Степени простых чисел в составе пифагоровых троек

Е. А. Горин

Устанавливается, что вопрос о пифагоровых тройках, в состав которых входят две степени простых, непосредственно связан с известными нерешенными классическими проблемами теории чисел. Хотя некоторые свойства множества таких троек удается довольно легко выяснить, уже́ вопрос о бесконечности этого множества остается открытым.

Введение

1. Пифагорова тройка — это (упорядоченный) набор $\{x, y, z\}$ натуральных чисел, для которых

$$x^2 + y^2 = z^2. \tag{1}$$

Тройка $\{x, y, z\}$ называется *примитивной*, если $\gcd(x, y, z) = 1$. Здесь и далее через $\gcd(a, b, \ldots)$ обозначается наибольший общий делитель набора $\{a, b, \ldots\}$ целых (в частности, натуральных) чисел.

В дальнейшем, если противное явно не оговаривается, имеются в виду примитивные тройки. Из соотношения (1) тогда следует, что одно из чисел x, y является четным, а другое — нечетным. Для определенности и для удобства в дальнейшем, если противное не оговаривается явно, *четным считается* x. Заметим, что для примитивных троек z всегда является нечетным.

Пифагоровы тройки — один из древнейших объектов математики, так что было бы наивным надеяться сказать о них что–нибудь особенно оригинальное. Однако наша цель в другом: мы хотим показать, что входящий в заглавие (немного странный) вопрос тесно связан с целым рядом нетривиальных классических проблем теории чисел.

Пифагоровы тройки при сделанных предположениях допускают следующую исчерпывающую параметризацию:

$$\begin{cases} x = 2ab, \\ y = a^2 - b^2, \\ z = a^2 + b^2, \end{cases} \tag{2}$$

где a и b — натуральные числа различной четности, причем $a > b$ и $\gcd(a, b) = 1$. Формулы (2) иногда называют *формулами индусов* (см., например, [1, с.10]), и мы будем использовать эту терминологию.

Отметим, что сформулированная задача о пифагоровых тройках со степенями простых разбивается на несколько других, существенно различных по степени сложности.

Действительно, используя формулы (2), совсем легко убедиться, что *все три* компоненты являются степенями простых только в случае тройки $\{4, 3, 5\}$, известной (по меньшей мере) со времен строительства египетских пирамид. На самом деле, кроме этой тройки, нет других, в которых x и y — степени простых.

Довольно легко разбирается другой крайний случай, когда речь идет о наличии *хотя бы одной* степени простого в составе пифагоровой тройки. Множество таких троек само естественно разбивается на три класса, каждый из которых бесконечен, причем исследование одного из этих классов (z — степень простого) не так тривиально, как исследование двух других.

Более интересны два оставшихся случая, когда среди компонент присутствуют в точности две степени простых.

Случай, когда степенями простых являются x и z, напрямую связан с простыми Ферма. В этом смысле «самая большая» из известных троек такого типа соответствует соотношению

$$2^{18} + (2^{16} - 1)^2 = (2^{16} + 1)^2.$$

Наиболее интересен тот случай, когда степенями простых являются y и z. Отметим (это легко получается из (2)), что в этом (но и не только в этом, см. ниже) случае $2z = 1 + y^2$ и $x = z - 1$. Поэтому в приведенных далее списках достаточно указать только y или только z и, с другой стороны, легко дописать x. Довольно простые и не очень скучные вычисления позволяют предъявить многочисленные примеры такого типа. В частности, к пифагоровым тройкам приводят следующие пары *простых*:

y	3	5	11	19	29	59	61	71	79	101
z	5	13	61	181	421	1741	1861	2521	3121	5101

В следующих парах встречаются квадраты простых:

y	7	3^2	5^2	41	7^2	11^2
z	5^2	41	313	29^2	1201	7321

Во втором списке квадраты не встречаются парами, и это не случайно (так не бывает). Оказывается, показатели степеней простых сами непременно имеют вид 2^k (как в случае чисел Ферма), причем степень выше

2–й в качестве z встречается лишь однажды, а именно в тройке, где

$$y = 239 \text{ и } z = 13^4.$$

Отмечу здесь еще одну, на первый взгляд экзотическую, тройку, для которой

$$y = 3^8 \text{ и } z = (3^{16} + 1)/2 \text{ (это число простое).}$$

Вероятно, множество подобных троек бесконечно, однако в дальнейшем я приведу, кроме данного, лишь несколько примеров на эту тему, так как объем вычислений для проверки простоты стремительно возрастает, тогда как мои возможности ограничены, и никакой общей теоремы на эту тему я не знаю[1)].

Я не знаю, конечно или нет множество всех пифагоровых троек с двумя простыми или с простым и степенью простого (другие возможности, как будет показано, исключены).

Бо̀льшая часть доказательств носит чисто арифметический характер, а другая в основном использует лишь классические результаты элементарной теории чисел (теории сравнений), восходящие к Эйлеру. Заинтересованный читатель найдет их доказательства во всех учебниках, названных в списке литературы. Замечу, что и сборник «Математическое просвещение» многократно писал (и продолжает писать) об этих материях.

Исключение составляют два утверждения о диофантовых уравнениях, которые я также использую, привожу ссылки, но не привожу доказательств. В оправдание отмечу, что отчасти их применение лишь упрощает окончательные формулировки и, с другой стороны, хотя формулировки этих утверждений элементарные, элементарных и коротких доказательств, кажется, до сих пор нет (такое случается часто, когда речь идет о диофантовых уравнениях).

2. В основном мы будем использовать стандартные обозначения:
$\mathbb{C}$ — поле комплексных чисел;
$\mathbb{R}$ — поле вещественных чисел;
$\mathbb{Q}$ — поле рациональных чисел;
$\mathbb{Z}$ — кольцо (группа) целых чисел;
$\mathbb{N}$ — натуральный ряд чисел,
а также
$\mathbb{P}$ — множество простых чисел;
$\mathbb{P}^\times$ — множество натуральных степеней простых чисел.

Кроме того, значок $\square$ будет символизировать конец доказательства, а иногда — примера или какого–нибудь иного рассуждения.

[1)] Список примеров заметно расширил М. Н. Вялый. В конце статьи мы кратко обсудим, как и зачем это делать.

3. С конца 80-х годов я пользовался поддержкой, советами и многочисленными консультациями по конкретным вопросам теории чисел (и другим) Л. Л. Степановой, к которой я всегда испытывал чувство симпатии и глубокого уважения. Несколько (довольно скептических) замечаний она успела сделать и по поводу первоначального варианта данного сочинения[2)].

Различные задачи, связанные с пифагоровыми тройками, обычно предлагает своим студентам Е. И. Деза, и мысль рассмотреть тройки со степенями простых посетила меня, когда по служебной необходимости я слушал отчеты ее подопечных.

Часть из детально описанных здесь результатов были сформулированы на Тульской конференции [2], и я признателен В. Н. Чубарикову, который посоветовал мне не стесняться объявить такой доклад.

Я благодарен Е. И. Деза и Б. Н. Кукушкину, которые указали мне на необходимость уточнить некоторые рассуждения. Наконец, вклад М. Н. Вялого в улучшение текста заметно превысил даже те стандарты, которые были приняты в прежние времена.

