отличные от нуля показатели через $\alpha_1, \alpha_2, \ldots, \alpha_m$ и получим равенство

$$a + e^{\alpha_1} + e^{\alpha_2} + \ldots + e^{\alpha_m} = 0.$$

Покажем, что $\alpha_1, \alpha_2, \ldots, \alpha_m$ — в точности все корни некоторого многочлена $\psi(x)$ с целыми коэффициентами (разумеется, степень $\psi(x)$ равна m). Рассмотрим вспомогательный многочлен

$$\varphi(x) = \prod_{\varepsilon_1=0}^{1} \ldots \prod_{\varepsilon_\nu=0}^{1} (x - (\varepsilon_1\gamma_1 + \ldots + \varepsilon_\nu\gamma_\nu)).$$

Посмотрим на многочлен $\varphi(x)$ как на симметрический многочлен от $\gamma_1, \gamma_2, \ldots, \gamma_\nu$. Он, конечно, представим в виде комбинации основных симметрических многочленов от $\gamma_1, \gamma_2, \ldots, \gamma_\nu$, правда, коэффициенты в таком представлении будут зависеть от x и $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_\nu$. Но основные симметрические многочлены от $\gamma_1, \gamma_2, \ldots, \gamma_\nu$ есть коэффициенты минимального многочлена числа γ, т. е. являются рациональными числами. Следовательно, $\varphi(x)$, как многочлен от x, имеет рациональные коэффициенты, а многочлен $r\varphi(x)$, где r — общий знаменатель коэффициентов $\varphi(x)$, имеет целые коэффициенты. Корни $\varphi(x)$ суть числа $\alpha_1, \alpha_2, \ldots, \alpha_m$ и число 0, которое является корнем кратности a. Поэтому многочлен $\psi(x) = \frac{r}{x^a}\varphi(x)$ имеет целые коэффициенты, а его корни есть в точности числа $\alpha_1, \alpha_2, \ldots, \alpha_m$.

Запомним этот многочлен, ибо именно его (правда чуть-чуть искалеченного) мы будем подставлять в тождество Эрмита для получения противоречия.

Положим в тождестве Эрмита

$$e^x \int_0^x f(t)e^{-t}dt = F(0)e^x - F(x)$$

последовательно $x = \alpha_1, \alpha_2, \ldots, \alpha_m$ и сложим все получившиеся равенства:

$$\sum_{k=1}^{m} F(0)e^{\alpha_k} - \sum_{k=1}^{m} F(\alpha_k) = \sum_{k=1}^{m} e^{\alpha_k} \int_0^{\alpha_k} f(t)e^{-t}dt,$$

т. е. (помним, что $a + e^{\alpha_1} + e^{\alpha_2} + \ldots + e^{\alpha_m} = 0$)

$$-aF(0) - \sum_{k=1}^{m} F(\alpha_k) = \sum_{k=1}^{m} e^{\alpha_k} \int_0^{\alpha_k} f(t)e^{-t}dt. \qquad (\spadesuit\spadesuit)$$

Далее все будет катиться как в доказательстве трансцендентности числа e. Тождество ($\spadesuit\spadesuit$) справедливо для любого многочлена $f(x)$. Положим

$$f(x) = \frac{1}{(n-1)!} b_m^{nm-1} x^{n-1} \psi^n(x),$$

где $\psi(x) = \dfrac{r}{x^a}\varphi(x) = b_m x^m + \ldots + b_1 x + b_0$, $b_m > 0$, $b_0 \neq 0$, — тот самый многочлен с целыми коэффициентами и корнями $\alpha_1, \alpha_2, \ldots, \alpha_m$, который мы построили выше, а $b_m = r$ — его старший коэффициент. Видно, что

$$f(x) = \frac{1}{(n-1)!} b_m^{(m+1)n-1} x^{n-1} (x-\alpha_1)^n (x-\alpha_2)^n \cdot \ldots \cdot (x-\alpha_m)^n,$$

а число $n \in \mathbf{N}$ мы определим позже и оно будет достаточно большим.

Сначала рассмотрим левую часть тождества ($\spadesuit\spadesuit$). Рассуждая как при доказательстве трансцендентности числа e, получим

$$f^{(l)}(0) = 0, \quad l = 0, 1, \ldots, n-2;$$

$$f^{(n-1)}(0) = b_m^{mn-1} b_0^m;$$

$$F(0) = \sum_{l=n-1}^{(m+1)n-1} f^{(l)}(0) = b_m^{mn-1} b_0^m + nA,$$

где A — некоторое подходящее целое число. Далее, так как α_k — корень $f(x)$ кратности n, то

$$f^{(l)}(\alpha_k)=0, \quad l=0,1,\dots,n-1, \quad k=1,\dots,m.$$

По лемме 1 из предыдущего пункта, все коэффициенты l-й производной многочлена $x^{n-1}\psi^n(x)$ делятся на $l!$. Поэтому при $l\geqslant n$ многочлен $f^{(l)}(x)$ имеет целые коэффициенты, делящиеся на nb_m^{mn-1}. Значит:

$$F(\alpha_k)=\sum_{l=n}^{(m+1)n-1} f^{(l)}(\alpha_k)=nb_m^{mn-1}\Phi(\alpha_k),$$

где $\Phi(z)$ — некоторый многочлен с целыми коэффициентами.

Сумма $\sum\limits_{k=1}^{m} F(\alpha_k)$ является симметрическим многочленом от $\alpha_1,\alpha_2,\dots,\alpha_m$, следовательно, она представляется в виде комбинации основных симметрических многочленов от $\alpha_1,\alpha_2,\dots,\alpha_m$. Поскольку основные симметрические многочлены от $\alpha_1,\alpha_2,\dots,\alpha_m$ суть целые числа (коэффициенты $\psi(x)$), то сумма $\sum\limits_{k=1}^{m} F(\alpha_k)$ является целым числом и это число делится на n. Значит, левая часть тождества (♠♠) есть

$$aF(0)+\sum_{k=1}^{m} F(\alpha_k)=ab_0^m b_m^{mn-1}+nB,$$

где B — подходящее целое число.

Если теперь взять $n\in\mathbf{N}$ таким, что

$$\begin{cases} (n,b_m)=1,\\ n>a\,|b_0|^m, \end{cases}$$

(или, на худой конец, просто $n>ab_0^m b_m^{mn-1}$), то левая часть (♠♠) окажется целым числом, не делящимся на n, т. е. **отличным от нуля целым числом**. Значит,

$$\left|aF(0)+\sum_{k=1}^{m} F(\alpha_k)\right|\geqslant 1.$$

Оценим теперь правую часть равенства (♠♠). Пусть все точки $\alpha_1,\alpha_2,\dots,\alpha_m$ содержатся в круге $|x|\leqslant R$. Обозначим

$$\max_{|x|\leqslant R}|b_m^m\psi(x)|=C.$$

Ясно, что C не зависит от n. Тогда

$$\max_{|x|\leqslant R}|f(x)| \leqslant \frac{R^{n-1}C^n}{(n-1)!} \underset{n\to\infty}{\longrightarrow} 0.$$

Значит, правая часть (♠♠)

$$\left|\sum_{k=1}^{m} e^{\alpha_k}\int_0^{\alpha_k} f(x)e^{-x}dx\right| \leqslant \sum_{k=1}^{m}\left|\int_0^{\alpha_k}|f(x)|\left|e^{(\alpha_k-x)}\right|dx\right| \leqslant$$

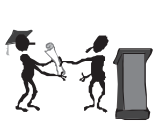
$$\leqslant \frac{R^{n-1}C^n}{(n-1)!}e^R\sum_{k=1}^{m}\left|\int_0^{\alpha_k}dx\right| \leqslant \left(\text{интеграл}\left|\int_0^{\alpha_k}dx\right| \leqslant R\right) \leqslant$$

$$\leqslant me^R\frac{(RC)^n}{(n-1)!} \underset{n\to\infty}{\longrightarrow} 0.$$

Таким образом, при больших $n \in \mathbf{N}$ правая часть (♠♠) меньше 1 и равенство (♠♠) невозможно. ♦

Поздравляю Вас, дорогие товарищи, с прочтением предпоследнего пункта этой книжки.

