В. СЕРПИНСКИЙ

ЧТО МЫ ЗНАЕМ И ЧЕГО НЕ ЗНАЕМ О ПРОСТЫХ ЧИСЛАХ

ФМ

WACŁAW SIERPIŃSKI

CO WIEMY, A CZEGO NIE WIEMY O LICZBACH PIERWSZYCH

WARSZAWA
PAŃSTWOWE ZAKŁADY WYDAWNICTW SZKOLNYCH

В. СЕРПИНСКИЙ

ЧТО МЫ ЗНАЕМ И ЧЕГО НЕ ЗНАЕМ О ПРОСТЫХ ЧИСЛАХ

Перевод с польского
И. Г. МЕЛЬНИКОВА

ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА • 1963 • ЛЕНИНГРАД

517 · 1
С 33

АННОТАЦИЯ

В книге выдающегося польского математика Вацлава Серпинского собраны наиболее важные, интересные и доступные широкому кругу читателей результаты, относящиеся к теории простых чисел. Приводятся многочисленные указания на нерешенные проблемы.

Доказательства теорем даются лишь в тех случаях, когда они элементарны и не очень утомительны. В основном книга имеет информационный характер. Она может быть использована учащимися старших классов средней школы, имеющими склонность к математике, студентами и учителями. Последние найдут в этой книге большой материал для занятий математического кружка.

517 · 1
С 33

АННОТАЦИЯ

В книге выдающегося польского математика Вацлава Серпинского собраны наиболее важные, интересные и доступные широкому кругу читателей результаты, относящиеся к теории простых чисел. Приводятся многочисленные указания на нерешенные проблемы.

Доказательства теорем даются лишь в тех случаях, когда они элементарны и не очень утомительны. В основном книга имеет информационный характер. Она может быть использована учащимися старших классов средней школы, имеющими склонность к математике, студентами и учителями. Последние найдут в этой книге большой материал для занятий математического кружка.

ВАЦЛАВ СЕРПИНСКИЙ

(К восьмидесятилетию со дня рождения)

14 марта 1962 г. исполнилось 80 лет со дня рождения выдающегося польского математика Вацлава Серпинского.

Интерес к математике и незаурядные способности обнаружились у Серпинского еще в школьные годы. В 1900 г. он поступил в Варшавский университет на физико-математический факультет, где в то время работал один из крупнейших представителей петербургской школы теории чисел Г. Ф. Вороной.

Свою первую научную работу Серпинский посвятил теоретико-числовой проблеме, которую сформулировал Вороной в качестве темы для конкурсных студенческих сочинений. В 1904 г. Серпинский представил сочинение «О суммировании ряда $\sum_{n>a}^{n\leq b} \tau(n) f(n)$ при условии, что $\tau(n)$ представляет число разложений n на сумму квадратов двух целых чисел». В том же году Варшавский университет на основании отзыва Вороного присудил Серпинскому за эту работу золотую медаль и присвоил ученую степень кандидата математических наук. С этого времени теория чисел становится излюбленным предметом занятий Серпинского. Число его арифметических работ быстро растет.

В 1905 г. Серпинский после забастовки учащейся молодежи, в которой он принимал участие, переезжает в Краков и поступает в Ягеллонский университет. Здесь ему была присвоена степень доктора.

В 1907 г. Серпинский получил свой первый результат по теории множеств. С этого момента начинается его исключительно плодотворная деятельность в области

теории множеств и ее приложений к топологии, теории функций действительного переменного и другим областям математики. Серпинский быстро приобретает известность. В 1908 г. он начал преподавать во Львовском университете и вскоре получил там профессуру. В 1911 г. Краковская Академия наук награждает Серпинского за работы, опубликованные им в 1909—1910 гг. на польском языке. Спустя два года эта же академия присуждает ему премию за «Очерк теории множеств», а в 1918 г. — за монографию «Теория чисел».

Во время первой мировой войны Серпинский был интернирован. Четыре года он провел в Москве и Вятке. Здесь он продолжал свою научную деятельность и имел полезные контакты с Н. Н. Лузиным и другими русскими математиками.

Весной 1917 г. Краковская Академия наук избрала Серпинского своим членом-корреспондентом.

С 1919 г. Серпинский — профессор Варшавского университета. Уже в следующем году он с профессорами С. Мазуркевичем и З. Янишевским основал в Варшаве журнал «Fundamenta Mathematicae», который сыграл большую роль в развитии современной математики. Этот журнал продолжает выходить и в настоящее время.

В 1921 г. Серпинский был избран действительным членом Польской Академии наук. Необычайная творческая активность, выдающиеся педагогические, литературные и организационные способности Серпинского ставят его во главе польской математической школы. Университеты различных стран и континентов присваивают ему звание почетного профессора, степень доктора honoris causa. Ряд академий и научных обществ избирают его своим членом-корреспондентом и почетным членом. Имя Серпинского приобретает огромную популярность. В обиход математиков входят термины: «Универсальная кривая Серпинского», «Треугольная кривая Серпинского», «Ковер Серпинского» и др.

В годы второй мировой войны Серпинский не прекращал научную работу и даже преподавал в подпольном университете. После освобождения Польши, с февраля 1945 г. Серпинский некоторое время работал в Ягеллонском университете в Кракове, а осенью 1945 г.

вернулся в Варшаву. И снова большой труд по восстановлению университета, снова, как и в предвоенные годы, лекции в различных университетах Европы, Индии, Канады, США.

В 1949 г. Серпинский был награжден в Польше первой Государственной премией за научную деятельность. В 1951 г. он был избран вице-президентом Польской Академии наук.

В апреле 1957 г. Серпинский принял участие в юбилейной научной сессии АН СССР, посвященной 250-летию со дня рождения Л. Эйлера. В том же году Серпинский возобновил издание международного журнала «Acta Arithmetica», посвященного вопросам теории чисел.

Список работ, опубликованных Серпинским, содержит свыше 600 названий. Среди них около 30 университетских учебников и монографий. Серпинский — член 11 иностранных академий и многих научных обществ. Более 20 его учеников являются в настоящее время профессорами в Польше и в других странах. Недавно степень доктора получил его ученик — молодой талантливый математик Андрей Шинцель, работы которого в области теории чисел уже приобрели широкую известность. Вацлав Серпинский — старейший академик Польши — по праву считается отцом польской школы математиков.

И. Г. Мельников

ОТ ПЕРЕВОДЧИКА

Настоящий перевод книги польского академика Вацлава Серпинского несколько отличается от оригинала, появившегося летом 1961 г. на польском языке. В последнее время наши познания о простых числах немного пополнились. В связи с этим в марте 1962 г. автор прислал мне ряд поправок и дополнений к книге. Все они учтены в настоящем издании.

Я весьма признателен редактору книги Н. М. Розенгауз, внесшей ряд улучшений в рукопись перевода.

И. Мельников

ПРЕДИСЛОВИЕ

Цель этой книги — сообщить в наиболее доступной форме о том, что мы знаем и чего не знаем о простых числах. С простыми числами мы встречаемся уже в элементарной арифметике, но они играют важную роль и в других разделах математики, главным образом в теории чисел и алгебре.

Математика считается, и справедливо, наукой дедуктивной. Тем не менее не следует умалять роль, которую сыграла в математике индукция, и притом не так называемая полная индукция, а индукция, основанная на наблюдении большого числа случаев и ведущая от них к предполагаемым общим теоремам. Особенно это относится к учению о простых числах, где именно таким путем было открыто много важных теорем, доказательства которых были найдены лишь позднее. Но этот путь часто приводил и к ошибочным предположениям. Известны также различные предположения, которые для многих частных случаев проверены, но о которых до сих пор неизвестно, истинны они или нет. Обо всем этом будет идти речь в данной книге.

Книга не является учебником по теории простых чисел; она имеет в основном информационный характер. В книге доказываются лишь некоторые теоремы, именно те, доказательства которых совершенно элементарны и не очень громоздки. Читателя, желающего познакомиться с доказательствами других теорем и углубить свои знания о простых числах, отсылаю ко второй части моей книги «Теория чисел» [1]), где указывается и дополнительная литература.

Варшава, март 1961 г. *Вацлав Серпинский*

---

[1]) См W. Sierpiński, Teoria liczb, II, Warszawa, 1959. (*Прим. перев.*)

1. Что такое простые числа?

К понятию простых чисел приводят уже самые простые задачи, которые возникают в связи с таким элементарным арифметическим действием, как умножение натуральных, т. е. целых положительных чисел.

Как известно, произведение двух натуральных чисел всегда является числом натуральным. Следовательно, существуют натуральные числа, представляющие собой произведения двух натуральных чисел, бóльших единицы. Но существуют также натуральные числа, бóльшие единицы, которые не являются произведениями двух натуральных чисел, бóльших единицы, например числа 2, 3, 5 или 13. Именно такие числа мы называем простыми.

Итак, *простым числом мы называем каждое натуральное число, бóльшее единицы, которое не является произведением двух натуральных чисел, бóльших единицы.*

Напрашивается вопрос, имеем ли мы возможность относительно каждого натурального числа $n > 1$ установить, простое оно или нет. Оказывается, само определение простых чисел позволяет ответить на этот вопрос.

Действительно, если натуральное число $n > 1$ не является простым, то оно представляет собой произведение двух натуральных чисел a и b, бóльших единицы, т. е. $n = ab$, где $a > 1$ и $b > 1$, откуда тотчас же следует, что $n > a$ и $n > b$. Натуральное число $n > 1$, не являющееся простым, есть, таким образом, произведение двух натуральных чисел, меньших n. Такое число мы называем составным. Если число n составное, то $n = ab$, где a и b — числа натуральные >1 и $<n$. Частное $n : a = b$ является натуральным числом,

следовательно, a есть делитель натурального числа n, больший 1 и меньший чем n. Поэтому, чтобы убедиться в том, что натуральное число $n > 1$ является простым, достаточно убедиться, что оно не имеет натурального делителя >1 и $<n$. Для этого достаточно выполнить $n-2$ делений числа n поочередно на числа 2, 3, ..., $n-1$. Если ни на одно из них число n не делится без остатка, то в этом и только в этом случае число n является простым.