§1. Простейшие случаи

1. Для удобства ссылок мы сформулируем следующие два очевидных утверждения в виде лемм.

Лемма 1. *Если в пифагоровой тройке x — степень простого, то*

$$x = 2^{\alpha+1}, \;\; y = 4^{\alpha} - 1, \;\; z = 4^{\alpha} + 1, \tag{3}$$

где α — натуральное число.

Доказательство. Ясно, что в формуле (2) в этом случае $a = 2^{\alpha}$, $b = 2^{\beta}$, где $0 \leqslant \beta < \alpha$. Если $\beta > 0$, то y окажется четным. □

Лемма 2. *Если в пифагоровой тройке y — степень простого, то*

$$x = 2b(b+1), \;\; y = 2b + 1, \;\; z = (b+1)^2 + b^2, \tag{4}$$

в частности, $z = x + 1$ и $2z = y^2 + 1$.

Доказательство. Действительно, в этом случае $a - b = 1$. □

Заметим, что в этих двух случаях очевидно, что когда одна из компонент пифагоровой тройки — степень простого, *две другие компоненты определяются однозначно.* Оказывается, это верно и тогда, когда степенью простого является z-компонента, однако в этом случае доказательство не так тривиально (см. ниже).

[2)] Лидия Леонидовна Степанова (1941–2004) работала доцентом кафедры теории чисел Московского педагогического гос. университета.

2. Следующая лемма «отсекает» еще один из тривиальных случаев.

Лемма 3. *Если в пифагоровой тройке $x \in \mathbb{P}^\times$ и $y \in \mathbb{P}^\times$, то $x = 4$, $y = 3$. В частности, все три компоненты — степени простых только для тройки $\{4, 3, 5\}$.*

Доказательство. Мы воспользуемся леммой 1. Так как $3 \mid (4^\alpha - 1)$, то из формулы (3) вытекает, что в условиях данной леммы

$$(2^\alpha - 1) \cdot (2^\alpha + 1) = 3^\beta$$

с некоторым натуральным β. При $\alpha > 1$ оба стоящих слева сомножителя были бы *натуральными* степенями числа 3. Но тогда число 3 оказалось бы делителем их разности, а это не так. Поэтому $\alpha = 1$. □

§2. Случай, когда z — степень простого

1. По формуле (2), в этом случае z представляется в виде суммы двух квадратов, и мы сначала напомним, когда это происходит.

Для простых z вопрос о такой представимости начал рассматривать Ферма, который угадал точный ответ. Доказательство нашел Эйлер. Он же начал рассматривать составные числа. Окончательное решение давно помещают в каждый учебник теории чисел, см., в частности, [3–7] из списка литературы.

Представление $c = a^2 + b^2$ натурального числа c называется *собственным,* если $\gcd(a, b) = 1$. По смыслу нашей задачи (неприводимость) и ввиду формул (2) нам интересны как раз такие представления. Используя комплексную символику, представление $c = a^2 + b^2$ можно переписать в виде $c = |a + ib|^2$, и такая запись может оказаться полезной. Например, из нее легко получается, что вместе с c при натуральном n собственное представление имеет c^n, а при нечетном c такое представление имеет $2c = |(1 + i)(a + ib)|^2$. Эти факты можно рассматривать как пояснение к формулировке следующей ниже леммы 4.

Имея представление $c = a^2 + b^2$, мы можем получить еще несколько представлений, меняя местами a и b и меняя их знаки. Говоря о единственности, мы всегда будем иметь в виду *единственность этого класса эквивалентности*.

Приведем для ясности несколько простых числовых примеров. Числа 3 и 4 не представляются в виде суммы двух квадратов, числа 5 и 10 представляются однозначно (в указанном выше смысле). Число 65 — минимальное из имеющих два собственных представления (и не имеющее других). Число 50 имеет два представления, из которых одно собственное, а второе нет. Число 20 собственных представлений не имеет, однако $20 = 2^2 + 4^2$.

Основная теорема состоит в том, что *простое нечетное p тогда и только тогда имеет (непременно собственное) представление, когда $p \equiv 1 \pmod 4$, причем представление единственно.*

В общем случае ответ несколько более сложен, однако есть ситуация, когда формулировка почти не меняется:

Лемма 4. *Пусть p — нечетное простое число, n — натуральное число и число c имеет вид p^n или $2p^n$. В таком случае условие $p \equiv 1 \pmod 4$ остается критерием представимости c в виде суммы двух квадратов. Кроме того, если условие $p \equiv 1 \pmod 4$ выполняется, то существует единственное собственное представление.*

2. Из леммы 4 сразу вытекает, что z-компонента (неприводимой) пифагоровой тройки тогда и только тогда принадлежит множеству $\mathbb{P}^\times$, когда для соответствующего простого p имеем $p \equiv 1 \pmod 4$. При этом в представлении $z = a^2+b^2$ по формуле (2) компоненты a и b однозначно определяются по z. Следовательно, однозначно определяются две другие компоненты тройки — числа x и y.

Сопоставляя это со сказанным выше, мы получаем, что *если в пифагоровой тройке какая-то из компонент — степень простого числа, то две другие компоненты однозначно определяются по этой компоненте.*

§3. Тройки с $\mathbb{P}^\times$-компонентами x, z

1. Число вида $2^m + 1$ с натуральным m может оказаться простым только в том случае, когда m не имеет нетривиальных нечетных делителей, т.е. $m = 2^n$, так что число имеет вид

$$f_n = 2^{2^n} + 1$$

(числа Ферма). Простые такого вида называются простыми Ферма. Согласно теореме Гаусса, простые Ферма играют центральную роль при описании случаев, когда правильный многоугольник может быть построен циркулем и линейкой.

При $n = 0, 1, 2, 3, 4$ числа f_n являются простыми, но число $f_5 = 2^{32} + 1$, как заметил Эйлер, делится на простое число 641 (дополнительный множитель также является простым числом). Не известно ни одного простого Ферма с $n > 4$, зато относительно многих чисел Ферма с $n \geqslant 5$ доказано, что они являются составными, в частности, это так, если $5 \leqslant n \leqslant 32$, и сейчас считается правдоподобным, что простых Ферма с $n \geqslant 5$ нет[3)].

[3)] С развитием вычислительной техники появляются новые сведения и о числах Ферма. Свежую информацию по этому поводу, разумеется, можно найти в Интернете, см., например, страницу, которую поддерживает Вильфрид Келлер (Wilfrid Keller) `http://www.prothsearch.net/fermat.html`

2. Простые Ферма естественно появляются при описании пифагоровых троек, указанных в заглавии данного параграфа. Нам будет удобно начать со следующей элементарной леммы.

Лемма 5. *Пусть k, l, m — натуральные числа. Если*

$$2^k + 1 = (2^l + 1)^m \tag{5}$$

и $m > 1$, то $k = 3$, $l = 1$ и $m = 2$.