Задачки



1. Докажите, что число π^2 иррационально.
2. Докажите, что число π^2 не является квадратичной иррациональностью.
3. Докажите, что число π^2 трансцендентно.

28. Трансцендентность значений функции e^z

Последний пункт нашей книжки имеет номер 28 — второе совершенное число — и посвящен обсуждению одного замечательного свойства показательной функции.

Теорема (Линдеман). *Если ξ — алгебраическое число и $\xi \neq 0$, то число e^ξ — трансцендентно.*

Поразительно, правда? Точки координатной плоскости с рациональными координатами всюду плотно заполняют эту плоскость, точки с обеими алгебраическими координатами (алгебраические точки) — тем более. Однако сплошная и ровная кривая — график функции $y = e^x$, не дергаясь из стороны в сторону, прохо-

дит спокойно и величаво между всеми алгебраическими точками, случайно раздавив только одну — $(0,1)$.

Из теоремы Линдемана также вытекает, например, что число $\ln 2$ — трансцендентно, ведь $2 = e^{\ln 2}$, а число 2 — алгебраическое. Оказывается, мы еще в средней школе видели массу трансцендентных чисел — $\ln 2, \ln 3, \ln \sqrt[5]{27}$ и т. п. — и совершенно не подозревали об этом.

Доказательство теоремы Линдемана можно провести с помощью тождества Эрмита, аналогично тому, как была доказана трансцендентность π, с некоторыми усложнениями в преобразованиях. Именно так ее и доказывал сам Линдеман. Однако я пойду другим путем, ибо хочу познакомить читателей с основными идеями советского математика А. О. Гельфонда, приведшими в середине XX в. к решению Седьмой проблемы Гильберта — проблеме о природе чисел вида α^β, где α, β — алгебраические и β — иррационально. Чтобы не дразнить ваше любопытство, скажу сразу, что числа вида α^β, где α, β — алгебраические и β — иррационально (например, $2^{\sqrt{2}}$), являются трансцендентными, но мы этого доказывать не будем, так как от этого наша маленькая книжка по теории чисел может сразу превратиться в большую.

Доказательство трансцендентности значений показательной функции, предложенное Гельфондом, основывается на применении интерполяционных методов. В этом доказательстве с помощью разложения функции $e^{\xi \cdot z}$ в интерполяционный ряд Ньютона строится последовательность многочленов $P_n(x,y)$ с целыми коэффициентами такая, что $\left|P_n(\xi, e^\xi)\right|$ достаточно быстро убывает с ростом n. Однако несложно получить оценку снизу значения произвольного многочлена с целыми коэффициентами от двух произвольных алгебраических чисел, поэтому предположение об алгебраичности чисел ξ и e^ξ породит противоречие между верхней и нижней оценками. Далее будут представлены три основных этапа доказательства Гельфонда: построение ряда Ньютона функции $e^{\xi \cdot z}$, построение многочленов $P_n(x,y)$ и их оценка сверху, оценка $\left|P_n(\xi, e^\xi)\right|$ снизу и сопоставление полученных оценок. Приступим.

Этап 1. Интерполяционный ряд Ньютона функции $e^{\xi \cdot z}$.

Пусть функция $f(z)$ аналитическая в области D, точки $z_1, z_2, \ldots, z_n \in D$ — фиксированы и, быть может, среди них есть совпадающие. Положим

$$F_0(t) = 1,$$
$$F_k(t) = (t - z_1)(t - z_2) \cdot \ldots \cdot (t - z_k); \quad k = 1, 2, \ldots, n.$$

Пусть $z \in D$. При каждом $k = 1, 2, \dots, n$ выполнено

$$\frac{1}{t-z}\left(1 - \frac{z-z_k}{t-z_k}\right) = \frac{1}{t-z_k}.$$

Умножим это тождество на $\dfrac{F_{k-1}(z)}{F_{k-1}(t)}$. Получим

$$\frac{1}{t-z}\left(\frac{F_{k-1}(z)}{F_{k-1}(t)} - \frac{F_k(z)}{F_k(t)}\right) = \frac{F_{k-1}(z)}{F_k(t)}.$$

Сложим эти тождества:

$$\frac{1}{t-z} - \frac{F_n(z)}{F_n(t)(t-z)} = \sum_{k=1}^{n} \frac{F_{k-1}(z)}{F_k(t)},$$

или

$$\frac{1}{t-z} = \frac{F_n(z)}{F_n(t)(t-z)} + \sum_{k=1}^{n} \frac{F_{k-1}(z)}{F_k(t)}. \qquad (\spadesuit)$$

Пусть C — простой замкнутый контур в D, точки $z_1, z_2, \dots, z_n \in D$ лежат внутри этого контура. Умножим тождество ($\spadesuit$) на $\dfrac{1}{2\pi i} f(t)$ и проинтегрируем, пользуясь формулой Коши:

$$f(z) = \frac{1}{2\pi i}\int\limits_C \frac{f(t)}{t-z}\,dt =$$

$$= \sum_{k=1}^{n} F_{k-1}(z) \cdot \frac{1}{2\pi i} \cdot \int\limits_C \frac{f(t)}{F_k(t)}\,dt + \frac{1}{2\pi i}\int\limits_C \frac{F_n(z)f(t)}{F_n(t)(t-z)}\,dt.$$

Обозначим

$$A_{k-1} = \frac{1}{2\pi i}\int\limits_C \frac{f(t)}{F_k(t)}\,dt, \quad k = 1, \dots, n;$$

$$R_n(z) = \frac{1}{2\pi i}\int\limits_C \frac{F_n(z)f(t)}{F_n(t)(t-z)}\,dt.$$

В этих обозначениях

$$f(z) = \sum_{k=0}^{n-1} A_k F_k(z) + R_n(z), \quad z \in D,$$

— **интерполяционная формула Ньютона** для функции $f(z)$ с узлами интерполяции $z_1, z_2, \ldots, z_n$. Если же $z_1, z_2, \ldots, z_n, \ldots$ — бесконечная последовательность узлов, а $R_n(z) \underset{n\to\infty}{\longrightarrow} 0$ для всех $z \in D$, то

$$f(z) = \sum_{k=0}^{\infty} A_k F_k(z) = \sum_{n=0}^{\infty} A_n (z - z_1)(z - z_2) \cdot \ldots \cdot (z - z_n)$$

— **интерполяционный ряд Ньютона** для функции $f(z)$ с узлами интерполяции $z_1, z_2, \ldots, z_n, \ldots$. Нетрудно заметить, что при $z_1 = z_2 = \ldots = z_n = \ldots$ из ряда Ньютона получается ряд Тейлора.