Итак, по крайней мере теоретически, мы всегда сумеем (при помощи конечного числа делений) убедиться, является ли данное натуральное число n простым или нет. На практике описанный способ может порождать значительные трудности, когда n большое число. Так, до сих пор мы не можем, ввиду длинноты необходимых вычислений, применить этот способ к числу $2^{101}-1$, имеющему тридцать одну цифру (в десятичной системе счисления), хотя другим путем доказано, что это число является составным. Впрочем, до сих пор неизвестно ни одного разложения этого числа в произведение двух натуральных чисел, бо́льших единицы (хотя мы и знаем, что такое разложение существует). Также неизвестно, является ли число $2^{2^{17}}+1$ (имеющее 39 457 цифр) простым или нет.

2. Простые делители натуральных чисел

Докажем теперь несколько несложных теорем о простых числах.

Теорема 1. *Каждое натуральное число $n>1$ имеет по меньшей мере один простой делитель.*

Доказательство. Пусть n — натуральное число >1. Это число имеет делители, бо́льшие единицы, например само n. Среди делителей числа n, бо́льших единицы, существует наименьший. Обозначим его через p. Если бы число p не было простым, то, согласно определению простых чисел, p было бы произведением двух натуральных чисел, бо́льших единицы: $p=ab>a$. В этом случае a было бы делителем числа p, а значит, и числа n, бо́льшим единицы и притом меньшим p, что противоречит определению числа p. Теорема 1 доказана.

Теорема 2. *Каждое составное число n имеет по меньшей мере один простой делитель $\leqslant\sqrt{n}$.*

Доказательство. Если n есть составное число, то $n=ab$, где a и b — натуральные числа >1 и $<n$. Мы можем, очевидно, предположить, что $a\leqslant b$. Тогда $n=ab\geqslant a^2$, и, следовательно, $a\leqslant\sqrt{n}$. Но a есть число >1. Поэтому, согласно теореме 1, число a имеет простой делитель p, который, очевидно, $\leqslant a$ и, следовательно, $\leqslant\sqrt{n}$. Но p как делитель делителя a числа n является делителем и числа n. Таким образом, число n имеет простой делитель $p\leqslant\sqrt{n}$. Итак, теорема 2 доказана.

3. Сколько существует простых чисел?

Чтобы ответить на этот вопрос, мы докажем следующую теорему.

Теорема 3. *Если n — натуральное число >2, то между n и $n!$ содержится по меньшей мере одно простое число.*

Доказательство. Так как $n>2$, то целое число $N=n!-1$, очевидно, >1 и, согласно теореме 1, имеет простой делитель p, который $\leqslant N$, а следовательно, и $<n!$. Если допустить, что $p\leqslant n$, то p будет одним из сомножителей произведения $n!=1\cdot2\cdot3\ldots n$ и, значит, будет делителем числа $n!$. Но, будучи также делителем числа N, p будет делителем разности этих чисел, или числа $n!-N=1$, что невозможно. Таким образом, $p>n$, а так как уже выяснено, что $p<n!$, то имеем $n<p<n!$, и, значит, теорема 3 доказана.

Итак, для каждого натурального числа существует простое число, бóльшее его. Отсюда следует, что простых чисел бесконечно много, об этом знал уже Евклид. В частности, отсюда следует, что существует простое число, имеющее (в десятичной системе счисления) по крайней мере тысячу цифр. Однако ни одного такого числа еще в 1960 г. мы не знали. Наибольшее известное тогда простое число $2^{3217}-1$ имело 969 цифр. (Подробнее об этом числе будет сказано в § 25.)

Стоит подчеркнуть, что в течение последнего десятилетия здесь наблюдался значительный прогресс. К началу 1951 г. наибольшим известным простым числом было число $2^{127}-1$, имеющее 39 цифр (то, что это число простое, было доказано уже в 1876 г.). В настоящее же время наибольшим известным простым числом является число $2^{4423}-1$, имеющее 1332 цифры.

В связи с теоремой 3 заметим, что в 1850 г. П. Л. Чебышев доказал более сильную теорему (так называемый постулат Бертрана), согласно которой для натуральных $n>3$ между n и $2n-2$ содержится хотя бы одно простое число. Отсюда следует, что в теореме 3 число $n!$ можно заменить числом $2n$. В настоящее время имеется элементарное доказательство этой теоремы, но оно довольно длинное [1]). Можно также доказать, что для натуральных $n>5$ между n и $2n$ содержатся по меньшей мере два простых числа [2]).

Из теоремы Чебышева легко вывести, что для каждого натурального числа s существует по крайней мере три простых числа, имеющих по s цифр каждое. Действительно, каждое из чисел 10^{s-1}, $2\cdot 10^{s-1}$, $4\cdot 10^{s-1}$ и $8\cdot 10^{s-1}$ имеет s цифр, а в силу теоремы Чебышева для $s>1$ существуют простые числа p, q и r такие, что

$$10^{s-1}<p<2\cdot 10^{s-1}<q<4\cdot 10^{s-1}<r<8\cdot 10^{s-1},$$

и, следовательно, каждое из чисел p, q, r имеет по s цифр.

Для $s=1$ мы имеем четыре однозначных простых числа: 2, 3, 5 и 7. Двузначных простых чисел имеется 21, трехзначных — 143. Существуют хотя бы три простых числа, имеющие по сто цифр каждое. Недавно Р. М. Робинзон нашел такие числа: $81\cdot 2^{824}+1$, $63\times 2^{326}+1$, $35\cdot 2^{827}+1$.

До сих пор мы не знаем ни одного простого числа, имеющего тысячу цифр, хотя известно, что существуют по меньшей мере три таких числа.

---

[1]) См., например, W. Sierpiński, Arytmetyka teoretyczna, Wyd. 2, Warszawa, 1959, str. 88—94.

[2]) См. W. Sierpiński, Teoria liczb, II, Warszawa, 1959, str. 400.

4. Как можно найти все простые числа, меньшие данного числа?

Способ, о котором будет идти речь, известен был уже в древности: он носит название решета Эратосфена.

Предположим, что мы хотим найти все простые числа, не превосходящие некоторого натурального числа a. С этой целью выпишем все последовательные натуральные числа от 1 до a и будем вычеркивать из этой последовательности все числа, которые не являются простыми: прежде всего число 1, а затем для каждого натурального числа $n > 1$ все числа, большие чем n и делящиеся на n. Легко видеть, что таким путем каждое составное число окажется вычеркнутым и останутся только простые числа.

Итак, из последовательности 1, 2, 3, 4, ..., a мы вычеркием число 1, затем числа, большие чем 2 и делящиеся на 2, далее числа, большие чем 3 и делящиеся на 3. Чисел, делящихся на 4, вычеркивать нам уже не придется, так как они вычеркнуты как числа >2 и делящиеся на 2. Таким образом, далее мы будем вычеркивать числа, большие чем 5 и делящиеся на 5 и т. д. При этом мы можем уже не вычеркивать ни одно из чисел $> \sqrt{a}$. Действительно, если n — составное число $> \sqrt{a}$ и $\leqslant a$, то, согласно теореме 2, число n имеет простой делитель $p \leqslant \sqrt{n}$, следовательно, $\leqslant \sqrt{a}$, и число n окажется вычеркнутым как число, бо́льшее p и делящееся на p.

Так, например, желая получить все простые числа $\leqslant 100$, вычеркнем из последовательности 1, 2, 3, ..., 100 число 1, затем числа >2 и делящиеся на 2, далее числа >3 и делящиеся на 3, затем числа >5 и делящиеся на 5 и, наконец, числа >7 и делящиеся на 7. Все числа, оставшиеся в нашей последовательности, будут простыми. Таким путем мы получим следующую последовательность (в которой все простые числа выделены жирным шрифтом):

1, **2**, **3**, 4, **5**, 6, **7**, 8, 9, 10, **11**, 12, **13**, 14, 15, 16, **17**, 18, **19**, 20, 21, 22, **23**, 24, 25, 26, 27, 28, **29**, 30, **31**, 32, 33, 34, 35, 36, **37**, 38, 39, 40, **41**, 42, **43**, 44, 45, 46, **47**, 48, 49, 50, 51, 52, **53**, 54, 55, 56, 57, 58, **59**, 60, **61**, 62, 63, 64, 65, 66,

67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100.

Обозначим n-е по порядку простое число через p_n. Тогда $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, $p_{10} = 29$, $p_{25} = 97$. Легко можно подсчитать, что $p_{100} = 541$.

В 1909 г. были изданы таблицы простых чисел, меньших 10 миллионов [1]), в которых для каждого натурального числа $\leqslant 10\,170\,000$, не делящегося на 2, 3, 5 или 7, дается его наименьший простой делитель. В 1951 г. были опубликованы таблицы простых чисел до 11-го миллиона [2]).

Якуб Филипп Кулик (1793—1863 гг.) составил таблицы простых чисел, содержащихся в первых ста миллионах [3]). Эти таблицы после проверки были использованы при составлении таблиц простых чисел 11-го миллиона, изданных в 1951 г. Недавно (1959 г.) К. Л. Бейкер и Ф. Ю. Груибергер составили микрофильм, содержащий все простые числа $\leqslant p_{6\,000\,000} = 104\,395\,301$ [4]).

5. Простые числа близнецы

Относительно бесконечной последовательности последовательных простых чисел, т. е. последовательности

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, ...,

возникает ряд вопросов. Лишь на некоторые из них удается легко дать ответ.

Так, например, два наименьших простых числа 2 и 3 являются последовательными натуральными числами. Напрашивается вопрос, существуют ли другие последовательные натуральные числа, которые оба были бы

---

[1]) D. N. Lehmer, Factor table for the first ten millions, Washington, Carnegie Institution, 1909.

[2]) J. P. Kulik, L. Poletti, R. J. Porter, Liste des nombres premiers du onzième million (plus précisément de 10 006 741 à 10 999 997), Amsterdam, 1951.

[3]) Неопубликованная рукопись Я. Ф. Кулика хранится в Австрийской Академии наук в Вене.

[4]) The first six million prime numbers, The RAND Corporation, Santa Monica, published by the Microcard Foundation, Madison, Wisconsin, 1959.

простыми. Легко доказать, что таких чисел иет. В самом деле, из каждых двух последовательиых натуральных чисел одно является четным, и, зиачит, если оно >2, то оио составиое.

Однако существует много пар последовательных иечетиых чисел, которые оба являются простыми, иапример пары 3 и 5, 5 и 7, 11 и 13, 17 и 19, 29 и 31, 41 и 43. Такие пары мы называем парами чисел близнецов. До 30 миллионов имеется 152 892 таких пар.