Доказательство. Из условий (5) и $m > 1$ вытекает, что $k > m \cdot l \geqslant 2l$. Раскрывая правую часть в (5) по формуле бинома, мы получим, что

$$2^{k-l} = m + n \cdot 2^l,$$

где $n \in \mathbb{N}$. Отсюда следует, что $2^l \mid m$. В частности, m — четное число, так что $(2^l + 1)^m = t^2$, где $t \in \mathbb{N}$. По формуле (5), имеются такие $k_1, k_2 \in \mathbb{N}$, что

$$t - 1 = 2^{k_1},\ t + 1 = 2^{k_2} \ \text{ и } \ k_1 + k_2 = k.$$

Очевидно, что $2^{k_1 - 1}(2^{k_2 - k_1} - 1) = 1$, откуда вытекает, что $k = 3$ и доказательство легко завершается. □

Теорема 1. *В (неприводимой) пифагоровой тройке $\{x, y, z\}$ компоненты x и z тогда и только тогда обе принадлежат к $\mathbb{P}^\times$, когда z — простое Ферма, причем $z > 3$.*

Доказательство. Предположим сначала, что z — простое Ферма и $z > 3$. Тогда, в частности, $z = 2^{2l} + 1$, где $l \in \mathbb{N}$. По лемме 4, простое число z имеет в точности одно собственное представление в виде суммы квадратов. Поэтому в формулах (2) будет $a = 2^l$, $b = 1$, так что $x = 2^{l+1}$.

Докажем обратное утверждение. По условию, $z = p^m$, где p — простое число и m — натуральное. Мы должны убедиться, что p — простое Ферма и что $m = 1$.

В соответствии с леммой 1 имеем представление $x = 2^{k+1}$, $z = 2^{2k} + 1$ с некоторым натуральным k. Так как $(p - 1) \mid (p^m - 1)$, то $p = 2^l + 1$ с некоторым натуральным l, и это означает, что p — простое Ферма. Далее,

$$2^{2k} + 1 = z = (2^l + 1)^m.$$

Так как степень двойки слева четная, то из леммы 5 вытекает, что $m = 1$.□

Из сказанного выше следует, что в данный момент мы в состоянии предъявить только четыре тройки данного типа. Не исключено, что других таких троек нет (а если есть, то заведомо их компоненты — фантастически большие числа). Поэтому тройки последнего типа, которыми мы займемся ниже, имеют особенный интерес.

§4. Тройки с $\mathbb{P}^\times$-компонентами y, z

1. Так как в рассматриваемом случае $y \in \mathbb{P}^\times$, то, по лемме 2,

$$2z = 1 + y^2. \tag{6}$$

Легко видеть, что каждое целочисленное решение уравнения (6) имеет нечетные компоненты и что мы получим пифагорову тройку, добавляя к y, z число $x = z - 1$.

Таким образом, дело свелось к вопросу о разрешимости в степенях простых очень простого (с виду) уравнения (6). Хотя вопрос о разрешимости этого уравнения *в целых числах* тривиален, целочисленная разрешимость уравнения

$$2v^l = 1 + u^k, \tag{7}$$

в зависимости от выбора k, l уже́ представляет большой интерес. Для наших целей достаточно четных k и простых u, v, однако не лишено смысла попытаться рассмотреть более общую ситуацию.

Замечание. Уравнение (7) — частный случай *диофантова уравнения* вида $f(u, v) = 0$, где f — полином с целочисленными коэффициентами. Основная проблема относительно таких уравнений — это проблема конечности числа целочисленных решений[4)]. Проблема разрешимости, а также проблема поиска нетривиальных решений могут существенно различаться по сложности для внешне очень похожих уравнений. Многочисленные примеры на эту тему имеются, в частности, в популярной когда-то брошюре [9].

Первые существенные результаты на эту тему в общем случае получил в 1909 г. А. Туэ, а окончательное решение проблемы конечности для таких уравнений через 20 лет нашел К. Зигель. Отметим популярную статью [10], из которой среди прочего легко понять, как действовал Туэ. Формулировка теоремы Зигеля предполагает знакомство с целым рядом дополнительных понятий, и мы от нее воздержимся.

Вместе с тем, для (невырожденных) двучленных диофантовых уравнений $au^k + bv^l = c$, включающих уравнение (7), ответ на один из основных вопросов в принципе описывается очень просто: если $k, l \geqslant 2$, причем хотя бы одно из этих неравенств строгое, то множество решений конечно, тогда как в других случаях реализуются и сравнительно просто распознаются все три возможности (решений нет, множество решений конечно или бесконечно).

[4)] Сравнительно недавно была решена заметно более сложная проблема конечности числа *рациональных* решений. Отметим очень интересную (но далеко не элементарную) статью [8] на эту тему.

Однако, вообще говоря, поиск конструктивных априорных оценок решений и, тем более, поиск всех решений, как правило, даже в самых простых (по виду) случаях — сложная задача. Дополнительное условие простоты (компонент) решений может как упростить, так и усложнить задачу.

2. Теперь мы приступим непосредственно к вопросу о разрешимости в степенях простых уравнения (6). В конце концов мы убедимся, что в случае разрешимости степени простых далеко не произвольны. Вначале мы рассмотрим некоторые частные случаи уравнения (7).

В следующей лемме $k, l, u \in \mathbb{N}$ и $q \in \mathbb{P}$.

Лемма 6. *Предположим, что $q \geqslant 3$ и что k — нечетное число. Если $2q^l = 1 + u^k$, то $k = 1$.*

Доказательство. Допустим, что $k \geqslant 3$, и покажем, что это приводит к противоречию. Не ограничивая общности, мы можем (и будем) считать, что $k \in \mathbb{P}$.

Так как k — нечетное число, то $(u+1) \mid (u^k+1)$. Кроме того, u — нечетное число, причем $u > 1$. Поэтому $u = 2q^t - 1$, где $t \in \mathbb{N}$. Далее, $2q^l \geqslant 1 + u^3 > (1+u)^2$, откуда легко следует, что $l > 2t$.

Имеем

$$\begin{aligned} 2q^l &= 1 + (-1 + 2q^t)^k \\ &= k \cdot (2q^t) - \frac{k(k-1)}{2} \cdot (2q^t)^2 + \dots, \end{aligned}$$

так что

$$q^{l-t} = k - \frac{k(k-1)}{2} \cdot (2q^t) + \dots.$$

Из этой формулы сразу вытекает, что $q \mid k$. Так как k — простое число, то $k = q$. Заменяя в этой формуле k на q и вспоминая, что $l > 2t$, мы получаем противоречие: левая часть и все слагаемые справа, кроме первого, делятся на q^{t+1}. □

Замечание. В последней лемме снять предварительное условие $q \in \mathbb{P}$ нельзя. Действительно, при произвольном целом k уравнение $2v = 1 + u^k$ разрешимо в натуральных числах: в качестве u годится любое нечетное число. Например, $2 \cdot 14 = 1 + 3^3$. □

Из леммы 6, в частности, вытекает, что разрешимость уравнения (7) в простых u, v влечет за собой тот факт, что фигурирующий там показатель *k не имеет нетривиальных нечетных делителей*, т. е. это число представляется в виде 2^n с целым $n \geqslant 0$. Оказывается, аналогичный факт имеет место и в отношении показателя l.

Следующая лемма — это теорема Штёрмера (C. Störmer), установленная им еще в 1895 г. Признаюсь, что первоначально, еще не зная об этой теореме, я собирался поместить (не очень короткое) доказательство аналогичного утверждения, но с дополнительным условием простоты переменной v. Однако затем я нашел работу Лунгрена [11], в которой среди прочего содержатся далеко идущие обобщения этого факта и детальные ссылки на многие предшествующие работы[5)]. Кроме того, я вспомнил один тезис П. Халмоша и решил ему последовать[6)].