Пусть $m \in \mathbf{N}$. Хитрый Гельфонд взял за узлы интерполяции бесконечную периодическую последовательность периода m:

$$1, 2, 3, \ldots, m-1, m, 1, 2, \ldots, m-1, m, 1, 2, \ldots$$

т. е.

$$z_n = n \quad \text{для} \quad n = 1, 2, \ldots, m;$$

$$z_{n+lm} = z_n.$$

Разложим функцию $f(z) = e^{\xi \cdot z}$, где $\xi \in \mathbf{C}$, $\xi \neq 0$, в ряд Ньютона с такими узлами интерполяции. Запишем формулу Ньютона:

$$e^{\xi \cdot z} = \sum_{k=0}^{n-1} A_k (z-1)(z-2) \cdot \ldots \cdot (z - z_k) + R_n(z),$$

где

$$R_n(z) = \frac{1}{2\pi i} \int\limits_C \frac{(z - z_1) \cdot \ldots \cdot (z - z_n) e^{\xi \cdot z}}{(t - z_1) \cdot \ldots \cdot (t - z_n)(t - z)}\, dt$$

— остаточный член. Пусть R — любое число, такое, что $R > m$. Оценим остаточный член при $n > 2R$ в круге $|z| \leqslant R$. Пусть C — окружность $|t| = n$. Имеем

$$1 \leqslant z_k \leqslant m,$$

следовательно,

$$|z - z_k| \leqslant |z| + |z_k| \leqslant R + m,$$

$$\left| \prod_{k=1}^{n} (z - z_k) \right| \leqslant (R + m)^n \tag{1}$$

для всех z из круга $|z| \leqslant R$. Далее, так как $n > 2R > 2m$, то на окружности $|t| = n$ имеем

$$|t - z_k| \geqslant |t| - |z_k| \geqslant n - m > \frac{n}{2},$$
$$|t - z| \geqslant |t| - |z| \geqslant n - R > \frac{n}{2},$$

значит,

$$\left|(t - z)\prod_{k=1}^{n}(t - z_k)\right| > \left(\frac{n}{2}\right)^{n+1}. \tag{2}$$

Пользуясь неравенствами (1), (2) и неравенством $\left|e^{\xi \cdot t}\right| \leqslant e^{|\xi| \cdot n}$, оценим интеграл:

$$|R_n(z)| \leqslant \frac{1}{2\pi} 2\pi n \frac{e^{|\xi| n}(R + m)^n}{\left(\frac{n}{2}\right)^{n+1}} = \frac{2^{n+1} e^{|\xi| n}(R + m)^n}{n^n} \underset{n \to \infty}{\longrightarrow} 0.$$

Число R может быть выбрано сколь угодно большим, поэтому при любом комплексном z функция $f(z) = e^{\xi \cdot z}$ представляется в виде суммы ряда Ньютона с целочисленной периодической последовательностью узлов интерполяции $z_1, z_2, \ldots, z_n, \ldots$.

Итак,

$$e^{\xi \cdot z} = \sum_{n=0}^{\infty} A_n (z - z_1)(z - z_2) \cdot \ldots \cdot (z - z_n),$$

где

$$A_n = \frac{1}{2\pi i} \int\limits_C \frac{e^{\xi \cdot t}}{(t - z_1) \cdot \ldots \cdot (t - z_{n+1})}\, dt, \quad n = 0, 1, 2, \ldots.$$

Выбирая за контур C окружность $|t| = n$, где $n > 2m$, аналогично оценке остаточного члена в формуле Ньютона получаем оценку сверху для коэффициентов ряда:

$$|A_n| \leqslant \frac{1}{2\pi} 2\pi n \frac{e^{|\xi| n}}{\left(\frac{n}{2}\right)^{n+1}} = \frac{e^{|\xi| n + (n+1)\ln 2}}{n^n} < \frac{e^{\gamma n}}{n^n} \underset{n \to \infty}{\longrightarrow} 0,$$

где число $\gamma > 0$ и зависит только от ξ. Этап 1 завершен.

Этап 2. Построение многочленов $P_n(x, y)$ и их оценка сверху.

Поскольку последовательность узлов интерполяции периодическая, то в произведении

$$F_{n+1}(t) = (t-1)(t-2)\cdot\ldots\cdot(t-z_{n+1})$$

есть повторяющиеся сомножители. Обозначим число сомножителей вида $(t-k)$ через n_k+1. Тогда это произведение можно переписать так (подразумевается, что $n > m$):

$$F_{n+1}(t) = (t-1)(t-2)\cdot\ldots\cdot(t-z_{n+1}) = \prod_{k=1}^{m}(t-k)^{n_k+1}.$$

Ясно, что $n_1+n_2+\ldots+n_m+m = n+1$ и n_k зависят от n. Кроме того, так уж устроена последовательность узлов интерполяции, что $n_1 - 1 \leqslant n_m \leqslant n_{m-1} \leqslant \ldots \leqslant n_1 \leqslant \dfrac{n}{m}$. Значит, коэффициенты ряда Ньютона можно записать так:

$$A_n = \frac{1}{2\pi i}\int\limits_C \frac{e^{\xi\cdot t}}{F_{n+1}(t)}\,dt = \\ = \frac{1}{2\pi i}\int\limits_C \frac{e^{\xi\cdot t}}{(t-1)^{n_1+1}(t-2)^{n_2+1}\cdot\ldots\cdot(t-m)^{n_m+1}}\,dt.$$

Окружим каждый узел интерполяции k $(1 \leqslant k \leqslant m)$ окружностью Γ_k с центром в точке k и радиусом, например, $\dfrac{1}{3}$. Эти окружности не пересекаются и лежат внутри контура C. Если зафиксировать на них положительное направление обхода, то, по теореме Коши,

$$A_n = \sum_{k=1}^{m}\frac{1}{2\pi i}\int\limits_{\Gamma_k} \frac{e^{\xi\cdot t}}{(t-1)^{n_1+1}(t-2)^{n_2+1}\cdot\ldots\cdot(t-m)^{n_m+1}}\,dt.$$

Обозначим $\eta = e^{\xi}$. Разложим для каждого k $(1 \leqslant k \leqslant m)$ функцию $e^{\xi\cdot t}$ в ряд Тейлора по степеням $(t-k)$:

$$e^{\xi\cdot t} = \eta^k e^{\xi(t-k)} = \eta^k\sum_{l=0}^{\infty}\frac{\xi^l}{l!}(t-k)^l.$$

Тогда

$$e^{\xi\cdot t}=\eta^k\sum_{l=0}^{n_k}\frac{\xi^l}{l!}(t-k)^l+H_k(t),$$

где $H_k(t)$ — остаточный член, являющийся целой функцией, имеющей в точке $t=k$ нуль порядка n_k+1. Это значит, что

$$\int\limits_{\Gamma_k}\frac{H_k(t)}{(t-1)^{n_1+1}(t-2)^{n_2+1}\cdot\ldots\cdot(t-m)^{n_m+1}}\,dt=0.$$

Тогда

$$\frac{1}{2\pi i}\int\limits_{\Gamma_k}\frac{e^{\xi\cdot t}}{(t-1)^{n_1+1}(t-2)^{n_2+1}\cdot\ldots\cdot(t-m)^{n_m+1}}\,dt=$$
$$=\sum_{l=0}^{n_k}\frac{\eta^k\xi^l}{l!}\frac{1}{2\pi i}\int\limits_{\Gamma_k}\frac{(t-k)^l}{(t-1)^{n_1+1}(t-2)^{n_2+1}\cdot\ldots\cdot(t-m)^{n_m+1}}\,dt,$$