Уже давно поставлен вопрос, существует ли бесконечно миого пар простых чисел близнецов. На этот вопрос мы не знаем ответа. Итак, мы не знаем, представимо ли число 2 бескоиечным числом способов в виде разности двух простых чисел.

Высказано предположение, что каждое четиое число можио бесконечным числом способов представить в виде разности двух последовательных простых чисел. Однако мы ие можем доказать даже того, что каждое четное число представимо в таком виде хотя бы одним способом, что проверено для многих последовательиых четиых чисел, например, $2 = 5 - 3$, $4 = 11 - 7$, $6 = 29 - 23$, $8 = 97 - 89$, $10 = 149 - 139$, $12 = 211 - 199$, $14 = 127 - 113$, $16 = 1847 - 1831$, $18 = 541 - 523$, $20 = 907 - 887$. Более того, мы не можем доказать даже того, что каждое четное число представляет собой разность двух простых чисел (хотя бы и иепоследовательных).

Но мы можем найти все нечетные числа, представляющие собой разность двух простых чисел. Действительно, если иатуральное нечетное число n является разиостью двух простых чисел, $n = p - q$, то одио из этих простых чисел должио быть четным, а другое нечетным, следовательно, одно из чисел p и q, и как легко видеть, имеиио число q, должно быть равно 2. Таким образом, имеем $n = p - 2$, где p — простое нечетное число. Итак, все иатуральные нечетные числа, которые являются разиостью двух простых чисел, меиьше простых нечетных чисел на 2, следовательио, это числа 1, 3, 5, 9, 11, ... Таких чисел бескоиечно миого.

Однако существует бескоиечио много и таких нечетиых чисел, которые не являются разностью двух простых чисел, иапример все числа вида $6k + 1$, где k — натуральиое число. В самом деле, равенство

$6k + 1 = p - 2$, где p — простое число, невозможно, так как из него следует, что $p = 6k + 3 = 3(2k + 1)$, т. е. что p есть составное число.

6. Гипотеза Гольдбаха

В 1742 г. Хр. Гольдбах высказал предположение, что каждое четное число >2 является суммой двух простых чисел. Это предположение до сих пор не доказано и не опровергнуто. Оно проверено для всех четных чисел вплоть до 100 000. Была высказана и более сильная гипотеза, а именно, что каждое четное число >6 является суммой двух различных простых чисел. Эту гипотезу С. Голашевский проверил для всех чисел $\leqslant 50\,000$.

Можно доказать, что последняя гипотеза равносильна утверждению, что каждое натуральное число >17 является суммой трех различных простых чисел. А. Шинцель доказал, что из гипотезы Гольдбаха следует, что каждое нечетное число >17 является суммой трех различных простых чисел.

Из гипотезы Гольдбаха следует также, что нечетное число >7 является суммой трех простых нечетных чисел. Действительно, если n есть натуральное число и $2n + 1 > 7$, то $2n + 1 - 3 = 2(n - 1) > 4$. Согласно гипотезе Гольдбаха, четное число $2(n - 1) > 4$ есть сумма двух простых чисел $p + q$, причем p и q не могут быть четными, так как наше число >4. Таким образом, числа p и q являются нечетными, и, значит, число $2n + 1 = 3 + p + q$ есть сумма трех простых нечетных чисел.

Мы не знаем, является ли каждое нечетное число >7 суммой трех простых нечетных чисел, однако для достаточно больших нечетных чисел это было доказаио И. М. Виноградовым в 1937 г. Мы даже знаем такое число a $(a = 3^{3^{16}})$, что каждое нечетное число $>a$ является суммой трех простых нечетных чисел.

Таким образом, решению вопроса, является ли каждое нечетное число >7 суммой трех простых нечетных чисел, препятствует лишь громоздкость необходимых для этого вычислений, так как здесь достаточно исследовать только нечетные числа >7 и $\leqslant a$, а для ка-

ждого данного нечетного числа можно при помощи конечного числа простых арифметических действий решить, является оно суммой трех простых нечетных чисел или нет.

Иначе обстоит дело с гипотезой Гольдбаха: здесь мы не можем сказать, что решению вопроса, верна или нет эта гипотеза, мешает только громоздкость необходимых вычислений.

Доказано, что каждое натуральное число >1 есть сумма двадцати или менее простых чисел.

Доказано, что каждое натуральное число >11 есть сумма двух или более различных простых чисел. Например, $12 = 5 + 7$, $13 = 2 + 11$, $17 = 2 + 3 + 5 + 7$, $29 = 3 + 7 + 19$. А. Монковский же доказал, что каждое натуральное число >55 есть сумма различных простых чисел вида $4k + 3$, и доказал три аналогичных теоремы о суммах простых чисел каждого из видов $4k + 1$, $6k + 1$ и $6k + 5$.

Из гипотезы Гольдбаха следует, что каждое целое нечетное число (положительное или отрицательное) может быть бесконечным числом способов представлено в виде $p + q - r$, где p, q, r — простые нечетные числа.

Действительно, для каждого целого числа k существует простое нечетное число r такое, что $2k - 1 + r > 4$ (в качестве r можно взять любое достаточно большое простое число). Но тогда $2k - 1 + r$ есть четное число >4 и, следовательно, согласно гипотезе Гольдбаха, $2k - 1 + r = p + q$, где p и q — простые нечетные числа. Таким образом, $2k - 1 = p + q - r$, причем простое число r может быть произвольно большим. Отсюда вытекает предложение, сформулированное выше.

Интересно отметить, что последнее предложение было доказано Дж. Г. ван дер Корпутом в 1923 г. Однако его доказательство весьма сложно [1]).

В связи с гипотезой Гольдбаха заметим, что каждое натуральное число >11 есть сумма двух составных чисел. Действительно, если $n > 11$ является числом четным, то $n - 4$ есть четное число >2, следовательно, число составное, и, значит, n есть сумма двух составных чисел: 4 и $n - 4$. Если же $n > 11$ является числом нечетным, то $n - 9$ есть четное число >2 и, следова-

[1]) См. J. G. van der Corput. Acta Mathematica, 44, 50.

тельно, составное, и, значит, n есть сумма двух составных чисел: 9 и $n-9$. Отсюда, однако, нельзя сделать вывод, что исследование составных чисел легче, чем исследование простых чисел. Так, мы не можем, например, дать ответ на вопрос, существует ли среди чисел $F_n = 2^{2^n}+1$, где $n=1, 2, 3, \ldots$, бесконечно много составных (до сих пор мы знаем только 37 таких составных чисел, среди которых наибольшим является F_{1945}).

Г. Г. Гарди и Дж. Е. Литтлвуд высказали предположение (до сих пор не доказанное), что каждое достаточно большое натуральное число, не являющееся квадратом, есть сумма квадрата целого числа и простого числа. Легко доказать, что существует бесконечно много квадратов натуральных чисел, которые являются, а также таких, которые не являются суммой квадрата целого числа и простого числа.

Действительно, с одной стороны, если p есть простое нечетное число, то $\frac{p+1}{2}$ является натуральным числом, и мы имеем

$$\left(\frac{p+1}{2}\right)^2 = \left(\frac{p-1}{2}\right)^2 + p;$$

с другой же стороны, если $n = 3k+2$, где k — натуральное число, то равенство

$$n^2 = x^2 + p$$

при целом неотрицательном x и простом p невозможно, так как из него следовало бы, что $n > x$ и

$$p = n^2 - x^2 = (n-x)(n+x),$$

откуда, принимая во внимание, что p есть простое число, $n-x=1$ и $n+x=p$ и, значит,

$$p = 2n-1 = 3(2k+1),$$

что при натуральном k исключено.

Другая теорема Гарди — Литтлвуда, согласно которой каждое достаточно большое натуральное число есть сумма двух квадратов целых чисел и простого числа, была доказана в 1959 г. Ю. В. Линником.

7. Гипотеза Гильбрайта

Н. Л. Гильбрайт высказал в 1958 г. следующее предположение.

Если мы выпишем последовательные простые числа, затем в первой строке — разности последовательных простых чисел, во второй — абсолютные величины разностей последовательных чисел первой строки, в третьей — абсолютные величины разностей последовательных чисел второй строки и т. д., то в каждой строке первым числом будет 1.

Так, напрнмер, первые 17 строк (следующих за последовательностью простых чисел) выглядят следующим образом:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61

1 2 2 4 2 4 2 4 6 2 6 4 2 4 6 6 2

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

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

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

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

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

1 2 0 2 0 2 0 2 0 0 0

1 2 2 2 2 2 2 2 0 0

1 0 0 0 0 0 0 2 0

1 0 0 0 0 0 2 2

1 0 0 0 0 2 0

1 0 0 2 2

1 0 2 0

1 2

1

Гипотеза Гильбрайта проверена для первых 63 418 строк. Однако мы не знаем общего доказательства ее истинности.

Обозначим для натуральных n через a_n наименьшее натуральное число такое, что $(a_n + 1)$-е число n-й строки является первым числом этой строки, которое >2. Таким образом, мы имеем, например, $a_1 = 3$, $a_2 = 8$, $a_3 = 14$. Подсчитано, что $a_4 = 14$, $a_5 = 25$, $a_6 = 24$, $a_7 = 23$, $a_8 = 22$, $a_9 = 25$, $a_{10} = 59$, $a_{14} = 97$, $a_{15} = 174$, $a_{22} = 280$, $a_{23} = 740$, $a_{24} = 874$, $a_{34} = 866$, $a_{35} = 2180$, $a_{64} = 5940$, $a_{65} = 23\,266$, $a_{94} = 31\,533$.

Если бы можно было доказать, что $a_n > 2$ для натуральных n, то отсюда легко можно было бы установить истинность гипотезы Гильбрайта.

8. Разложение натурального числа на простые сомножители

Опираясь на теорему 1, докажем следующую теорему.

Теорема 4. *Любое натуральное число > 1 является произведением, каждый сомножитель которого есть простое число.*

Доказательство. Пусть n — данное натуральное число >1. Согласно теореме 1, число n имеет (по крайней мере один) простой делитель p', и мы можем предположить, что p' есть наименьший простой делитель числа n. Итак, имеем $n = p'n'$, где n' — натуральное число.