Лемма 7. *Пусть $l \geqslant 3$ — нечетное натуральное число. Тогда уравнение $2v^l = 1 + u^2$ не имеет натуральных решений $\{u, v\}$, для которых $v > 1$.*

3. Соединяя леммы 6 и 7, мы получаем ту информацию о степенях простых в пифагоровых тройках, о которой сказано во введении. Однако, если иметь в виду замечание на с. 112, то ясно, что в первую очередь имеет смысл более тщательно разобраться с проблемой разрешимости в натуральных числах $\{u, v\}$ двух конкретных уравнений:

$$2v^2 = 1 + u^4 \text{ и } 2v^4 = 1 + u^2.$$

Первое из этих уравнений существенно проще второго (причем проще и ответ на вопрос, и путь к нему).

Лемма 8. *Уравнение $2v^2 = 1 + u^4$ не имеет никаких натуральных решений, кроме тривиального $u = v = 1$.*

Доказательство. Положим $w = v^2 - 1$. Тогда w, u, v — неотрицательные целые числа, и выполняется равенство $w^2 + u^4 = v^4$. Вместе с тем, хорошо известно, что последнее уравнение не имеет натуральных решений (см., например, [14, с.81]). Поэтому $w = 0$. □

Следующая лемма, касающаяся второго уравнения — это теорема Лунгрена, доказанная им в 1942 г. Первоначальное доказательство было весьма сложным. Различные обобщения и подробные ссылки на предшествующие результаты можно найти в его статье [12]. Кстати, неоднократно предпринимались попытки найти простое и короткое доказательство, однако достигнутый прогресс лишь отчасти решает эту задачу.

[5)] Кстати, фотокопии журнала Mathematica Scandinavica, в котором содержится данная и ряд других работ Лунгрена, свободно доступны в Интернете.

[6)] В своем хорошо известном (специалистам) задачнике по гильбертовым пространствам (с. 68 русского перевода) он пишет в связи со спектральной теоремой: «Мощные общие теоремы затем и существуют, чтобы их использовали, и упрямое пренебрежение ими приводит к потере понимания по меньшей мере так же часто, как и к достижению его.» Другое дело, что, используя такое средство, полезно узнать, откуда оно взялось, т. е. в какой-то момент проверить доказательство или придумать новое.

Лемма 9. *Уравнение* $2v^4 = 1+u^2$, *кроме тривиального, имеет в точности одно решение:* $u = 239, v = 13$.

Из сказанного выше вытекает следующая теорема, которая в качестве следствия дает (общее, но не полное) описание степеней простых, которые могут появляться в пифагоровой тройке в качестве y и z.

Теорема 2. *При натуральных* $k \geqslant 2$ *и* l *уравнение* $2q^l = 1 + u^k$ *относительно* $3 \leqslant q \in \mathbb{P}$ *и* $u \in \mathbb{N}$ *может иметь решения только в следующих случаях*: $l = 4$, $k = 2$; $l = 2$, $k = 2$; $l = 1$, $k = 2^n$ *с натуральным* n.

По поводу теоремы 2 имеет смысл сделать несколько замечаний. Во-первых, при $l = 4$, $k = 2$ в соответствии с леммой 9 (т. е. теоремой Лунгрена) имеется в точности одно решение $q = 13$, $u = 239$, даже без предварительного предположения $q \in \mathbb{P}$. Тот факт, что в теореме Лунгрена обе компоненты оказались простыми числами можно, по-моему, отнести к разряду чудес, и это действительно делает пифагорову тройку с $y = 239$, $z = 13^4$ по-своему исключительной.

Во-вторых, в §5 мы предъявим (хорошо известный) алгоритм, позволяющий выписывать по возрастанию компоненты *всех* натуральных решений уравнения $2v^2 = 1+u^2$. Среди этих пар встречаются пары простых (и это помогает составить короткую из таблиц, указанных во введении), однако не известно, конечно или нет множество таких пар (см. по этому поводу, например, [13, с.83]; этот популярный источник заметно устарел, но проблема, по-моему, остается). Кстати, на этом пути довольно быстро появляется пара Лунгрена.

Наконец, третий случай в теореме 2 приводит к поиску таких простых нечетных p и неотрицательных целых n, что $(p^{2^n} + 1)/2$ — снова простое, и это напоминает классическую проблему о простых Ферма. Некоторые из таких чисел для $n = 1$ собраны в верхней строке первой из таблиц во введении. Кроме того, есть и «большие» пары, например, $y = 3^8$, $z = (3^{16} + 1)/2$ (также упомянутая во введении). Однако, хотя по сравнению с проблемой о простых Ферма возможности вроде бы расширяются (можно менять не только n, но и p), я не знаю, бесконечно ли это множество.

§5. Комментарии и вычисления

1. Нам осталось более детально прокомментировать второй и третий случаи в теореме 2. В этом пункте мы разберем второй случай, т. е. уравнение

$$u^2 - 2v^2 = -1. \tag{8}$$

Наряду с уравнением (8) имеет смысл рассматривать так называемое *уравнение Пелля*[7)]

$$u^2 - 2v^2 = 1. \tag{9}$$

Существует несколько подходов к описанию множества всех решений диофантовых уравнений (8) и (9), и мы вкратце опишем некоторые из них (детали можно найти в учебниках, перечисленных в списке литературы; там же указаны некоторые дополнительные источники).

Обозначим через $\mathbb{Q}(\sqrt{2})$ поле, которое получается в результате присоединения к полю $\mathbb{Q}$ числа $\sqrt{2}$. Таким образом, каждый элемент $\lambda \in \mathbb{Q}(\sqrt{2})$ однозначно представляется в виде $\lambda = \alpha + \beta\sqrt{2}$, где $\alpha, \beta \in \mathbb{Q}$. В частности, $\mathbb{Q}(\sqrt{2})$ естественно наделяется структурой двумерного векторного пространства над полем $\mathbb{Q}$ с базисом $\{1, \sqrt{2}\}$.

Каждому элементу $\lambda = \alpha + \beta\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ сопоставим $\mathbb{Q}$-линейный оператор T_λ умножения на λ. Заметим, что в базисе $\{1, \sqrt{2}\}$ оператору T_λ отвечает матрица

$$\begin{pmatrix} \alpha & 2\beta \\ \beta & \alpha \end{pmatrix}$$

с детерминантом $\det(T_\lambda) = \alpha^2 - 2\beta^2$. В (алгебраической) теории чисел это рациональное число часто называют *нормой* числа λ и обозначают $\|\lambda\|$. Мы будем использовать промежуточное обозначение. Именно, имея в виду, что соответствие $\lambda \to T_\lambda$ — изоморфизм полей, мы будем писать $\det(\lambda)$ вместо $\det(T_\lambda)$. Одно из основных свойств детерминанта влечет за собой соотношение

$$\det(\lambda_1 \cdot \lambda_2) = \det(\lambda_1) \cdot \det(\lambda_2),$$

справедливое для каждой пары чисел $\lambda_1, \lambda_2 \in \mathbb{Q}(\sqrt{2})$.