т. е. суммировать можно только до n_k. Обозначим при каждом k $(1\leqslant k\leqslant m)$

$$a_{k,l}=\frac{1}{2\pi i}\int\limits_{\Gamma_k}\frac{(t-k)^l}{(t-1)^{n_1+1}(t-2)^{n_2+1}\cdot\ldots\cdot(t-m)^{n_m+1}}\,dt,\qquad(\clubsuit)$$
$$l=0,1,\ldots,n_k.$$

В этих новых обозначениях коэффициент ряда Ньютона выглядит так:

$$A_n=\sum_{k=1}^{m}\sum_{l=0}^{n_k}\frac{a_{k,l}\xi^l\eta^k}{l!}.$$

Пусть M — наименьшее общее кратное чисел $1,2,\ldots,m$. Сейчас я докажу, что все числа $a_{k,l}$ в коэффициенте A_n рациональные, а числа $M^n a_{k,l}$ будут целыми. Число $a_{k,l}$ равно вычету в точке $t=k$ подынтегральной функции из интеграла $(\clubsuit)$, т. е. равно коэффициенту при $(t-k)^{-1}$ в разложении этой функции в ряд Лорана по степеням $(t-k)$. Найдем это разложение.

Пусть $s\in\mathbf{N}$, $1\leqslant s\leqslant m$, $s\neq k$. Имеем

$$\frac{1}{t-s}=\frac{1}{(t-k)-(s-k)}=-\frac{1}{s-k}\cdot\frac{1}{1-\dfrac{t-k}{s-k}}.$$

Если положить $t-k=Mu$ и разложить функцию $\dfrac{1}{t-s}$ в ряд по степеням u, то получится

$$\frac{1}{t-s}=-\frac{1}{s-k}\sum_{\nu=0}^{\infty}\left(\frac{M}{s-k}\right)^{\nu}u^{\nu}=$$

$$=-\frac{1}{M}\sum_{\nu=0}^{\infty}\left(\frac{M}{s-k}\right)^{\nu+1}u^{\nu}=\frac{1}{M}\sum_{\nu=0}^{\infty}b_{\nu}u^{\nu},$$

где $b_{\nu}=-\left(\dfrac{M}{s-k}\right)^{\nu+1}$. Этот ряд абсолютно сходится в круге $|u|<\dfrac{|s-k|}{M}$. Очевидно, что числа $b_{\nu}=-\left(\dfrac{M}{s-k}\right)^{\nu+1}$ целые, так как M — наименьшее общее кратное чисел $1,2,\ldots,m$, а число $|s-k|$ — целое и $1\leqslant|s-k|\leqslant m-1$.

Теперь, для того чтобы получилось нечто похожее на подынтегральное выражение из строчки (♣), надо перемножать ряды $\dfrac{1}{t-s}=\dfrac{1}{M}\sum\limits_{\nu=0}^{\infty}b_{\nu}u^{\nu}$ в подходящих степенях и при разных s. Произведение

$$\prod_{\substack{s\neq k\\ s=1}}^{m}\frac{1}{(t-s)^{n_s+1}}$$

есть кусок подынтегрального выражения в (♣), оно отличается от самого подынтегрального выражения отсутствием множителя $\dfrac{(t-k)^{l}}{(t-k)^{n_k+1}}=(t-k)^{l-n_k-1}$. Стало быть, это произведение содержит $(n_1+1)+\ldots+(n_{k-1}+1)+(n_{k+1}+1)+\ldots+(n_m+1)=n-n_k$ сомножителей вида $\dfrac{1}{t-s}$. Посчитаем, наконец, это произведение:

$$\prod_{\substack{s\neq k\\ s=1}}^{m}\frac{1}{(t-s)^{n_s+1}}=\frac{1}{M^{n-n_k}}\sum_{\nu=0}^{\infty}c_{\nu}u^{\nu}=\frac{1}{M^{n-n_k}}\sum_{\nu=0}^{\infty}\frac{c_{\nu}}{M^{\nu}}(t-k)^{\nu},$$

где все c_{ν}, очевидно, целые числа, так как они есть суммы произведений целых b_{ν} (так уж ряды перемножаются, тут ничего не попишешь). Тогда подынтегральная функция в (♣) равна

$$\frac{(t-k)^l}{(t-k)^{n_k+1}}\prod_{\substack{s\neq k\\ s=1}}^{m}\frac{1}{(t-s)^{n_s+1}}=$$

$$=\frac{1}{M^{n-n_k}}\sum_{\nu=0}^{\infty}\frac{c_\nu}{M^\nu}(t-k)^\nu\cdot(t-k)^{l-n_k-1}=$$

$$=\frac{1}{M^{n-n_k}}\sum_{\nu=0}^{\infty}\frac{c_\nu}{M^\nu}(t-k)^{\nu+l-n_k-1}.$$

Это и есть искомое разложение в ряд Лорана. Нетрудно сообразить, что показатель $\nu+l-n_k-1$ равен -1 при $\nu=n_k-l$. Значит, искомый вычет есть

$$a_{k,l}=\frac{c_{n_k-l}}{M^{n-l}}$$

и является рациональным числом. Тогда, бесспорно, число $M^n a_{k,l}$ — целое.

Далее все просто. Обратим снова свой взор на коэффициенты ряда Ньютона:

$$A_n=\sum_{k=1}^{m}\sum_{l=0}^{n_k}\frac{a_{k,l}\xi^l\eta^k}{l!},\quad \eta=e^\xi.$$

Если обозначить через $r=\max\limits_{1\leqslant k\leqslant m} n_k=n_1$, то, очевидно, выражение

$$P_n(\xi,\eta)=r!\,M^nA_n=\sum_{k=1}^{m}\sum_{l=0}^{n_k}\frac{r!\,M^n a_{k,l}\xi^l\eta^k}{l!}$$

будет многочленом с целыми коэффициентами от двух переменных ξ и η, его степень по переменной ξ не превосходит r, а степень по переменной η не превосходит m. Это и есть те самые многочлены с целыми коэффициентами, которые мы запланировали построить на втором этапе нашего доказательства.

Оценим высоту H_n (максимум среди абсолютных величин коэффициентов) многочлена P_n. Помним, что

$$a_{k,l}=\frac{1}{2\pi i}\int\limits_{\Gamma_k}\frac{(t-k)^l}{(t-1)^{n_1+1}(t-2)^{n_2+1}\cdot\ldots\cdot(t-m)^{n_m+1}}\,dt,$$

$$l=0,1,\ldots,n_k,$$
$$k=1,2,\ldots,m.$$

Поскольку $t \in \Gamma_k$ и радиус Γ_k мы взяли $\frac{1}{3}$, то $|t-k| < \frac{1}{2}$, а при $s \neq k$, $|t-s| > \frac{1}{2}$. Значит,

$$|a_{k,l}| \leqslant \frac{1}{2\pi} \cdot \underbrace{\left(\frac{2}{3}\pi\right)}_{\text{длина } \Gamma_k} \cdot \frac{1}{\left(\frac{1}{2}\right)^{n-l+1}} < 2^n$$

и высота H_n многочлена P_n удовлетворяет неравенству

$$H_n < r!(2M)^n.$$

Оценим, наконец, $|P_n(\xi,\eta)|$ сверху. В конце первого этапа мы получили оценку

$$|A_n| < \frac{e^{\gamma n}}{n^n} = e^{\gamma n - n\ln n}.$$

Поскольку $P_n(\xi,\eta) = r!M^n A_n$, а $r \leqslant \frac{n}{m}$, то

$$|P_n(\xi,\eta)| < e^{\gamma n - n\ln n + n\ln M + r\ln r} < e^{-\frac{m-1}{m}n\ln n + Cn},$$

где C >0 — константа, не зависящая от n .