Если $n' = 1$, то $n = p'$ и n является произведением, составленным только из одного простого сомножителя. Если же $n' > 1$, то n' имеет простой делитель p'', о котором мы можем предположить, что он есть наименьший простой делитель числа n'. Одновременно он является простым делителем числа n, причем из определения числа p' следует, что $p' \leqslant p''$.

Таким образом, $n' = p''n''$, и либо $n'' = 1$, и тогда n есть произведение двух простых чисел p' и p'' (не обязательно разных), либо $n'' > 1$, и тогда с числом n'' мы можем поступить, как ранее с числами n и n' и т. д. Так как $n = p'n'$ и $p' > 1$, то имеем $n' < n$. Аналогично найдем, что $n'' < n'$ и т. д. Поэтому натуральные числа n, n', n'', ... образуют убывающую последовательность, которая не может содержать более чем n членов. Следовательно, при некотором натуральном k число $n^{(k)}$

будет последним членом этой последовательности. Но в таком случае $n^{(k)} = 1$, ибо в случае $n^{(k)} > 1$ мы могли бы положить

$$n^{(k)} = p^{(k+1)} n^{(k+1)}$$

и получили бы дальнейший член $n^{(k+1)}$ нашей последовательности. Итак, имеем $n = p'n'$, $n' = p''n''$, ..., $n^{(k-1)} = p^{(k)} n^{(k)}$ и $n^{(k)} = 1$, откуда найдем

$$n = p'p''p''' \ldots p^{(k)}, \qquad (1)$$

где p', p'', ..., $p^{(k)}$ — простые числа, причем можно предполагать, что $p' \leqslant p'' \leqslant p''' \leqslant \ldots \leqslant p^{(k)}$ (если для каждого из чисел n, n', ... мы будем определять его наименьший простой делитель).

Среди сомножителей произведения (1) могут быть равные. Формулу (1) можно записать в виде:

$$n = q_1^{a_1} q_2^{a_2} \ldots q_s^{a_s}, \qquad (2)$$

где s — натуральное число, q_1, q_2, ..., q_s — различные простые числа, расположенные в порядке возрастания, a_1, a_2, ..., a_s — натуральные показатели степени.

Формула (2) называется каноническим разложением числа n на простые сомножители.

Итак, мы не только доказали теорему 4, но и указали способ нахождения для каждого натурального числа $n > 1$ его канонического разложения на простые сомножители. Таким образом, нахождение этого разложения для любого данного натурального числа $n > 1$ теоретически всегда возможно. Однако на практике оно может потребовать проведения утомительных вычислений, которые для некоторых чисел оказываются столь длинными, что в настоящее время их невозможно осуществить даже при помощи самых лучших вычислительных машин. Например, мы не знаем разложения на простые сомножители числа $2^{101} - 1$ (имеющего 31 цифру); доказано только, что оно является произведением двух различных простых сомножителей, меньший из которых (впрочем, до сих пор неизвестный) имеет не менее 11 цифр. Мы не знаем также разложения на простые сомножители числа $F_{17} = 2^{2^{17}} + 1$, о котором неизвестно даже, является ли оно простым или нет. Зато для числа $F_{1945} = 2^{2^{1946}} + 1$, имеющего более

чем 10^{582} цифр (ибо $2^{1945} = 32 \cdot 2^{1940} = 32 \cdot (2^{10})^{194} > 30 \cdot (10^3)^{194} = 3 \cdot 10^{583}$, откуда $F_{1945} > 2^{3 \cdot 10^{582}} = (2^{10})^{3 \cdot 10^{582}} > 10^{9 \cdot 10^{582}}$), несколько лет назад был найден наименьший простой делитель. Этим делителем является число $5 \cdot 2^{1947} + 1$, имеющее 587 цифр. Но мы не знаем разложения числа F_{1945} на простые сомножители и даже не знаем других простых делителей этого числа (см. § 22).

Напрашивается вопрос, является ли разложение (2) числа $n > 1$ на простые сомножители единственным (если числа $q_1, q_2, \ldots, q_s$ составляют возрастающую последовательность). Доказательство однозначности разложения опирается на несколько несложных теорем о простых числах.

Теорема 5. *Простое число p имеет только два натуральных делителя 1 и p.*

Доказательство. Если бы число p, кроме делителей 1 и p, имело еще делитель a, то, очевидно, было бы $1 < a < p$ и $p = ab$, где b — натуральное число > 1, ибо если $b = 1$, то $p = a$, что противоречит предположению относительно a. Таким образом, число p было бы произведением двух натуральных чисел, больших единицы, а это противоречит предположению о том, что p есть простое число. Итак, теорема 5 доказана.

Как легко видеть, справедлива также теорема, согласно которой натуральное число p, имеющее точно два натуральных делителя, является простым. Действительно, в этом случае должно быть $p > 1$. Далее, если бы p не было простым числом, то p являлось бы произведением двух натуральных чисел a и b, больших единицы. Но из того, что $p = ab$ и $b > 1$, следовало бы, что $1 < a < p$, т. е. a было бы делителем числа p, отличным от 1 и p, и, значит, число p имело бы по меньшей мере три различных натуральных делителя.

Таким образом, имеет место

Теорема 6. *Для того чтобы натуральное число было простым, необходимо и достаточно, чтобы оно имело точно два натуральных делителя (очевидно, единицу и самого себя).*

Докажем теперь следующую теорему.

Теорема 7. *Если a и b — натуральные числа и произведение ab делится на простое число p, то по крайней мере одно из чисел a и b делится на p.*

Доказательство. Если бы теорема 7 не была справедлива, то существовало бы наименьшее простое число p, для которого она не верна. Для такого простого числа p существовало бы наименьшее произведение ab двух натуральных чисел a и b, делящееся на p, несмотря на то, что ни один из сомножителей a и b не делится на p. Покажем, что тогда числа a и b были бы меньше, чем p. В самом деле, если, например, оказалось бы, что $a > p$, то мы имели бы равенство $a = kp + a_1$, где $a_1 < p$ и $a_1 > 0$, ибо a не делится на p. Отсюда $ab = (kp + a_1)b = kpb + a_1b$, и так как числа ab и kpb делятся на p, то и a_1b делится на p. Но $a_1 < p < a$ и a_1 не делится на p, причем $a_1b < ab$, что противоречит предположению относительно произведения ab. Итак, доказано, что $a < p$. Подобным же образом мы докажем, что $b < p$ и, значит, $ab < p^2$.

Далее, поскольку ab делится на p, имеем $ab = lp$, где l — натуральное число, большее 1, так как иначе было бы $p = ab$, где $a > 1$ и $b > 1$ (ибо числа a и b не делятся на p).

С другой стороны, на основании неравенства $ab < p^2$ получаем $l < p$. Число l, будучи натуральным числом > 1, имеет простой делитель $q \leqslant l < p$. Учитывая теперь определение числа p, а также то, что произведение ab, делящееся на l, делится также на простое число $q < p$, мы заключим, что хотя бы один из сомножителей a и b должен делиться на q. Если, например, a делится на q, то $a = a'q$. Но l делится на q, следовательно, $l = tq$, где t — натуральное число. А так как $ab = lp$, то $a'qb = tqp$, откуда $a'b = tp$, причем, учитывая, что $a = a'q$, имеем $a' < a$, откуда $a'b < ab$, что противоречит предположению относительно произведения ab. Итак, предположение о том, что теорема 7 неверна, приводит к противоречию.

Из доказанной теоремы при помощи индукции можно получить следующее

Следствие. Если $a_1, a_2, \ldots, a_m$ — натуральные *числа, произведение которых делится на простое число* p, *то по крайней мере одно из чисел* $a_1, a_2, \ldots, a_m$ *должно делиться на* p.

Доказательство. Это следствие справедливо для $m = 2$. Предположим, что оно справедливо для m чисел, и пусть числа $a_1, a_2, \ldots, a_m, a_{m+1}$ являются

натуральными. Если произведение $a_1a_2 \dots a_ma_{m+1}$ делится на простое число p, то, согласно теореме 7, по крайней мере одно из двух чисел $a_1a_2 \dots a_m$ и a_{m+1} делится на p. Если число $a_1a_2 \dots a_m$ делится на p, то в силу предположения, что следствие справедливо для m чисел, заключаем, что хотя бы одно из чисел $a_1, a_2, \dots, a_m$ делится на p. Итак, из справедливости следствия для m чисел следует его справедливость для $m+1$ чисел.

Предположим теперь, что существуют натуральные числа, имеющие два различных канонических разложения на простые сомножители. Среди таких натуральных чисел существует, очевидно, наименьшее. Пусть это будет число n, которое кроме канонического разложения

$$n = q_1^{a_1}q_2^{a_2} \dots q_s^{a_s} \tag{2}$$

обладает разложением

$$n = r_1^{b_1}r_2^{b_2} \dots r_t^{b_t}, \tag{3}$$

где $r_1, r_2, \dots, r_t$ — возрастающая последовательность простых чисел, а $b_1, b_2, \dots, b_t$ — числа натуральные. Согласно (2), число n делится на q_1, и поэтому, в силу (3) и следствия теоремы 7, по крайней мере одно из чисел $r_1, r_2, \dots, r_t$ должно делиться на q_1. Очевидно, это будет число r_1, так как q_1 — наименьший простой делитель числа (3). Но, согласно теореме 5, простое число r_1 имеет только два натуральных делителя: 1 и r_1, поскольку же простое число q_1 также является делителем числа r_1, то должно быть $r_1 = q_1$. Заменив в формуле (3) r_1 на q_1, мы, ввиду (2), получим для числа n', где $n = q_1n'$, следующее равенство:

$$n' = q_1^{a_1-1}q_2^{a_2} \dots q_s^{a_s} = q_1^{b_1-1}r_2^{b_2} \dots r_t^{b_t}.$$

Так как число n' меньше чем n, то, в соответствии с предположением относительно числа n, число n' имеет только одно каноническое разложение на простые сомножители, откуда уже легко следует, что должно быть $s = t$, $r_2 = q_2$, $r_3 = q_3, \dots, r_s = q_s$, $a_1 = b_1$, $a_2 = b_2, \dots, a_s = b_s$. Таким образом, вопреки предположению, разложения (2) и (3) оказались идентичными. Следовательно, предположение, что существуют натуральные числа, имеющие два различных канонических разложения на простые сомножители, приводит к противоречию.