Обозначим через $\mathbb{Z}(\sqrt{2})$ совокупность всех тех $\lambda = \alpha + \beta\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, для которых $\alpha, \beta \in \mathbb{Z}$. Очевидно, что $\mathbb{Z}(\sqrt{2})$ составляет подкольцо в $\mathbb{Q}(\sqrt{2})$.

Если $\lambda \in \mathbb{Z}(\sqrt{2})$, то $\det(\lambda) \in \mathbb{Z}$. Так как $\det(1) = 1$, то для обратимых (относительно умножения) элементов $\lambda \in \mathbb{Z}(\sqrt{2})$ число $\det(\lambda)$ будет обратимым элементом кольца $\mathbb{Z}$, так что в этом случае $\det(\lambda) = \pm 1$. Правило составления обратной матрицы показывает, что обратное тоже верно: если $\lambda \in \mathbb{Z}(\sqrt{2})$ и $\det(\lambda) = \pm 1$, то λ — обратимый элемент кольца $\mathbb{Z}(\sqrt{2})$.

Так как $\det(\alpha+\beta\sqrt{2}) = \alpha^2-2\beta^2$, то описание решений уравнения Пелля равносильно описанию группы тех обратимых элементов $\lambda \in \mathbb{Z}(\sqrt{2})$, для которых $\det(\lambda) = 1$. Особенно просто выглядит описание тех обратимых

[7)] Это уравнение точнее было бы называть уравнением Эйлера, уравнением Ферма или даже (в соответствии с легендой) уравнением Архимеда. Однако Эйлер в своих исследованиях назвал его по имени английского математика, который как раз этим уравнением никогда не занимался, и традиция называть уравнение (9) уравнением Пелля нарушается не часто. Напротив, иногда уравнением Пелля называют и уравнение (8).

$\lambda = \alpha + \beta\sqrt{2}$, для которых $\alpha, \beta > 0$. Оказывается, что среди них имеется $\lambda_1 = \alpha_1 + \beta_1\sqrt{2}$ с наименьшим значением $\alpha + \beta\sqrt{2}$, и все остальные (вместе с этим в качестве первого члена) составляют последовательность, которая формируется по правилу

$$\alpha_n + \beta_n\sqrt{2} = (\alpha_1 + \beta_1\sqrt{2})^n, \;\; n = 1, 2, 3, \ldots .$$

Легко убедиться, что $\alpha_1 = 3, \beta_1 = 2$. Детальное (причем вполне элементарное) обсуждение этого факта можно найти, например, в [3, с. 340].

Пара $\{1, 1\}$ служит (минимальным) положительным решением уравнения (8). Это эквивалентно тому, что $\det(\mu_1) = -1$, где $\mu_1 = 1 + \sqrt{2}$. Заметим, что $\mu_1^2 = \lambda_1$. Все остальные натуральные решения уравнения (8) получаются из $\mu_1 \cdot \lambda_1^n = \mu_1^{2n+1}$, где $n \in \mathbb{N}$.

Замечание. Аналогично можно размножать решения уравнения $u^2 - 2v^2 = m$ с $m \in \mathbb{Z}$. Однако у такого уравнения натуральные решения существуют не при каждом m. Например, при $m = 2$, как легко видеть, решения есть, тогда как при $m = 3$ решений нет. □

Детальное изучение таких уравнений — предмет академической науки, с которым можно познакомиться по первым главам монографии [15], однако без предварительной алгебраической подготовки сознательное чтение этой монографии практически невозможно.

Еще один способ найти натуральные решения уравнений (8) и (9) дает разложение числа $\sqrt{2}$ в цепную дробь. Прочесть о цепных дробях можно во всех учебниках, включенных в список литературы. Более подробную информацию можно найти, например, в [16] и [17].

Если не прибегать к оборотам вроде «выражение вида» (фактически превращающих вводимое понятие в первичное), первая сложность появляется, когда возникает желание дать корректное определение (бесконечной) цепной дроби[8)]. Мы не будем давать общего определения, но поясним всё на примере упомянутого выше разложения.

Ясно, что

$$\sqrt{2} = 1 + \frac{1}{1+\sqrt{2}} = 1 + \frac{1}{2 + \dfrac{1}{1+\sqrt{2}}} = 1 + \frac{1}{2 + \dfrac{1}{2 + \dfrac{1}{1+\sqrt{2}}}} \tag{10}$$

и т. д. Вычеркивая в заключенных между знаками равенства выражениях

[8)] Кстати, ситуация здесь практически не отличается от той, которая имеет место, когда начинают рассматривать, например, бесконечные ряды. Довольно часто, особенно в тех вузах, где математика имеет как бы вспомогательный характер (не говоря уже́ о школе) определение ряда фактически не дается. Быть может, как раз в таких случаях этот вульгаризм («выражение вида») можно считать оправданным, однако тогда не стоит удивляться, почему именно *хорошие* студенты долго привыкают к рядам. Кстати, подобно рядам, цепные дроби можно «составлять» не только из чисел.

последнее $1/(1+\sqrt{2})$, мы получим последовательность «многоэтажных» дробей, которые в результате естественного приведения (не надо, например, в самом начале заменять $1/2$ на $3/6$) превращается в последовательность несократимых дробей

$$1 = 1/1,\ 3/2,\ 7/5,\ 17/12, \ldots.$$

Члены этой последовательности очень хорошо (с разных сторон) приближаются к $\sqrt{2}$ и называются *подходящими дробями* цепной дроби. Между элементами (числителями и знаменателями) подходящих дробей имеются простые рекуррентные соотношения (ниже они указаны). Это позволяет в данном случае бесконечную цепную дробь понимать как *последовательность всех ее подходящих дробей,* и на этом пути можно корректно ввести и общее понятие. Тот факт, что построенная цепная дробь представляет число $\sqrt{2}$ теперь можно (красиво) записать в виде

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

Положим дополнительно $u_0 = 1, v_0 = 0$ и обозначим через u_n и v_n при натуральных n соответственно последовательность числителей и знаменателей подходящих дробей.

Оказывается, при четных n пары $\{u_n, v_n\}$ будут давать (указанную выше) последовательность решений уравнения Пелля, а при нечетных — уравнения (8).

Рекуррентные соотношения между элементами пар можно записывать по-разному, в частности, так:

$$\begin{cases} v_{n+1} = u_n + v_n, \\ u_{n+1} = v_n + v_{n+1}. \end{cases}$$

Так как $u_0 = 1, v_0 = 0, u_1 = 1, v_1 = 1$, то мы без хлопот можем найти и рассмотреть первый десяток пар (так как обе последовательности экспоненциально возрастают, то затем возникают большие числа),

n	0	1	2	3	4	5	6	7	8	9
u_n	1	1	3	7	17	41	99	239	577	1393
v_n	0	1	2	5	12	29	70	169	408	985

Так как при четных n числа v_n четные, то легко убедиться, что, кроме $\{3, 2\}$, уравнение Пелля не имеет решений, v-компонента которых — степень простого.

С другой стороны, даже из приведенной краткой таблицы видно, что уравнение (8) вначале имеет решения, обе компоненты которых — простые

числа. Вместе с тем, бесконечно ли множество таких решений, кажется, никто не знает.