Этап 3. Оценка $|P_n(\xi,\eta)|$ снизу.

Пусть $\alpha_1, \alpha_2, \ldots, \alpha_m$ — алгебраические числа, $\mathbf{Q}$ — поле рациональных чисел, $K = \mathbf{Q}[\alpha_1, \alpha_2, \ldots, \alpha_m]$ — алгебраическое расширение поля $\mathbf{Q}$, h — степень этого алгебраического расширения.

Напомню, что степенью алгебраического расширения называется степень примитивного минимального многочлена, корнями которого это расширение порождается. Это означает, что у каждого порождающего элемента поля $K = \mathbf{Q}[\alpha_1, \alpha_2, \ldots, \alpha_m]$ (примитивного элемента из K) имеется h штук сопряженных. В алгебраическом поле $K = \mathbf{Q}[\alpha_1, \alpha_2, \ldots, \alpha_m]$ степени h максимальное число линейно независимых над $\mathbf{Q}$ элементов равно h.

Сейчас мы докажем основной факт третьего этапа: для любого многочлена с целыми коэффициентами $P(z_1, z_2, \ldots, z_m)$ степени k и высоты H существует постоянная $c = c(\alpha_1, \alpha_2, \ldots, \alpha_m) > 0$ такая, что

$$\text{либо } |P(\alpha_1, \alpha_2, \ldots, \alpha_m)| \geqslant \frac{c^k}{H^{h-1}},$$

$$\text{либо } P(\alpha_1, \alpha_2, \ldots, \alpha_m) = 0.$$

Таким образом, алгебраические числа $\alpha_1, \alpha_2, \ldots, \alpha_m$ произвольный многочлен с целыми коэффициентами либо обращают в ноль (в этом случае говорят, что числа $\alpha_1, \alpha_2, \ldots, \alpha_m$ являются алгебраически зависимыми), либо значение этого многочлена находится достаточно далеко от нуля.

Пусть $\alpha_i = \alpha_i^{(1)}, \alpha_i^{(2)}, \ldots, \alpha_i^{(h)}$ — все сопряженные с α_i в поле $K = \mathbf{Q}[\alpha_1, \alpha_2, \ldots, \alpha_m]$, $1 \leqslant i \leqslant m$. Введем два обозначения. Через $|\overline{\alpha_i}|$ обозначим размер алгебраического числа α_i, $|\overline{\alpha_i}| = \max\limits_{1 \leqslant k \leqslant h} |\alpha_i^{(k)}|$ — максимальный из модулей чисел, сопряженных с α_i. Через $\|\alpha_i\|_K$ обозначим норму алгебраического числа α_i в поле K, $\|\alpha_i\|_K = \alpha_i^{(1)} \alpha_i^{(2)} \ldots \alpha_i^{(h)}$ — произведение всех сопряженных с α_i. Проверьте сами, что $\|\alpha_i\|_K$ действительно удовлетворяет всем аксиомам нормы.

Еще одно замечание. *Целым алгебраическим числом* называется алгебраическое число, минимальный многочлен которого (у него старший коэффициент всегда единица) имеет целые коэффициенты. Так, например, $\sqrt{3}$ и $\dfrac{1+\sqrt{5}}{2}$ — целые алгебраические числа, а $\dfrac{\sqrt{3}}{2}$ — не целое, так как их минимальные многочлены суть, соответственно, $x^2 - 3, x^2 - x - 1$ и $x^2 - \dfrac{3}{4}$. Если α — не целое алгебраическое число, то всегда можно подобрать некоторое натуральное число r такое, что $r\alpha$ будет корнем многочлена с целыми коэффициентами и старшим коэффициентом 1, т. е. будет целым алгебраическим числом. Множество целых алгебраических чисел поля K обозначим через $\mathbf{Z}_K$. Несложно проверить, что $\mathbf{Z}_K$ — кольцо и всегда $\mathbf{Z} \subset \mathbf{Z}_K$.

Приступим к доказательству основного факта третьего этапа. Предположим, что $P(\alpha_1, \alpha_2, \ldots, \alpha_m) \neq 0$. Подберем натуральное число r так, что $r\alpha_i \in \mathbf{Z}_K$, $i = 1, \ldots, m$. Так как многочлен p есть многочлен степени k с целыми коэффициентами, то

$$\beta = r^k P(\alpha_1, \ldots, \alpha_m) \in \mathbf{Z}_K, \quad \beta \neq 0.$$

Возможны два случая.

Случай 1. $h = 1$ (т. е. $K = \mathbf{Q}$). Тогда

$$|\beta| = r^k \, |P(\alpha_1, \ldots, \alpha_m)| \geqslant 1, \quad |P(\alpha_1, \ldots, \alpha_m)| \geqslant \frac{1}{r^k}.$$

Случай 2. $h > 1$. Обозначим

$$A_j = P(\alpha_1^{(j)}, \alpha_2^{(j)}, \ldots, \alpha_m^{(j)}), \quad j = 1, \ldots, h.$$

Числа $A_1, \dots, A_h$ будут сопряженными в поле K. По свойствам нормы

$$|\|\beta\|_K| = \left|\left\|r^k A_1\right\|_K\right| = r^{kh}\,|A_1 A_2 \cdot \ldots \cdot A_h| \geqslant 1.$$

Отсюда вытекает, что

$$|A_1| \geqslant \frac{1}{r^{kh}\prod\limits_{j=2}^{h}|A_j|}.$$

Если

$$P(z_1, \dots, z_m) = \sum_{0 \leqslant k_1 + \ldots + k_m \leqslant k} c_{k_1,\ldots,k_m} z_1^{k_1} z_2^{k_2} \cdot \ldots \cdot z_m^{k_m}, \quad c_{k_1,\ldots,k_m} \in \mathbf{Z},$$

то

$$|A_j| \leqslant H\left(1 + \sum_{i=1}^{m} |\overline{\alpha_i}|\right)^k = c_0^k H, \quad c_0 = 1 + \sum_{i=1}^{m} |\overline{\alpha_i}|.$$

Тогда из двух последних неравенств следует

$$|P(\alpha_1, \dots, \alpha_m)| \geqslant \frac{1}{\left(r^h c_0^{h-1}\right)^k H^{h-1}} = \frac{c^k}{H^{h-1}}, \quad c = \frac{1}{r^h c_0^{h-1}},$$

а, собственно, это и требовалось доказать.