Итак, доказана

Теорема 8. *Каждое натуральное число $n > 1$ дает только одно разложение на простые сомножители, если не обращать внимания на порядок сомножителей.*

9. Какими цифрами могут начинаться и заканчиваться простые числа?

Последняя цифра простого числа, имеющего более чем одну цифру, не может быть четной, так как тогда число было бы >2 и четным и, следовательно, было бы составным; последняя цифра не может быть и 5, так как в этом случае число было бы >5 и делилось бы на 5 и, значит, было бы составным. Таким образом, последней цифрой простого числа >10 может быть только 1, 3, 7 или 9.

Ничего больше о цифрах простых чисел, превосходящих 10, в частности о комплексах нескольких последних или нескольких первых цифр простых чисел, сообщить нельзя, так как имеет место следующая теорема:

Если имеются две произвольные конечные последовательности цифр (в десятичной системе счисления) $a_1, a_2, \ldots, a_m$ *и* $b_1, b_2, \ldots, b_n$, где $b_n = 1, 3, 7$ *или* 9, *то существует достаточно большое простое число p, у которого первыми m цифрами будут последовательно* $a_1, a_2, \ldots, a_m$, *а n последними цифрами будут последовательно* $b_1, b_2, \ldots, b_n$ [1]).

Из этой теоремы, в частности, следует, что существуют простые числа, имеющие в начале и в конце достаточно большое число цифр, равных 1 (в средней части числа могут быть цифры, отличные от 1). Но существует ли бесконечное множество простых чисел, все цифры которых являются единицами, мы не знаем. Мы знаем лишь несколько простых чисел, все цифры которых суть единицы, например, 11 и $11\,111\,111\,111\,111\,111\,111\,111 = \frac{10^{23}-1}{9}$. Доказательство простоты последнего числа (предложенное М. Крайчиком)

---

[1]) Доказательство этой теоремы см. W. Sierpiński, Sur les nombres premiers ayant des chiffres initiaux et finals donnés, Acta Arithmetica, 5, 1959, 265—266.

сложно. Зато легко доказать, что если число, все цифры которого суть единицы, простое, то число его цифр также должно быть простым. Это условие, однако, не является достаточным, так как, например,

$$111 = 3 \cdot 37, \quad 11\,111 = 41 \cdot 271, \quad 1\,111\,111 = 239 \cdot 4649.$$

Число $\frac{10^{37}-1}{9}$, имеющее 37 цифр, также составное.

Найдены простые числа, составленные не только из одних цифр 1, которые остаются простыми при каждой перестановке их цифр. Среди двузначных таковыми являются числа: 13 и 31, 17 и 71, 37 и 73, 79 и 97, среди трехзначных — числа: 113, 131, 311; 199, 919, 991; 337, 373, 733. Мы не знаем других таких чисел и не знаем, конечно ли их число. Х. Е. Рихерт доказал, что для $3 < n < 6 \cdot 10^{175}$ нет таких чисел, имеющих n цифр, кроме простых чисел, все цифры которых суть единицы.

Л. Мозер нашел все простые числа <100000, не меняющие своего значения, если их цифры выписать в обратном порядке. Их оказалось 102. Вот все такие числа <1000: 101, 131, 151, 181, 313, 353, 373, 383, 727, 757, 787, 797, 919, 929. Неизвестно, существует ли бесконечно много таких простых чисел.

Мы не знаем, существует ли бесконечное множество простых чисел, первая и последняя цифры которых суть единицы, а остальные — нули, как, например, число 101. Легко доказать, что такие простые числа должны быть вида $10^{2^n} + 1$, где n — натуральное число, однако это условие не является достаточным, так как, например, $10^{2^2} + 1 = 73 \cdot 137$.

Нам известно много простых чисел, среди цифр которых нет ни одного нуля, но мы не знаем, конечно или нет множество таких чисел. Можно доказать, что для всякого натурального числа m существуют простые числа, среди цифр которых имеется более чем m нулей. Мы не знаем, существует ли для всякого натурального числа m такое число a, что сумма всех цифр всякого простого числа p, большего a, будет больше чем m.

10. Число простых чисел, не превосходящих данное число

Для данного числа x обозначим через $\pi(x)$ число простых чисел, не превосходящих x. Например, мы имеем: $\pi(1) = 0$, $\pi(2) = 1$, $\pi(3) = 2$, $\pi(4) = 2$, $\pi(5) = 3$,

$\pi(10) = 4$, $\pi(100) = 25$, $\pi(1000) = 168$, $\pi(10000) = 1229$, $\pi(10^6) = 5\,761\,455$, $\pi(10^9) = 50\,847\,534$, $\pi(10^{10}) = 455\,052\,512$.

Л. Лохер-Эрнст заметил, что для $n > 50$ выражение

$$f(n) = \frac{n}{\frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \ldots + \frac{1}{n}}$$

дает достаточно хорошее приближенное значение числа $\pi(n)$. Например, $\pi(10^3) = 168$, а $f(10^3) = 167{,}1$. Для $n = 10^6$ отношение $\pi(n) : f(n)$ равно 1,007, а для $n = 10^{10}$ оно составляет 1,005.

Можно доказать элементарно (хотя доказательство будет длинным и сложным), что отношение $\pi(n) : f(n)$ стремится к единице, когда n возрастает неограниченно.

При больших n вычисление выражения $f(n)$ представляет значительные трудности. Однако известны другие приближенные выражения для $\pi(n)$, например выражение $\frac{n}{\ln n}$ (где $\ln n$ обозначает натуральный логарифм числа n). Ж. Адамар и Ш. де ла Валле-Пуссен в 1896 г. доказали, что отношение $\pi(n)$ к $\frac{n}{\ln n}$ стремится к единице, когда n неограниченно возрастает. Отсюда следует, что отношение n-го простого числа p_n к $n \ln n$ стремится к единице, когда n неограниченно возрастает[1]). Можно доказать, что миллиардное простое число (т. е. число p_{10^9}) имеет 11 цифр.

Легко доказать, что для натуральных $n > 1$ имеет место неравенство $\frac{\pi(n-1)}{n-1} < \frac{\pi(n)}{n}$, если n есть простое число, и неравенство $\frac{\pi(n-1)}{n-1} > \frac{\pi(n)}{n}$, если n — число составное. Можно доказать, что отношение $\pi(n)$ к n стремится к нулю, когда n неограниченно возрастает. Вполне очевидно, что $\pi(p_n) = n$ для натуральных n.

Легко доказать, что существуют сколь угодно длинные последовательности, составленные из последовательных натуральных чисел, которые не содержат ни одного простого числа. Примером последовательности,

---

[1]) См. W. Sierpiński, Teoria liczb, II, Warszawa, 1959, str. 415.

состоящей из m таких чисел, может служить последовательность

$$(m+1)!+2,\ (m+1)!+3,\ (m+1)!+4,\ \ldots,$$
$$\ldots,\ (m+1)!+(m+1),$$

ибо первое из чисел этой последовательности делится на 2, второе на 3 и т. д., последнее на $m+1$ и, таким образом, все они являются числами составными.

Для $m=100$ это были бы огромные числа, однако уже между простыми числами 370 261 и 370 373 лежат 111 последовательных составных чисел. Среди ста последовательных чисел от 1 671 800 до 1 671 900 нет ни одного простого числа

Труднее было бы доказать, что существует простое число, которое с обеих сторон окружено произвольно большим числом составных чисел, т. е. что для каждого натурального числа m существует простое число p такое, что каждое из чисел $p-k$ и $p+k$, где $k=1, 2, \ldots, m$, является составным.

Также трудным является доказательство теоремы Э. Ландау о том, что для достаточно больших натуральных чисел n мы имеем $\pi(2n)<2\pi(n)$, или, иначе говоря, что для таких n простых чисел $\leqslant n$ больше, чем простых чисел, лежащих между n и $2n$.

Мы не знаем, для всех ли натуральных $x>1$ и $y>1$ выполняется неравенство $\pi(x+y)\leqslant\pi(x)+\pi(y)$.

11. Некоторые свойства n-го по порядку простого числа

Согласно теореме Х. Ж. Шерка, доказанной им в 1830 г., для натуральных n при соответствующем выборе знаков + или — имеем следующие формулы:

$$p_{2n}=1\pm p_1\pm p_2\pm\ldots\pm p_{2n-2}+p_{2n-1},$$
$$p_{2n+1}=1\pm p_1\pm p_2\pm\ldots\pm p_{2n-1}+2p_{2n}.$$

Так, например,

$$p_6=1+p_1-p_2-p_3+p_4+p_5,$$
$$p_7=1+p_1-p_2-p_3+p_4-p_5+2p_6,$$

или $13=1+2-3-5+7+11$, $17=1+2-3-5+7-11+2\cdot 13$.

Можно также доказать, что для натуральных n при соответствующем выборе знаков $+$ или $-$ имеем

$$p_{2n+1} = \pm p_1 \pm p_2 \pm \ldots \pm p_{2n-1} + p_{2n}.$$

Например, $p_7 = p_1 + p_2 - p_3 - p_4 + p_5 + p_6$, или $17 = 2 + 3 - 5 - 7 + 11 + 13$.

А. Шинцель доказал, что если a и b — положительные числа, причем $a < b$, то существуют простые числа p и q такие, что $a < \frac{p}{q} < b$.

Можно доказать, что для каждого вещественного положительного x последовательность с общим членом $\frac{p_{\pi(nx)}}{n}$ стремится к x, когда n неограниченно возрастает.

Доказано, что существует бесконечное множество простых чисел p таких, что последующее простое число ближе к числу p, чем простое число, предшествующее ему, а также таких, что предшествующее простое число ближе к числу p, чем простое число, следующее после p. Иными словами, доказано, что существует бесконечное множество натуральных чисел n таких, что $p_{n+1} - p_n < p_n - p_{n-1}$, т. е. $p_n > \frac{p_{n-1} + p_{n+1}}{2}$, а также, что существует бесконечно много натуральных чисел n таких, что $p_n < \frac{p_{n-1} + p_{n+1}}{2}$.