Пара Лунгрена — это $\{u_7, v_7\}$. Используя теорему Лунгрена (лемма 9) и простые соображения типа леммы 8, легко убедиться, что за исключением чисел 0 и 1 в самом начале строк $\{u_n\}$ и $\{v_n\}$ *в этих строках, кроме* $v_7 = 13^2$*, нет других квадратов.* При нечетных n это уже установлено. Поэтому остается проверить, что уравнения

$$x^4 - 2y^2 = 1 \text{ и } x^2 - 2y^4 = 1$$

не имеют натуральных решений. Эта проверка не требует особой фантазии, и мы ее опустим, тем более, что этот факт имеет лишь косвенное отношение к нашей теме. Заметим только, что в конечном счете второе уравнение сводится к первому.

2. Нам осталось обсудить последнюю возможность из указанных в теореме 2. В этом пункте мы сформулируем некоторые общие определения и результаты и приведем основанные на них примеры. Затем мы приведем дальнейшие примеры, требующие «нечеловеческих» вычислений. Кстати, каждый, кто имеет доступ к продвинутой вычислительной технике, сможет расширить список таких примеров.

Пусть $a, b \in \mathbb{N}$, причем $\gcd(a, b) = 1$. Рассмотрим арифметическую прогрессию $A \stackrel{\text{def}}{=} \{ak + b \mid k \in \mathbb{N}\}$. При $t > 0$ обозначим через $\pi_A(t)$ количество простых чисел $p < t$, попадающих в арифметическую прогрессию A.

Классическая теорема Дирихле устанавливает, что $\pi_A(t) \to \infty$ при $t \to \infty$. Другими словами, прогрессия A содержит бесконечное множество простых. Представление о том, как рассуждал Дирихле, можно получить по очень красивому (простому, но не элементарному) описанию этой темы в [18].

В дальнейшем теорема Дирихле уточнялась и обобщалась. Эти уточнения и обобщения опирались на изучение так называемой ζ-функции Римана как аналитической функции в комплексной плоскости[9)].

Здесь (и в дальнейшем) нам потребуется функция Эйлера $\varphi = \varphi(n)$ натурального аргумента, значение которой равно количеству таких m, где $1 \leqslant m \leqslant n$, что $\gcd(m, n) = 1$. По определению, $\varphi(1) = 1$. Легко показать,

[9)] ζ-функцию как функцию вещественного переменного знал Эйлер, а Дирихле использовал в своем доказательстве теоремы об арифметической прогрессии. Заслуга Римана в данном случае в том, что он первым начал изучать ζ-функцию как аналитическую функцию комплексного переменного, поняв среди прочего значение ее поведения в комплексной плоскости для точного описания распределения простых чисел. Заметим, кстати, что Риман слушал лекции Дирихле и что в своем единственном мемуаре по теории чисел он ссылается на Гаусса и Дирихле, но почему-то не ссылается на П. Л. Чебышева (с написанными по-французски работами которого он мог быть знаком) и на Мёбиуса.

что $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ и что $\varphi(xy) = \varphi(x)\varphi(y)$, если $\gcd(x,y) = 1$, и это позволяет легко находить значения φ при небольших значениях аргумента. С алгебраической точки зрения, $\varphi(n)$ — это количество обратимых (по умножению) элементов кольца $\mathbb{Z}/(n)$ классов вычетов по модулю n.

Указанные обобщения описаны, например, в [19]. Результат состоит в том, что имеет место эквивалентность:

$$\pi_A(t) \sim \frac{1}{\varphi(a)} \cdot \frac{t}{\log t},$$

где $\log t$ обозначает натуральный логарифм.

При $n \in \mathbb{N}$ и $3 \leqslant p \in \mathbb{P}$ положим

$$g_p^n \stackrel{\text{def}}{=} (p^{2^n} + 1)/2.$$

Удобно представлять себе $G = \{g_p^n\}$ как бесконечную вправо и вверх матрицу, *столбцы* C_p которой занумерованы простыми числами и идут снизу вверх, а *строки* S_n — натуральными и идут слева направо.

С точки зрения нашей исходной проблемы наибольший интерес представляет вопрос о бесконечности подмножества простых среди элементов матрицы G. Ответа на этот вопрос я не знаю. По аналогии с числами Ферма представляет интерес не только специальный вопрос о бесконечности подмножества простых в столбцах C_p, но и вопрос о бесконечности подмножества составных в них. Некоторая (довольно скудная) информация по этому поводу имеется (и приводится немного ниже). Следующий пример показывает, что, применяя теорему Дирихле, на остающийся (самый неинтересный) вопрос о составных в строках матрицы G легко дать положительный ответ.

Пример. Пусть b — четное положительное число, $m \in \mathbb{N}$ и $a = 1 + b^m$. Рассмотрим прогрессию $A = \{ak + b \mid k = 1, 2, \ldots\}$. Так как $\gcd(a,b) = 1$, то, по теореме Дирихле, A содержит бесконечное подмножество простых. Далее, если $q = ak + b$, то $q^m \equiv b^m \equiv -1 \pmod{a}$, т.е. $a \mid (q^m + 1)$. Так как $a > 2$ то, в частности (при $m = 2^n$) получается, что *каждая строка* S_n *матрицы* G *содержит бесконечное подмножество составных чисел.* □

В обзоре [20] автор отмечает, что еще в 1877 г. Пепэн (T. Pepin) установил, что число Ферма $f > 3$ тогда и только тогда является простым, когда

$$3^{(f-1)/2} \equiv -1 \pmod{f}.$$

Доказательство этого факта дано, например, в [6, с.47].

Если $f = 2^m + 1$, то $(f-1)/2 = 2^{m-1}$. Поэтому из теоремы Пепэна сразу вытекает следующее сравнительно содержательное утверждение: множество $F \cup C_3$, где F — множество чисел Ферма, содержит бесконечное подмножество составных чисел.

На самом деле число 3 в теореме Пепэна, а потому и в последнем утверждении легко заменить многими другими (см. ниже).

Пусть $m \geqslant 2$ — натуральное число. Следующая теорема (см., например, [6, с.16]) при $m \in \mathbb{P}$ была найдена Ферма (Малая теорема Ферма), а в общем случае — Эйлером. Именно, если $\gcd(a, m) = 1$, то $a^{\varphi(m)} \equiv 1 \pmod{m}$. Легко привести примеры, когда $a^k \equiv 1 \pmod{m}$ для $k < \varphi(m)$. Если d — наименьшее натуральное k с этим свойством, то говорят, что a принадлежит показателю d по модулю m. Легко убедиться, что $d \mid k$ для всех остальных k с указанным свойством. В частности, $d \mid \varphi(m)$.

Теперь мы приведем обобщение теоремы Пепэна. В отличие от исходного случая удобно вместо критерия дать два простых утверждения, с формальной точки зрения различающихся по степени общности. Вместе с тем, мы почти не отступаем от доказательства, приведенного в [6].

Лемма 10. *Пусть $f \geqslant 3$ — число Ферма. Если при некотором $a \in \mathbb{Z}$ выполняется сравнение*

$$a^{(f-1)/2} \equiv -1 \pmod{f}, \tag{11}$$

то f — простое число.

Доказательство. Пусть q — простой делитель числа f. Мы должны убедиться, что $q = f$. Неравенство $q \leqslant f$ очевидно.

Из сравнения (11) вытекает, что аналогичное сравнение выполняется при замене модуля f на q (с сохранением самого сравнения), так как $q \mid f$.