Наступил тот славный момент, когда у нас все готово для того, чтобы достойно завершить доказательство теоремы Линдемана. Давайте проделаем это. От противного. Пусть $\xi \neq 0$ и $\eta = e^{\xi}$ — алгебраические числа, h — степень алгебраического расширения $K = \mathbf{Q}[\xi, \eta]$, $h > 1$. Разложим $e^{\xi \cdot z}$ в ряд Ньютона с периодической целочисленной последовательностью узлов интерполяции

$$1, 2, \dots, m-1, m, 1, 2, \dots, m-1, m, 1, 2, \dots,$$

где $m = h + 1$. Построим многочлены $P_n(\xi, \eta)$. Мы только что доказали, что либо $P_n(\xi, \eta) = 0$, либо

$$|P_n(\xi, \eta)| \geqslant \frac{c^k}{H^{h-1}} = e^{k \ln c - (h-1)\ln H},$$

где (вспоминаем устройство многочленов $P_n(\xi, \eta) = r!\, M^n A_n$ и оценку их высоты из второго этапа):

$$k \leqslant r + m, \quad H \leqslant r \ln r + n \ln(2M), \quad r \leqslant \frac{n}{m}.$$

Отсюда моментально получается, что

$$|P_n(\xi, \eta)| > e^{-\frac{m-2}{m} n \ln n - Dn},$$

где $D > 0$ — некоторая подходящая константа. Последнее неравенство и неравенство

$$|P_n(\xi, \eta)| < e^{-\frac{m-1}{m} n \ln n + Cn},$$

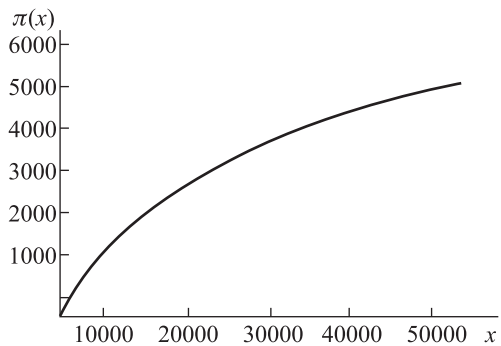
полученное в конце второго этапа, при достаточно больших n противоречивы, значит, при всех достаточно больших n остается только возможность $P_n(\xi, \eta) = 0 = r!\, M^n A_n$. Это означает, что, начиная с некоторого номера, все $A_n = 0$, т. е. ряд Ньютона функции $e^{\xi \cdot z}$содержит лишь конечное число членов и функция $e^{\xi \cdot z}$ является многочленом. Но этого не может быть потому, что не может быть никогда. (Например, потому, что функция $e^{\xi \cdot z}$ периодическая, а любой нетривиальный многочлен — нет). Этим и заканчивается доказательство теоремы Линдемана. ♦

Закончился последний пункт нашей небольшой книжки по теории чисел, но я не буду говорить здесь никаких прощальных слов, ибо, как всегда во всех сказках, самое интересное только еще начинается. Идите вперед! Изучайте теорию чисел и она оправдает ваши надежды. Числа не подвержены инфляции, политическим и экономическим потрясениям, коррупции и обману. Математика не может приносить разочарований, она приносит только восхищение окружающим миром и человеческим разумом. Я желаю вам — будьте счастливы!

Пункт-дополнение ко второму изданию. [1] Немного о распределении простых чисел.

В разные периоды человеческой истории многие выдающиеся математические умы напрягались в поиске ответа на простой вопрос: как часто встречаются простые числа в натуральном ряду? Конкретнее: сколько существует простых чисел, меньших заданного натурального числа x? Вопрос, казалось бы, простой и понятный, но точного ответа на него до сих пор не знает никто. Развитие математической мысли показало, что задача точного вычисления функции $\pi(x)$ — количества простых чисел, не превосходящих x, является чрезвычайно трудной. Но разгадка тайн природы является благородным и увлекательным занятием, поэтому изучение с разных сторон функции $\pi(x)$ (или, как говорят, «закона распределения простых чисел») продолжается во всем математическом мире. Поговорим немного и мы на эту тему.

Ясно, что $\pi(0) = 0$ и $\pi(x)$ скачком увеличивается на 1 в точках $x = 2; 3; 5; 7; \ldots$, т. е. когда x равно простому числу. Если вы немного поработаете и построите график функции $\pi(x)$ хотя бы для x меньших 100, то станет видно, что несмотря на малые колебания, функция $\pi(x)$ растет довольно регулярно. Если же нарисовать график $\pi(x)$ на промежутке, скажем, от 0 до 50000 (при таком масштабе мелкие скачки на единицу функции $\pi(x)$ просто незаметны), то от отчетливости проявившейся регулярности просто захватит дух:



[1] Этот пункт появился в ответ на замечание сотрудника нашей кафедры Игоря Олеговича Корякова: «Что же, Вы, Сережа, не написали в своей книжке ничего о законе распределения простых чисел?»

По мнению многих математиков, плавность, с которой поднимается эта кривая, следует отнести к числу удивительнейших фактов математики. А где закономерность, там и попытки ее разгадать, предпринимавшиеся на протяжении столетий.

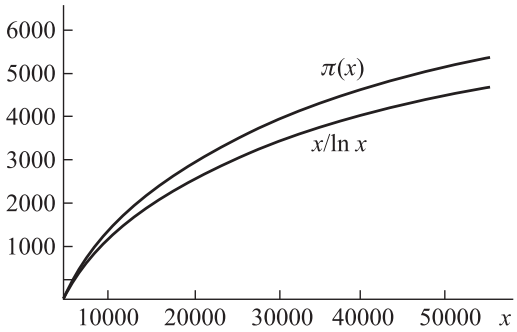
Поскольку точную формулу для $\pi(x)$ получить никак не удавалось, исследователи были вынуждены придумывать различные эмпирические приближения, асимптотические формулы. Смотрите:

x	$\pi(x)$	$x/\pi(x)$
10	4	2,5
100	25	4,0
1000	168	6,0
10 000	1 229	8,1
100 000	9 592	10,4
1 000 000	78 498	12,7
10 000 000	664 579	15,0
100 000 000	5 761 455	17,4
1 000 000 000	50 847 534	19,7
10 000 000 000	455 052 512	22,0

Вы не представляете себе, какое количество труда потребовалось для составления этой скромной с виду таблицы значений функции $\pi(x)$. Разглядывая таблицу, подобную этой (и составленную им самостоятельно), пятнадцатилетний Гаусс заметил, что при переходе от данной степени десятки к следующей, отношение $x/\pi(x)$ все время увеличивается примерно на 2,3. Каким-то непостижимым образом наблюдательный Гаусс узнал в константе 2,3 логарифм 10 по основанию e, после чего ему ничего не оставалось делать, как выдвинуть предположение, что

$$\pi(x) \approx \frac{x}{\ln x},$$

причем знак $\approx$ означает, что отношение соединенных им выражений стремится к 1 с ростом x. Это асимптотическое равенство впервые было доказано уже после смерти Гаусса лишь в 1896 г. Вот графики $\pi(x)$ и $\dfrac{x}{\ln x}$:



Другой великий математик, француз Лежандр, в 1808 г. также разглядывал таблицу значений отношения $x/\pi(x)$ и обнаружил, что оно почти точно равно $\ln x - 1$. Проведя много часов за нудными вычислениями, Лежандр (фантастика!) открыл, что особенно хорошее приближение получается, если из логарифма вычесть не единицу, а число 1,08366 [1]), т. е.

$$\pi(x) \approx \frac{x}{\ln x - 1{,}08366}.$$

Графики $\pi(x)$ и приближения Лежандра я рисовать не буду, так как в пределах точности рисунка они просто совпадают.