Но мы не знаем, существует ли бесконечное множество таких n, для которых $p_n = \frac{p_{n-1} + p_{n+1}}{2}$. Высказано предположение, что ответ на этот вопрос должен быть положительным. Так, например, мы имеем

$$p_n = \frac{p_{n-1} + p_{n+1}}{2} \text{ для } n = 16,\ 37,\ 40,\ 47,\ 55,\ 56,\ 240,\ 273.$$

П. Эрдеш и П. Туран доказали, что существует бесконечно много натуральных чисел n таких, что $p_n^2 > p_{n-1}p_{n+1}$, и бесконечно много n таких, что $p_n^2 < p_{n-1}p_{n+1}$.

Доказано, кроме того, что $p_{n+1} < p_{n-1} + p_n$ для $n = 3,\ 4,\ 5,\ \ldots$

Для последовательных простых чисел имеет место также следующая теорема (доказательство которой хотя и не трудное, но довольно длинное):

Для каждого натурального m существует натуральное число n такое, что

$$\frac{1}{p_1}+\frac{1}{p_2}+\ldots+\frac{1}{p_n}>m.$$

(Уже для $m=10n$ составляло бы несколько десятков тысяч.)

Можно указать четыре последовательных простых числа, дающих две пары чисел близнецов, например 11, 13, 17, 19 или 179, 181, 191, 193. Если такой комплекс составлен из простых чисел p, $p+2$, $p+6$ и $p+8$, то мы говорим, что имеется четверка. В первом из указанных здесь примеров мы имеем четверку, а во втором нет. Другие примеры четверок мы получаем для $p=5$, 101, 191, 821, 1481, 3251. Высказано предположение, что четверок существует бесконечно много.

В первых десяти миллионах, как подсчитал В. А. Голубев в 1959 г., имеется 899 четверок, в первых же пятнадцати миллионах — 1209. Самая далекая четверка, известная в настоящее время, была указана А. Ферье. Она получается при $p=2\,863\,308\,731$.

12. Многочлены и простые числа

Напрашивается вопрос, существует ли многочлен $f(x)$ от переменной x с целыми коэффициентами, который для каждого натурального значения x дает простое число $f(x)$. Докажем, что такого многочлена нет. Пусть

$$f(x)=a_0x^m+a_1x^{m-1}+\ldots+a_{m-1}x+a_m$$

есть многочлен степени m с целыми коэффициентами a_0, a_1, ..., a_m, где $a_0\neq 0$. Если бы мы взяли $a_0<0$, то для достаточно больших x было бы $f(x)<0$, поэтому будем предполагать, что $a_0>0$. Тогда, как известно, существует такое целое число x_0, что $n=f(x_0)>1$ и $f(x)>f(x_0)$ для $x>x_0$.

Докажем, что при любом натуральном k число $f(x_0+kn)$ будет составным. Пусть x и h — натуральные числа, тогда при всяком натуральном i число $(x+h)^i-x^i$ делится на $(x+h)-x=h$, откуда следует, что числа, $a_i(x+h)^{m-i}-a_ix^{m-i}$ для $i=0, 1, 2, \ldots, m$ делятся на h и, значит, число $f(x+h)-f(x)$ также делится на h. Но в таком случае $f(x_0+kn)-f(x_0)$,

делится на kn, или $f(x_0+kn)-n=tn$, что дает $f(x_0+kn)=(t+1)n$ и доказывает, что число $f(x_0+kn)$, которое, как мы знаем, $>f(x_0)=n$, делится на натуральное число $n>1$ и, следовательно, является составным, что и требовалось доказать.

Итак, мы доказали, что если $f(x)$ есть многочлен с целыми коэффициентами, где коэффициент при высшей степени x — число положительное, то для бесконечного множества натуральных чисел x число $f(x)$ является составным.

Однако мы знаем такие многочлены, которые для многих последовательных натуральных чисел x принимают значения, являющиеся простыми числами. Примером такого многочлена может служить многочлен Эйлера x^2+x+41, который для $x=0, 1, 2, \ldots, 39$ дает разные простые числа. Высказано предположение, что существует бесконечно много натуральных чисел x, для которых x^2+x+41 есть простое число.

Мы не знаем, существует ли такое натуральное число $a>41$, чтобы каждое из чисел x^2+x+a для $x=0, 1, 2, \ldots, a-2$ было простым. Во всяком случае таких чисел $a\leqslant 10^9$ не существует.

Многочлен $x^2-79x+1601$ дает простые числа для $x=0, 1, 2, \ldots, 79$, однако эти числа не все разные.

Возникает вопрос, существуют ли многочлены, которые для натуральных значений переменной дают бесконечное множество простых чисел. Очевидно, существуют такие многочлены первой степени, например многочлен $2x+1$, но мы не знаем ни одного такого многочлена степени >1. Мы не знаем, является ли таким двучлен x^2+1, дающий простые числа для $x=1, 2, 4, 6, 10$. Подсчитано, что для $x\leqslant 10\,000$ есть 842 простых числа вида x^2+1 (где x — натуральное число); для $x\leqslant 100\,000$ есть 6656 таких чисел, для $x\leqslant 180\,000$ их 11 223. Высказано предположение, что для каждого натурального числа k существует бесконечно много простых чисел вида x^2+k, где x есть натуральное число.

Существует, очевидно, только одно простое число вида x^3+1, где x — натуральное число, однако высказано предположение, что существует бесконечно много простых чисел вида x^3+2, а также вида x^3-2, где x — натуральное число (простые числа получаем при $x=1, 3, 5, 29$ и $x=9, 15, 19, 27$ соответственно).

В 1962 г. Б. М. Бредихин доказал, что существует бесконечно много простых чисел вида $x^2 + y^2 + 1$, где x и y — целые числа. Можно доказать (хотя это и трудно), что существует бесконечное множество простых чисел вида $x^2 + y^2 + z^2 + 1$, где x, y, z — натуральные числа. Позднее (в § 19) мы докажем, что существует бесконечно много простых чисел вида $x^2 + y^2$, где x и y — натуральные числа. Мы не знаем, существует ли бесконечное множество простых чисел, являющихся суммами кубов трех целых чисел.

13. Арифметические прогрессии, образованные из простых чисел

Доказано, что существует бесконечно много арифметических прогрессий, образованных из трех разных простых чисел. Мы знаем много прогрессий, образованных из трех различных простых чисел, первыми членами которых является число 3, например: 3, 7, 11; 3, 11, 19; 3, 13, 23; 3, 17, 31; 3, 23, 43; 3, 31, 59; 3, 37, 71; 3, 41, 79; 3, 43, 83. Однако неизвестно, существует ли их бесконечно много.

Легко доказать, что не может быть арифметической прогрессии, образованной из трех разных простых чисел, первым членом которой было бы число 2 (так как третий член последовательности был бы четный >2). Высказано предположение, что существует бесконечно много арифметических прогрессий, образованных из трех простых чисел, первым членом которых является любое простое нечетное число.

Существует только одна арифметическая прогрессия с разностью 2, составленная из трех простых чисел, именно: 3, 5, 7 (так как из трех последовательных нечетных чисел одно всегда делится на 3), а также только одна такая арифметическая прогрессия с разностью 4, именно: 3, 7, 11. Очевидно, не может быть арифметических прогрессий, составленных из трех простых чисел, с нечетной разностью. Высказано предположение, что существует бесконечно много прогрессий с разностью 6, образованных тремя простыми числами. Таковыми являются, например, прогрессии: 5, 11, 17; 11, 17, 23; 17, 23, 29. Имеется также прогрессия с разностью 6, обра-

зованная из пяти простых чисел: 5, 11, 17, 23, 29. Однако она является единственной, так как в каждой прогрессии с разностью 6, составленной из пяти натуральных чисел, один из членов должен делиться на пять.

Напрашивается вопрос, существует ли арифметическая прогрессия, состоящая из любого числа разных простых чисел. Среди известных нам наибольшую длину имеет прогрессия, состоящая из 12 членов. Эта прогрессия была найдена В. А. Голубевым, ее первый член 23 143, а разность 30 030.

Мы не знаем, существует ли арифметическая прогрессия, образованная из ста разных простых чисел. М. Кантор доказал, что в арифметической прогрессии, составленной из $n > 1$ простых чисел, больших n, разность прогрессии должна делиться на каждое простое число $\leqslant n$. Отсюда следует, что если существует арифметическая прогрессия, образованная из ста разных простых чисел, то разность ее должна быть огромным числом, имеющим по крайней мере несколько десятков цифр.

Высказано предположение, что если r есть натуральное число, делящееся на каждое простое число $\leqslant n$ (где n — заданное натуральное число > 1), то существует бесконечно много арифметических прогрессий с разностью r, образованных из n последовательных простых чисел. Например, 47, 53, 59 есть арифметическая прогрессия с разностью 6, образованная тремя последовательными простыми числами. Другими такими прогрессиями являются 151, 157, 163; 167, 173, 179. Мы знаем также арифметические прогрессии с разностью 6, образованные из четырех последовательных простых чисел, например, 251, 257, 263, 269 или 1741, 1747, 1753, 1759.

14. Малая теорема Ферма

Теорема 9. *Если p — простое число, то для каждого целого числа a число $a^p - a$ делится на p.*

Доказательство. Пусть p — данное простое число. Теорема, очевидно, справедлива для числа $a = 1$ Предположим, что она справедлива для некоторого

натурального числа a. Согласно формуле Ньютона для двучлена, имеем

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \ldots + \binom{p}{p-1} a + 1, \tag{1}$$

где для $k = 1, 2, \ldots, p-1$

$$\binom{p}{k} = \frac{p(p-1)(p-2)\ldots(p-k+1)}{1 \cdot 2 \ldots k},$$

причем, как известно, числа $\binom{p}{k}$ являются целыми. Отсюда мы заключаем, что число $1 \cdot 2 \ldots k \cdot \binom{p}{k}$ делится на p и, следовательно, согласно следствию теоремы 7, по крайней мере одно из чисел $1, 2, \ldots, k, \binom{p}{k}$ должно делиться на p. Но так как $k < p$, то ни одно из чисел $1, 2, \ldots, k$ не делится на p, следовательно, на p должно делиться число $\binom{p}{k}$. Отсюда, учитывая (1), мы заключаем, что число $(a+1)^p - a^p - 1$ делится на p. Прибавив к нему число $a^p - a$, делящееся на p (так как мы предполагаем, что теорема справедлива для числа a), мы обнаружим, что число $(a+1)^p - (a+1)$ делится на p, т. е. что теорема справедлива для числа $a+1$.

Таким образом, мы доказали посредством индукции, что теорема справедлива для каждого натурального числа a. Для числа 0 она, очевидно, также верна.