Пусть $f = 2^m + 1$ и пусть d — показатель, которому принадлежит a по модулю q. Тогда $d \mid 2^m$, поскольку

$$a^{f-1} \equiv 1 \pmod{q},$$

так что $d = 2^\mu$ с некоторым $\mu \in \mathbb{N}$, причем $\mu \leqslant m$. Вместе с тем из (11) вытекает, что

$$a^{(f-1)/2} \equiv -1 \pmod{q},$$

так что $d > (f-1)/2$. Поэтому $\mu > m-1$. Следовательно, $\mu = m$ и $d = f-1$. Но тогда $(f-1) \mid (q-1)$, так как $\varphi(q) = q-1$. Следовательно, $f \leqslant q$. □

Для справедливости обратного (к лемме 10) утверждения относительно a придется сделать некоторое дополнительное (по существу, формальное) предположение.

Пусть $3 \leqslant p \in \mathbb{P}$. Тогда $\mathbb{Z}/(p)$ — конечное поле, так что группа его обратимых элементов — циклическая группа порядка $p-1$. Классическая формулировка (существование первообразного корня) и доказательство этого факта имеется, например, в [5, с.95], в приведенной здесь форме теорема доказана, например, в [21, с.12] (кстати, доказательство становится существенно более прозрачным, если считать известными основные свойства

φ-функции Эйлера). Количество элементов, которые могут служить образующими в циклической группе обратимых элементов поля $\mathbb{Z}/(p)$ равно $\varphi(p-1)$. В частности, если f — простое Ферма, то получается, что образующими могут служить $(f-1)/2$ элемента.

Пусть $\lambda = \lambda_p$ — нетривиальный гомоморфизм (мультипликативной) группы обратимых элементов поля $\mathbb{Z}/(p)$ в мультипликативную группу $\{\pm 1\}$ и пусть g — (какая-нибудь) образующая исходной группы. Тогда $\lambda_p(g) = -1$, так как в противном случае гомоморфизм будет тривиальным. Поэтому $\lambda_p(g^k) = (-1)^k$. Обычно продолжают λ_p на всё поле $\mathbb{Z}/(p)$, полагая $\lambda_p(0) = 0$. Результат сквозного гомоморфизма $\mathbb{Z} \to \mathbb{Z}/(p) \to \{-1, 0, 1\}$ (это числовая полугруппа по умножению) называется символом Лежандра и имеет классическое обозначение, похожее на обозначение биномиального коэффициента,

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если } p \nmid a \text{ и сравнение } x^2 \equiv a \pmod p \text{ имеет решение,} \\ 0, & \text{если } p \mid a, \\ -1, & \text{если сравнение } x^2 \equiv a \pmod p \text{ не имеет решения.} \end{cases}$$

Довольно часто удобнее использовать для символа Лежандра обозначение «в строчку»: (a/p). Среди чисел a, для которых $1 \leqslant a < p$, в точности половина, т. е. $(p-1)/2$ удовлетворяют условию $(a/p) = 1$ (квадратичные вычеты). Отсюда следует, что для простых Ферма f равенство $(a/f) = -1$ выполняется тогда и только тогда, когда a служит образующей в группе обратимых элементов. Число 3 годится для всех простых Ферма (и с этим связана теорема Пепэна). При $f = 5$ появляется еще $a = 2$, а при $f = 17$ возникает множество

$$\{3, 5, 6, 7, 10, 11, 12, 14\}. \tag{12}$$

Вычислять значение символа Лежандра, исходя только из приведенного определения, — унылое занятие. Однако во всех учебниках теории чисел описаны различные способы для сравнительно небольших p и a сделать это довольно быстро (надо ввести символ Якоби и применять квадратичный закон взаимности — один из самых красивых фактов элементарной теории чисел).

Следующий факт (доказательство которого также есть во всех учебниках) был предсказан Лежандром и строго доказан Эйлером: при простом $p \geqslant 3$

$$a^{(p-1)/2} \equiv (a/p) \pmod p.$$

Из сказанного сразу вытекает следующая лемма, включающая вторую часть теоремы Пепэна.

Лемма 11. *Если f — простое Ферма и $(a/f) = -1$, то*

$$a^{(f-1)/2} \equiv -1 \pmod{f}.$$

Пример. Данный пример представляет собой частную, но более деликатную версию примера со с. 120. Рассмотрим арифметическую прогрессию, члены которой имеют вид $q = 17k + l$, где $k = 0, 1, 2, \ldots$, а l — какой-нибудь элемент строки (12). По теореме Эйлера, $17 \mid (q^8 + 1)$ для всех таких b. По теореме Дирихле, при каждом фиксированном l среди них встречается бесконечное подмножество простых, и для всех таких простых число $(q^8 + 1)/2$ составное. Минимальное простое, которое не попадает в эту категорию — число 13 (т.е. $13^8 + 1$ не делится на 17; более того, оказывается, что число $(13^8 + 1)/2$ простое.). □

Отмечу, что ряд других фактов, известных для чисел Ферма, с небольшими модификациями или почти дословно переносится на числа g_p^n.

Делитель 641 для числа $2^{32} + 1$ Эйлер получил не «в слепую»: сначала он доказал, что каждый простой делитель числа f_n имеет вид $k \cdot 2^{n+2} + 1$ (по поводу доказательства см., например, [6, с.47]). Делитель 641 появляется при $k = 5$.

Аналогичное утверждение *сохраняется* (вместе с доказательством) *при переходе к числам g_p^n, однако в выражении для делителя $n+2$ следует поменять на $n + 1$.* Кстати, как в этом утверждении, так и в упомянутой теореме Эйлера, предположение о простоте делителя, как легко видеть, не существенно.

Далее, как и в случае чисел Ферма, числа, *стоящие в столбцах матрицы G попарно взаимно просты.* Снова доказательство, приведенное в [6, с.47–48]), сохраняется. Конечно, в отношении строк матрицы G это не верно.

3. Теперь я приведу результаты вычислений, проделанных практически «голыми руками», т. е. с использованием калькулятора. Они собраны в таблицу 1, которая аналогична начальному участку указанной выше матрицы G, однако в левом столбце вместо чисел n стоят $m = 2^n$, а вместо самих элементов g_p^n — та информация о простоте, которая у меня появилась. Буква p символизирует простоту соответствующего элемента, c — ее отсутствие, а крестик $\times$ означает, что проверить простоту соответствующего числа на калькуляторе не удалось.

В частности, неоднократно упомянутое число $(3^{16} + 1)/2$ простое. Для заполнения нижней строки и левой половины следующей за ней не требуется даже калькулятора. Кроме того, имеется еще 6 клеток таблицы, которым отвечают числа с делителем 17. Действительно, $19^4 \equiv -1 \pmod{17}$, а строчка (12) показывает, что $a^8 \equiv -1 \pmod{17}$ при $a = 3, 5, 7, 11$ и 23

Табл. 1.