Еще одно хорошее приближение функции $\pi(x)$ на основе анализа экспериментальных фактов обнаружил все тот же Гаусс:

$$\pi(x) \approx \mathrm{Li}(x) = \int\limits_2^x \frac{dt}{\ln t}.$$

Функция $\mathrm{Li}(x) = \int\limits_2^x \frac{dt}{\ln t}$ носит название «интегральный логарифм»; известно, что сам интеграл $\int\limits_2^x \frac{dt}{\ln t}$ не выражается через элементарные функции, а представление неопределенного интеграла в виде ряда таково:

$$\int \frac{dx}{\ln x} = \ln\ln x + \ln x + \frac{\ln^2 x}{2 \cdot 2!} + \frac{\ln^3 x}{3 \cdot 3!} + \frac{\ln^4 x}{4 \cdot 4!} + \dots .$$

[1]) Это число, на мой взгляд, — какая-то мистика. Это же додуматься надо! Ну, не ангел же, в самом деле, спустился с небес на землю, чтобы сообщить Лежандру эту константу!

Приближение Лежандра при небольших x (примерно до 1 миллиона) значительно точнее приближения Гаусса $\mathrm{Li}(x)$, однако уже начиная с 5 миллионов точнее становится интегральный логарифм и математикам известно доказательство, что с дальнейшим ростом x это становится все вернее. Еще один интересный и поучительный факт о сложных взаимоотношениях интегрального логарифма и функции $\pi(x)$ состоит в следующем. Экспериментальной проверкой чисел до 1 миллиарда установлено, что для них $\mathrm{Li}(x)$ всегда больше $\pi(x)$. От этого у некоторых (даже весьма крупных) математиков сложилось впечатление, что интегральный логарифм принципиально переоценивает количество простых чисел, меньших x. Однако матушка-природа в лице своенравной и вздорной функции $\pi(x)$ и тут преподнесла нам очередной сюрприз. Оказывается, существуют промежутки, в которых $\pi(x)$ меняется настолько быстро, что становится больше $\mathrm{Li}(x)$. Такие значения x до сих пор не найдены, но англичанин Литтлвуд в тридцатых годах XX в. показал, что такие x существуют, а Скьюз (другой англичанин) установил даже, что одно из них не больше

$$10^{10^{10^{34}}}.$$

По поводу этого дичайшего числа, называемого теперь константой Скьюза, математик Харди (третий англичанин) заметил как-то, что это, пожалуй, самое большое число, служившее в математике какой-нибудь определенной цели. Вот, упертая троица англичан! Один доказал, другой оценил, третий заметил. Кембрижд ликует.

Я думаю, что после вышеизложенных фактов у вас уже сложилось вполне определенное мнение о непредсказуемости функции $\pi(x)$. Доказать закон распределения простых чисел долгое время не удавалось никому. Начало укрощения строптивой $\pi(x)$ положили, как и полагается, русские люди. В 1850 г. выдающийся математик Пафнутий Львович Чебышев доказал, что при достаточно больших x справедлива оценка

$$0,89\frac{x}{\ln x} < \pi(x) < 1,11\frac{x}{\ln x},$$

т. е. что закон распределения простых чисел справедлив с относительной погрешностью не более 11 %. Мы с вами проделаем упрощенный вариант этого красивого доказательства, но оценки, разумеется, получатся несколько хуже.

Теорема (Чебышев). *При* $n > 200$ *верно*

$$\frac{2}{3}\frac{n}{\ln n} < \pi(n) < 1{,}7\frac{n}{\ln n}.$$

Доказательство. Сначала докажем оценку сверху: $\pi(n) < 1{,}7\frac{n}{\ln n}$. Это неравенство непосредственно проверяется для $x < 1200$. Далее рассуждаем по индукции.

Пусть наше неравенство доказано для всех $x \leqslant n$. Рассмотрим внимательно «центральный» биномиальный коэффициент [1] $\binom{2n}{n}$. Поскольку

$$2^{2n} = (1+1)^{2n} = \binom{2n}{0} + \binom{2n}{1} + \ldots + \binom{2n}{n} + \ldots + \binom{2n}{2n},$$

то он, безусловно, меньше 2^{2n}. С другой стороны,

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \frac{1 \cdot 2 \cdot \ldots \cdot (2n-1) \cdot (2n)}{(1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n)^2}.$$

Ясно, что каждое простое число p, меньшее $2n$, но большее n, входит в числитель, но не входит в знаменатель. Это значит, что биномиальный коэффициент $\binom{2n}{n}$ делится на каждое простое число, лежащее между n и $2n$, т. е. делится на их произведение:

$$\left(\prod_{n<p\leqslant 2n} p\right) \Bigg| \binom{2n}{n}.$$

В произведении слева $\pi(2n) - \pi(n)$ сомножителей и каждый из них больше n, поэтому

$$n^{\pi(2n)-\pi(n)} < \prod_{n<p\leqslant 2n} p \leqslant \binom{2n}{n} < 2^{2n}.$$

---

[1] Напомню, что $\binom{n}{m} = \frac{n!}{m!\,(n-m)!}$. В старинных манускриптах и даже более поздних изданиях для биномиальных коэффициентов весьма употребимо также обозначение $\mathbf{C}_n^m$.

Умеющие логарифмировать сразу поймут, что отсюда следует

$$\pi(2n) - \pi(n) < \frac{2n \ln 2}{\ln n} < 1{,}39\frac{n}{\ln n}.$$

Согласно предположению индукции, неравенство выполнено для n, т. е.

$$\pi(n) < 1{,}7\frac{n}{\ln n}.$$

Сложим два последних неравенства. Как ни крути, получается, что

$$\pi(2n) < 3{,}09\frac{n}{\ln n} < 1{,}7\frac{2n}{\ln(2n)} \qquad (n > 1200),$$

т. е. утверждение верно и для $2n$. Так как

$$\pi(2n+1) \leqslant \pi(2n) + 1 < 3{,}09\frac{n}{\ln n} + 1 < 1{,}7\frac{2n+1}{\ln(2n+1)}$$

при $n > 1200$, то неравенство верно и для $2n+1$, чем благополучно и завершается шаг индукции.

Теперь докажем оценку снизу:

$$\pi(n) > \frac{2}{3}\frac{n}{\ln n}.$$

Пусть $\binom{n}{k} = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$ — разложение биномиального коэффициента на простые множители. Так как

$$\binom{n}{k} = \frac{1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n}{(1 \cdot 2 \cdot \ldots \cdot (k-1) \cdot k) \cdot (1 \cdot 2 \cdot \ldots \cdot (n-k))},$$

то $p_j^{\alpha_j} \leqslant n$ для всех $j = 1, 2, \ldots, r$ [1]).

---

[1]) Если это утверждение сразу не уясняется, то наверняка поможет очень простая лемма 1 из п. 12 этой книжки, утверждающая, что показатель, с которым простое число p входит в разложение на простые множители числа $n!$ равен $\alpha = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$, где квадратными скобками обозначена целая часть числа. Именно поэтому

$$\alpha_j = \sum_{s \geqslant 1} \left(\left[\frac{n}{p_j^s}\right] - \left[\frac{k}{p_j^s}\right] - \left[\frac{n-k}{p_j^s}\right] \right).$$

В этой сумме каждое слагаемое есть 0 или 1, причем заведомо 0, если $s > \ln n / \ln p_j$. Значит,

$$\alpha_j \leqslant \left[\frac{\ln n}{\ln p_j}\right] \leqslant \frac{\ln n}{\ln p_j},$$

т. е. $p_j^{\alpha_j} \leqslant n$.