Если a — целое отрицательное число, то при $p = 2$ имеем $a^2 - a = a(a-1)$, и так как из двух последовательных целых чисел $a-1$ и a одно всегда четное, то всегда $2 | a^2 - a$ [1]). Далее, при p простом нечетном имеем $(-a)^p = -a^p$, и поэтому $(-a)^p - (-a) = -(a^p - a)$. Следовательно теорема справедлива и для целых отрицательных чисел a. Таким образом, теорема 9 доказана полностью.

В качестве частного случая теоремы 9, для $a = 2$, мы получаем теорему, согласно которой для любого простого числа p число $2^p - 2$ делится на p. Возникает

---

[1]) Символ r/s означает, что число s делится на r. Читается так: «r делит s».

вопрос, будет ли верна обратная теорема, т. е. если n — натуральное число >1, такое, что $n|2^n-2$, то должно ли n быть простым числом?

Для многих предполагаемых теорем, относящихся к простым числам, производилась проверка на большом числе частных случаев. Если бы мы проверили, например, все последовательные натуральные числа >1 и $\leqslant 300$, то обнаружили бы, что каждое такое натуральное число n, для которого 2^n-2 делится на n, является простым числом. Быть может, именно этот путь привел китайцев 25 веков назад к теореме, согласно которой, если для натурального числа $n>1$ число 2^n-2 делится на n, то число n простое. Однако эта теорема оказалась ложной, ибо число $2^{341}-2$, как мы сейчас покажем, делится на 341, а число $341=11\cdot 31$ является составным.

В том, что число $2^{341}-2$ делится на 341, мы можем убедиться следующим образом. Очевидно, $2^{341}-2=(2^{31})^{11}-2^{11}+2^{11}-2$. Число $2^{10}-1=1023=3\cdot 341$ делится на 341. Значит, и число $(2^{10})^3-1$ также делится на 341 (так как для натуральных a, b, и k число a^k-b^k, как известно, делится на $a-b$). Числа $2^{11}-2=2(2^{10}-1)$ и $2^{31}-2=2[(2^{10})^3-1]$ делятся на 341, откуда следует, что и число $(2^{31})^{11}-2^{11}$ делится на 341. Отсюда, в силу нашего равенства для числа $2^{341}-2$, тотчас же получаем, что это число делится на 341, что и требовалось доказать.

Естественно, возникает вопрос, существует ли бесконечно много натуральных чисел n, для которых китайская теорема неверна. Чтобы доказать, что ответ на этот вопрос является утвердительным, достаточно (имея в виду, что составное нечетное число 341 не удовлетворяет теореме) доказать, что для каждого составного нечетного числа n, не удовлетворяющего указанной теореме, существует составное нечетное число, большее n, также не удовлетворяющее ей.

Итак, предположим, что нечетное составное число $n=ab$, где a и b — натуральные числа >1, не удовлетворяет китайской теореме и, значит, $n|2^n-2$. Число $m=2^n-1=(2^a)^b-1$ есть нечетное составное, так как оно делится на число 2^a-1, большее 1 (ибо $a>1$) и меньшее чем m (ибо $b>1$), причем $m>n$ (ибо $n>1$). Таким образом, достаточно еще только

показать, что $m|2^m - 2$. Мы имеем $n|2^n - 2$, но n есть нечетное число, следовательно, $n|2^{n-1} - 1$, т. е. $2^{n-1} - 1 = kn$, где k — натуральное число. Отсюда $2^{m-1} = 2^{2^{(2^{n-1}-1)}} = 2^{2kn} = (2^n)^{2k}$. Число $2^{m-1} - 1 = (2^n)^{2k} - 1$, таким образом, делится на число $2^n - 1 = m$. Следовательно, и число $2^m - 2$ делится на m, и, значит, составное число m не удовлетворяет китайской теореме, что и требовалось доказать.

Возникает также вопрос, существуют ли составные четные числа, не удовлетворяющие китайской теореме. Только в 1950 г. Д. Х. Лемер нашел такое число: 161 038. Нахождение этого числа было очень сложным делом, проверить же, что оно является делителем числа $2^{161\,038} - 2$, нетрудно. Легко проверить, что $161\,038 = 2 \cdot 73 \cdot 1103$, $161\,037 = 3^2 \cdot 29 \cdot 617$, $2^9 - 1 = 7 \cdot 73$, $2^{29} - 1 = 1103 \cdot 486\,737$, откуда следует, что число $2^{161\,037} - 1$ делится на $2^9 - 1$ и $2^{29} - 1$, а значит, также на 73 и 1103. Таким образом, число $2^{161\,038} - 2$ делится на 2, 73 и 1103, а так как эти числа являются разными простыми числами, то $2^{161\,038} - 2$ делится на их произведение, т. е. на число 161 038, что и требовалось доказать.

В 1951 г. Н. Г. В. Х. Биджер доказал, что существует бесконечно много четных чисел n, для которых число $2^n - 2$ делится на n.

Доказано также, что существует бесконечно много пар разных простых чисел p и q таких, что число $2^{pq} - 2$ делится на pq. В 1958 г. А. Шинцель доказал, что для любого целого числа a и любого натурального m существуют разные простые числа $p > m$ и $q > m$ такие, что $pq|a^{pq} - a$.

В связи с ложностью китайской теоремы напрашивается вопрос, существуют ли составные числа n такие, что для каждого целого a число $a^n - a$ делится на n. Такие составные числа n мы называем абсолютно псевдопростыми[1]). Высказано предположение (до сих пор не доказанное), что таких чисел имеется бесконечно много. Наименьшее из них есть число $561 = 3 \cdot 11 \cdot 17$.

Чтобы доказать, что число 561 есть абсолютно псевдопростое, достаточно доказать, что для всех целых a

[1]) Название псевдопростые оставлено для составных чисел n, для которых число $2^n - 2$ делится на n.

число $a^{561} - a$ делится на каждое из простых чисел 3, 11, 17.

Число $a^{561} - a$, очевидно, делится на 3, если a делится на 3. Если же a не делится на 3, то a есть число вида $3k \pm 1$, откуда $a^2 - 1 = (3k \pm 1)^2 - 1 = 3(3k \pm \pm 2)k$, следовательно, $3 | a^2 - 1$; отсюда $3 | a^{2 \cdot 280} - 1$, а значит, и $3 | a^{561} - a$.

Число $a^{561} - a$, очевидно, делится на 11, если число a делится на 11. Согласно теореме Ферма, для всех целых a имеем $11 | a^{11} - a = a(a^{10} - 1)$, так что если число a не делится на 11, то отсюда вытекает, что $11 | a^{10} - 1$ и, следовательно, $11 | a^{10 \cdot 56} - 1$, откуда уже заключаем, что $11 | a^{561} - a$.

Число $a^{561} - a$ делится на 17, если число a делится на 17. Согласно теореме Ферма, для всех целых a имеем $17 | a^{17} - a$. Поэтому если число a не делится на 17, то отсюда вытекает, что $17 | a^{16} - 1$, откуда $17 | a^{16 \cdot 35} - 1$ и, значит, $17 | a^{561} - a$ (ибо $16 \cdot 35 + 1 = 561$). Итак, мы доказали, что число 561 является абсолютно псевдопростым.

Числами абсолютно псевдопростыми являются также

$$5 \cdot 29 \cdot 73, \quad 7 \cdot 13 \cdot 31, \quad 7 \cdot 23 \cdot 31, \quad 7 \cdot 31 \cdot 73,$$
$$13 \cdot 37 \cdot 61, \quad 5 \cdot 17 \cdot 29 \cdot 113 \cdot 337 \cdot 673 \cdot 2689;$$

известно и много других таких чисел.

Из малой теоремы Ферма вытекает, что если p — простое число >2, то число $2^{p-1} - 1$ делится на p. Возникает вопрос, существуют ли простые числа p, для которых $2^{p-1} - 1$ делится на p^2. Мы знаем только два таких простых числа p, именно 1093 и 3511, и знаем, что нет других таких простых чисел $p < 100\,000$; но мы не знаем, существуют ли такие числа, превосходящие 100 000, и конечно ли их количество. Мы не знаем также, существует ли бесконечно много простых чисел таких, для которых число $2^{p-1} - 1$ не делится на p^2.

Из теоремы Ферма легко вытекает, что если p — простое число, то число $1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots + \\ + (p-1)^{p-1} + 1$ делится на p. Г. Джуга высказал в 1950 г. предположение, что эта делимость имеет место только для простых чисел, и проверил его для всех чисел $\leqslant 10^{1000}$.

15. Доказательство теорем, согласно которым имеется бесконечно много простых чисел каждого из видов $4k+1$, $4k+3$ и $6k+5$

Пусть n означает любое натуральное число >1. Тогда число $n!$ есть число четное, а нечетное число $(n!)^2+1$ как число, большее единицы, согласно теореме 1, имеет простой делитель p, очевидно, нечетный и, следовательно, имеющий вид $4k+1$ или $4k+3$ (где k — целое число), причем $p>n$. Предположим, что $p=4k+3$. Очевидно, мы имеем $(n!)^2+1 \mid (n!)^{2(2k+1)}+1$, ибо, как известно, для натуральных a и нечетных m число a^m+1 делится на $a+1$ (причем $a^m+1=(a+1)(a^{m-1}-a^{m-2}+\ldots-a+1)$. Так как $2(2k+1)=4k+2=p-1$, то, учитывая, что $p \mid (n!)^2+1$, мы можем заключить, что $p \mid (n!)^{p-1}+1$ и, следовательно, $p \mid (n!)^p+n!$. Но, согласно теореме Ферма, $p \mid (n!)^p-n!$. Отсюда $p \mid 2n!$, что невозможно, так как p есть простое нечетное число $>n$. Следовательно, p должно быть числом вида $4k+1$. Таким образом, мы доказали, что для каждого натурального числа $n>1$ существует простое число $>n$, имеющее форму $4k+1$ (и что таким числом является каждый простой делитель числа $(n!)^2+1$). Тем самым доказана

Теорема 10. *Простых чисел вида $4k+1$ имеется бесконечно много.*

В связи с нашим доказательством напрашивается вопрос, для каждого ли простого числа p вида $4k+1$ существует натуральное число n такое, что $p \mid (n!)^2+1$. (Например, имеем: $5 \mid (2!)^2+1$, $13 \mid (6!)^2+1$). Можно показать (см. § 19), что если p есть простое число вида $4k+1$, то $p \mid \left[\left(\frac{p-1}{2}\right)!\right]^2+1$. Следовательно, $17 \mid (8!)^2+1$, $29 \mid (14!)^2+1$, $37 \mid (18!)^2+1$.