16	p	c	×	×	×	×	×	×
8	c	c	c	c	p	c	c	c
4	p	p	p	p	p	p	c	p
2	p	p	c	p	c	c	p	c
	3	5	7	11	13	17	19	23

(ибо $23 = 6 + 17$). В последнем случае имеем

$$23^8 + 1 = 78\,310\,985\,282 = 2 \cdot 17 \cdot 3697 \cdot 623009.$$

М. Н. Вялый, используя программу Maple, заметно расширил эту таблицу. В таблице 2 собрана часть результатов этих вычислений. В левом столбце указан показатель степени $m = 2, 4, 8, \ldots$, а в строках — те простые $p < 100$, для которых $(p^m + 1)/2$ — также простое.

Табл. 2.

64	3										
32	3										
16	3	29	41	73							
8	13	43	47	53							
4	3	5	7	11	13	17	23	29	61	71	73
2	3	5	11	19	29	59	61	71	79		

Заинтересованный читатель сможет повторить эти вычисления (это не лишено смысла). Использование таких программ, как Maple, Mathematica, PARI и им подобных позволит значительно расширить и эту таблицу. Такое расширение имеет не только спортивный интерес, оно позволит сформулировать правдоподобные гипотезы, от чего пока, вероятно, стоит воздержаться.

Список литературы

[1] Хинчин А.Я. *Великая теорема Ферма.* М.–Л., ОНТИ ГТТИ, 1934.

[2] Горин Е.А. *Пифагоровы тройки, включающие степени простых.* Тезисы 4-й межд. конф. «Совр. проблемы теории чисел и ее прил.», Тула, 10–15 сент. 2001 г., с. 47–48.

[3] Айерленд К., Роузен М. *Классическое введение в современную теорию чисел.* М., Мир, 1987 (пер. с англ.).

[4] Бухштаб А.А. *Теория чисел.* М., Просвещение, 1966.

[5] Виноградов И.М. *Основы теории чисел.* М., Гостехиздат, 1953.

[6] Трост Э. *Простые числа.* М., Физматгиз, 1959 (пер. с нем.).

[7] Чандрасекхаран К. *Введение в аналитическую теорию чисел.* М., Мир, 1974 (пер. с англ.).

[8] McMullen C.T. *From dynamics on surfaces to rational points on curves.* Bull. of the Am. Math.Soc., 2000. Vol. 37, no 2. P. 119–140.

[9] Серпинский В. *О решении уравнений в целых числах.* М., Физматгиз, 1961 (пер. с польского).

[10] Гельфонд А.О. *О проблеме приближения алгебраических чисел рациональными.* Мат. просвещение, сер. 2, вып.2, (1957), с. 35–50.

[11] Ljunggren W. *On the Diophantine equation* $Cx^2 + D = 2y^n$. Math. Scand., 1966. Vol. 18. P. 69–86.
См. также `http://www.mscand.dk/article.php?id=1772`

[12] Ljunggren W. *On the Diophantine equation* $Ax^4 - By^2 = C$ $(C = 1, 4)$. Math. Scand., 1967. Vol. 21. P. 149–158.
См. также `http://www.mscand.dk/article.php?id=1845`

[13] Серпинский В. *Что мы знаем и чего не знаем о простых числах.* М.–Л., Физматгиз, 1963 (пер. с польского).

[14] Степанова Л.Л. *Избранные главы элементарной теории чисел.* М., Прометей, 2001.

[15] Боревич З.И., Шафаревич И.Р. *Теория чисел.* М., Наука, 1972.

[16] Хинчин А.Я. *Цепные дроби.* М.–Л., Гостехиздат, 1949.

[17] Ленг С. *Введение в теорию диофантовых приближений.* М., Мир, 1970 (пер. с англ.).

[18] Дэвенпорт Г. *Мультипликативная теория чисел.* М., Наука, 1971 (пер. с англ.).

[19] Гельфонд А.О. *Аналитический метод оценки числа простых чисел в натуральном ряде и арифметической прогрессии.* (Приложение редактора перевода к книге [6]).

[20] Рибенбойм П. *Рекорды простых чисел.* Успехи мат.наук, 1987. Т. 42, вып. 5. С. 119–176 (сокр. пер. с англ.).

[21] Серр Ж.–П. *Курс арифметики.* М., Мир, 1972 (пер. с фр.).

Горин Евгений Алексеевич, проф. кафедры мат. анализа МПГУ.
e-mail: `evgeny.gorin@mtu-net.ru`

Издательство МЦНМО

Р. Л. Добрушин. **Избранные работы по математической физике.** Под ред. Р. А. Минлоса, Ю. М. Сухова и С. Б. Шлосмана. 2007. 720 с.

Сборник содержит избранные статьи Роланда Львовича Добрушина (1929–1995) — выдающегося математика, одного из создателей современной математической статистической физики. Эти статьи были опубликованы в основном в зарубежных журналах, которые в настоящее время малодоступны современному читателю. Сборник дополнен комментариями, в которых прослеживается современное развитие идей, изложенных в публикуемых работах.

М. А. Акивис, Б. А. Розенфельд. **Эли Картан (1869–1951).** 2007. 328 с.

Книга посвящена описанию жизни и творчества великого французского математика Эли Картана, работы которого оказали огромное влияние на развитие математики в XX веке.

Р. Э. Клима, Дж. К. Ходж. **Математика выборов.** 2007. 224 с.

Вопрос о том, являются ли те или иные выборы демократичными, соответствуют ли результаты выборов воле народа, имеет много разных аспектов. В книге американских преподавателей Дж. К. Ходжа и Р. Э. Клима в научной форме, живо и наглядно обсуждаются проблемы математической теории выборов и референдумов.

Книга написана в форме учебника и рассчитана прежде всего на студентов. Для ее понимания вполне достаточно школьных знаний по математике. Книга предназначена для политологов, социологов и юристов.

Всероссийские олимпиады школьников по математике 1993–2006: Окружной и финальный этапы. Под ред. Н.Х.Агаханова. 2007. 472 с.

В книге приведены задачи заключительных (четвертого и пятого) этапов Всероссийских математических олимпиад школьников 1993–2006 годов с ответами и полными решениями.

Все приведенные задачи являются авторскими. Многие из них одновременно красивы и трудны, что отражает признанный в мире высокий уровень российской олимпиадной школы. Часть задач уже стала олимпиадной классикой.

Книга предназначена для подготовки к математическим соревнованиям высокого уровня. Она будет интересна педагогам, руководителям кружков и факультативов, школьникам старших классов. Для удобства работы приведен тематический рубрикатор.

Московские математические регаты. Сост. А. Д. Блинков, Е. С. Горская, В. М. Гуровиц. 2007. 360 с.

Математическая регата — ежегодное соревнование для школьных команд, В данном сборнике представлены материалы всех московских математических регат по 2005–06 уч. год. Приведены также правила проведения регаты, описана технология ее проведения и особенности подготовки. В приложение включены материалы школьных математических регат и регат, проведенных на всероссийских фестивалях.

Книжка адресована учителям средней школы, методистам, школьникам и может быть интересна всем любителям математики.

Геометрические олимпиады им. И. Ф. Шарыгина. Сост. А. А. Заславский, В. Ю. Протасов, Д. И. Шарыгин. 2007. 152 с.

В книге собраны задачи геометрических олимпиад им. И. Ф. Шарыгина (2005–2007) с подробными решениями. В приложении приведены две статьи И. Ф. Шарыгина и воспоминания о нем.

Пособие предназначено для школьников, учителей математики и руководителей кружков. Книга будет интересна всем любителям красивых геометрических задач.