Теперь легко понять, что для любого биномиального коэффициента справедлива оценка

$$\binom{n}{k} = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r} \leqslant n^{\pi(n)}.$$

Совершенно очевидно, что

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} \leqslant (n+1) \cdot n^{\pi(n)}.$$

После совершения акта натурального логарифмирования, получим

$$\pi(n) \geqslant \frac{n \ln 2}{\ln n} - \frac{\ln(n+1)}{\ln n} > \frac{2}{3}\frac{n}{\ln n} \qquad (n > 200),$$

что, собственно, и требовалось. ♦

Задачки

1. Постройте график функции $y = \pi(x)$ для $0 \leqslant x \leqslant 100$.

2. Поэкспериментируйте самостоятельно. Расположите натуральные числа на плоскости каким-нибудь регулярным образом, например, по спирали:

$$\begin{array}{ccccc} 16 & 15 & 14 & 13 & 12 \\ 17 & 4 & 3 & 2 & 11 \\ \downarrow & 5 & 0 & 1 & 10 \\ \downarrow & 6 & 7 & 8 & 9 \\ \rightarrow & \rightarrow & \rightarrow & \cdots & \end{array}$$

Обведите кружочком все простые. Не заметите ли вы какой-нибудь закономерности в расположении кружочков? А если заметите, то не сможете ли ее объяснить? [1)]

[1)] Это творческая и еще никем не решенная задача. Сложная это штука — поиск закономерностей, а тем более — их объяснение.

Значения различных констант, о которых шла речь в этой книжке, приводимые для удовлетворения чисто человеческого любопытства и проверки правильности решения некоторых встретившихся выше задач (сорок верных десятичных знаков)

$1 = 1{,}0000000000000000000000000000000000000000\ldots$

$\sqrt{2} = 1{,}41421\ 35623\ 73095\ 04880\ 16887\ 24209\ 69807\ 85697\ldots$

$\sqrt{3} = 1{,}73205\ 08075\ 68877\ 29352\ 74463\ 41505\ 87236\ 69428\ldots$

$\sqrt{5} = 2{,}23606\ 79774\ 99789\ 69640\ 91736\ 68731\ 27623\ 54406\ldots$

$\sqrt{10} = 3{,}16227\ 76601\ 68379\ 33199\ 88935\ 44432\ 71853\ 37196\ldots$

$\ln 2 = 0{,}69314\ 71805\ 59945\ 30941\ 72321\ 21458\ 17656\ 80755\ldots$

$\ln 3 = 1{,}09861\ 22886\ 68109\ 69139\ 52452\ 36922\ 52570\ 46475\ldots$

$\ln 10 = 2{,}30258\ 50929\ 94045\ 68401\ 79914\ 54684\ 36420\ 76011\ldots$

$\pi = 3{,}14159\ 26535\ 89793\ 23846\ 26433\ 83279\ 50288\ 41972\ldots$

$e = 2{,}71828182845904523536028747135266249775 72\ldots$

$\dfrac{1}{e} = 0{,}36787\ 94411\ 71442\ 32159\ 55237\ 70161\ 46086\ 74458\ldots$

$\dfrac{1}{\pi} = 0{,}31830\ 98861\ 83790\ 67153\ 77675\ 26745\ 02872\ 40689\ldots$

$\pi^2 = 9{,}86960\ 44010\ 89358\ 61883\ 44909\ 99876\ 15113\ 53137\ldots$

$e^2 = 7{,}38905\ 60989\ 30650\ 22723\ 04274\ 60575\ 00781\ 31803\ldots$

$\Phi = \dfrac{1+\sqrt{5}}{2} = 1{,}61803\ 39887\ 49894\ 84820\ 45868\ 34365\ 63811\ 77203\ldots$

$\sqrt{\pi} = 1{,}77245\ 38509\ 05516\ 02729\ 81674\ 83341\ 14518\ 27975\ldots$

$\sqrt[3]{2} = 1{,}25992\ 10498\ 94873\ 16476\ 72106\ 07278\ 22835\ 05703\ldots$

$\zeta(3) = 1{,}20205\ 69031\ 59594\ 28539\ 97381\ 61511\ 44999\ 07650\ldots$

$\gamma = 0{,}57721\ 56649\ 01532\ 86060\ 65120\ 90082\ 40243\ 10422\ldots$

$e^{\pi/4} = 2{,}19328\ 00507\ 38015\ 45655\ 97696\ 59278\ 73822\ 34616\ldots$

$$\sin 1 = 0{,}84147\,09848\,07896\,50665\,25023\,21630\,29899\,96226\ldots$$

$$\cos 1 = 0{,}54030\,23058\,68139\,71740\,09366\,07442\,97660\,37323\ldots$$

$$\frac{1}{\ln 10} = 0{,}43429\,44819\,03251\,82765\,11289\,18916\,60508\,22944\ldots$$

$$\frac{1}{\ln 2} = 1{,}44269\,50408\,88963\,40735\,99246\,81001\,89213\,74266\ldots$$

Список литературы, в которую поглядывал автор при написании этой книжки

1. *Виноградов И. М.* Основы теории чисел. — М.: Наука, 1981.
2. *Окстоби Дж.* Мера и категория. — М.: Мир, 1974.
3. *Шидловский А. Б.* Трансцендентные числа. — М.: Наука, 1987.
4. *Хинчин А. Я.* Цепные дроби. — М.: Гос. изд-во физ.-мат. лит., 1961.
5. *Карацуба А. А.* Основы аналитической теории чисел. — М.: Наука, 1975.
6. *Боро В.*, *Цагир Д.*, *Рольфс Ю.*, *Крафт Ч.*, *Янцен Е.* Живые числа. — М.: Мир, 1985.
7. *Кнут Д.* Искусство программирования для ЭВМ». Т. 2. Получисленные алгоритмы. — М.: Мир, 1977.
8. *Стройк Д. Я.* Краткий очерк истории математики. — М.: Наука, 1990.
9. *Клейн Ф.* Элементарная математика с точки зрения высшей. — М.: Наука, 1987.
10. *Фельдман Н. И.* Седьмая проблема Гильберта. — М.: Изд-во МГУ, 1982.
11. *Фаддеев Д. К.* Лекции по алгебре. — М.: Наука, 1984.
12. *Кострикин А. И.* Введение в алгебру. — М.: Наука, 1977.
13. *Пойа Д.* Математика и правдоподобные рассуждения. — М.: Наука, 1975.
14. *Вилейтнер Г.* История математики от Декарта до середины XIX столетия. — М., Наука, 1966.
15. *Серр Ж. П.* Курс арифметики. — М.: Мир, 1982.
16. *Маркушевич А. И.* Краткий курс теории аналитических функций. — М.: Наука, 1978.
17. *Шклярский Д. О.*, *Ченцов Н. Н.*, *Яглом И. М.* Избранные задачи и теоремы элементарной математики. — М.: Наука, 1976.

18. *Сизый С. В.*, *Савинов В. Б.*, *Сафронович Е. Л.*, *Спевак Л. Ф.*, *Дунаев М. В.* Книжка, прочитанная вслух. — Екатеринбург: УрГУ, 1995.

19. *Грэхем Р.* Начала теории Рамсея. — М.: Мир, 1984.

20. *Демидович Б.Ѝ.* Сборник задач и упражнений по математическому анализу. — М.: Наука, 1990.

21. *Проскуряков И. В.* Сборник задач по линейной алгебре. — М.: Наука, 1974.

22. *Литлвуд Дж.* Математическая смесь. — М.: Наука, 1978.