Возникает также вопрос, сколько имеется простых чисел вида $4k+3$. Доказательство того, что их бесконечно много, опирается на следующую лемму.

Лемма. *Каждое натуральное число вида $4k+3$ имеет по меньшей мере один простой делитель того же вида.*

Доказательство. Пусть $n=4k+3$. Это число имеет, очевидно, натуральные делители вида $4l+3$ (где

t есть целое число), так как само является одним из них. Обозначим через p наименьший из таких делителей. Ясно, что $p > 1$. Если бы p было числом составным, мы имели бы $p = ab$, где a и b были бы натуральными числами >1 и меньшими p, причем нечетными, так как p, будучи числом вида $4k + 3$, есть число нечетное. Оба числа a и b не могут быть вида $4t + 1$, так как тогда их произведение $p = ab = (4t_1 + 1)(4t_2 + 1) = 4(4t_1t_2 + t_1 + t_2) + 1$ было бы вида $4t + 1$, что исключено. Следовательно, по крайией мере одно из чисел a и b есть число вида $4t + 3$. Так как делители p являются одновременно делителями n, то n будет иметь натуральный делитель вида $4t + 3$, меньший p, что противоречит определению числа p. Итак, p — простое число. Таким образом, лемма доказана.

Пусть теперь n обозначает любое натуральное число. Число $4n! - 1$ есть, очевидно, натуральное число вида $4k + 3$. Согласно лемме, оно имеет по крайней мере один простой делитель p вида $4t + 3$. Здесь должно быть $p > n$, так как число $4n! - 1$, делясь на p, очевидно, не делится ни на одно натуральное число >1 и $\leqslant n$. Итак, мы доказали, что для каждого натурального числа n существует простое число $>n$, имеющее вид $4k + 3$.

Таким образом, доказана

Теорема 11. *Простых чисел вида* $4k + 3$ *имеется бесконечно много.*

Обозначим для вещественного числа x через $\pi_1(x)$ число простых чисел вида $4k + 1$, не больших чем x, а через $\pi_3(x)$ — число простых чисел вида $4k + 3$, не больших чем x. Например, $\pi_1(10) = 1$; $\pi_3(10) = 2$; $\pi_1(17) = \pi_3(17) = 3$; $\pi_1(100) = 11$, $\pi_3(100) = 13$. Проверено, что $\pi_1(x) \leqslant \pi_3(x)$ для $x < 26\,861$. Однако было бы ошибочно думать, что всегда $\pi_1(x) \leqslant \pi_3(x)$, ибо, как установил Дж. Лич в 1957 г., для $x = 26\,861$ $\pi_1(x) = 1473$, а $\pi_3(x) = 1472$.

Уже в 1914 г. Литтлвуд доказал, что существует бесконечное множество натуральных чисел x, для которых $\pi_1(x) > \pi_3(x)$, а также бесконечное множество натуральных x, для которых $\pi_1(x) < \pi_3(x)$. Мы видим, таким образом, какими ненадежными могут быть гипотезы относительно простых чисел, если они выдвигаются даже на основании большого числа наблюдений.

Теоремы 10 и 11 можно сформулировать следующим образом.

Каждая из арифметических прогрессий

$$1, 5, 9, 13, 17, 21, \ldots$$

и

$$3, 7, 11, 15, 19, 23, \ldots$$

содержит бесконечно много простых чисел.

В связи с этим напрашивается вопрос: какие бесконечные арифметические прогрессии, составленные из натуральных чисел, содержат бесконечно много простых чисел?

Пусть дана бесконечная арифметическая прогрессия

$$a, a + r, a + 2r, \ldots,$$

у которой первый член a и разность r — натуральные числа.

Если a и r имеют общий делитель $d > 1$, то, очевидно, каждое из чисел нашей последовательности будет делиться иа d и поэтому, как легко видеть, ни один член прогрессии, кроме, быть может, первого члена, не будет простым числом. Отсюда следует: для того чтобы арифметическая прогрессия с первым членом a и разностью r содержала бесконечное число простых чисел, необходимо, чтобы a и r не имели общего делителя, большего 1. Как доказал еще в 1837 г. П. Г. Лежен Дирихле, это условие является также и достаточным.

Доказательство теоремы Дирихле, хотя позднее и было упрощено различными авторами, является сложиым и длинным. Не менее сложно доказательство теоремы о том, что в каждой арифметической прогрессии, первый член и разность которой суть натуральные числа, не имеющие общего делителя, большего единицы, найдется по крайней мере одно простое число. Можно было бы подумать, что последняя теорема слабее теоремы Дирихле, однако нетрудно доказать, что она равносильна ей.

Некоторые частные случаи теоремы Дирихле (так называемой теоремы об арифметической прогрессии) могут быть доказаны просто. Дадим, например, дока-

зательство для случая $a = 5$, $r = 6$, для чего рассмотрим следующую лемму.

Лемма. *Каждое натуральное число вида* $6k + 5$ *имеет по крайней мере один простой делитель того же вида.*

Доказательство этой леммы совершенно аналогично доказательству леммы о числах вида $4k + 3$, с той лишь разницей, что вместо формы $4k + 3$ берем форму $6k + 5$, а затем используем замечание, что число вида $6t + 5$, как не делящееся на 2 и 3, может иметь делители только вида $6t + 1$ или $6t + 5$, а также что произведение двух чисел вида $6t + 1$ есть число того же вида.

Для доказательства самой теоремы возьмем какое-нибудь натуральное число n. Тогда число $6n! - 1$ будет, очевидно, вида $6k + 5$ и, согласно лемме, будет иметь простой делитель p того же вида, причем, как легко показать, $p > n$. Итак, для каждого натурального числа n существует простое число $p > n$, имеющее форму $6k + 5$. Отсюда следует

Теорема 12. *Простых чисел вида* $6k + 5$ *имеется бесконечно много.*

Итак, арифметическая прогрессия 5, 11, 17, 23, 29, 35, ... содержит бесконечно много простых чисел. Следовательно, арифметическая прогрессия

$$2, 5, 8, 11, 14, 17, 20, \ldots,$$

включающая в себя все члены первой прогрессии, и подавно содержит бесконечно много простых чисел, т. е. существует бесконечное множество простых чисел вида $3k + 2$.

Существуют еще некоторые другие арифметические прогрессии, относительно которых можно легко доказать, что они содержат бесконечно много простых чисел. Таковой является, например, прогрессия $8k + 1$ (где $k = 1, 2, 3, \ldots$).

16. Некоторые гипотезы относительно простых чисел

Пусть теперь n — данное натуральное число > 1. Расположим натуральные числа $1, 2, 3, \ldots, n^2$ в n строк

по n чисел в каждой строке, т. е. составим таблицу

$$\begin{array}{rrcrr}
1, & 2, & \ldots, & k, & \ldots, \quad n, \\
n+1, & n+2, & \ldots, & n+k, & \ldots, \quad 2n, \\
2n+1, & 2n+2, & \ldots, & 2n+k, & \ldots, \quad 3n, \\
\ldots & \ldots & \ldots & \ldots & \ldots \\
(n-1)n+1, & \ldots, & (n-1)n+k, & \ldots, & n^2
\end{array}$$

Столбцы этой таблицы образуют арифметические прогрессии (с n членами). А. Шинцель высказал предположение, что если k есть натуральное число $<n$, не имеющее общего с n делителя >1, то k-й столбец нашей таблицы содержит по меньшей мере одно простое число. А. Горжелевский проверил это предположение для всех натуральных чисел $n \leqslant 100$.

В. Серпинский высказал предположение, что каждая строка рассматриваемой таблицы (где $n > 1$) содержит по меньшей мере одно простое число. Это предположение было проверено А. Шинцелем при помощи таблиц А. Вестерна и Д. Х. Лемера для всех $n \leqslant 4500$. Первая строка таблицы (для $n > 1$) содержит всегда простое число 2. Утверждение о том, что вторая строка таблицы содержит по крайней мере одно простое число, как легко видеть, равносильно теореме Чебышева и, следовательно, справедливо. Доказано также, что для $n \geqslant 3$ третья строка таблицы содержит по крайней мере одно простое число, иными словами, что (для $n \geqslant 3$) между $2n$ и $3n$ лежит хотя бы одно простое число (что справедливо также для $n = 2$). Вообще доказано, что для $n \geqslant 9$ каждая из девяти первых строк таблицы содержит по крайней мере одно простое число.

Так как двумя последними строчками таблицы являются

$$(n-1)^2, \quad (n-1)^2+1, \ldots, n^2-n,$$
$$n^2-n+1, \quad n^2-n+2, \ldots, n^2,$$

то из предположения В. Серпинского вытекает, что между каждыми двумя последовательными квадратами натуральных чисел лежит по меньшей мере два простых числа. Далее, так как легко доказать, что если

m — натуральное число, то существует натуральное число n такое, что

$$m^3 \leqslant (n-1)^2 \quad \text{и} \quad n^2 \leqslant (m+1)^3,$$

то из предположения В. Серпинского следует, что между каждыми двумя последовательными кубами натуральных чисел содержится по крайней мере два простых числа. Мы не знаем, справедливо ли это, однако доказано, что для достаточно больших натуральных чисел m между m^3 и $(m+1)^3$ содержится произвольно много простых чисел.

Упомянем здесь еще о том, что, как заметил Ладислав Скуля, из предположения относительно рассматриваемой таблицы (для $n = 2, 3, \ldots$) следует, что как $(n+1)$-я, так и $(n+2)$-я строки содержат хотя бы по одному простому числу (или что для натуральных $n > 1$ каждая из последовательностей $n^2+1, n^2+2, \ldots, n^2+n$ и $n^2+n+1, n^2+n+2, \ldots, n^2+2n$ содержит по крайней мере одно простое число). Для $(n+3)$-й строки это, вообще говоря, неверно. Например, при $n = 2$ или при $n = 4$ получаются последовательности 9, 10 и 25, 26, 27, 28, не содержащие ни одного простого числа.

Из предположения относительно рассматриваемой таблицы можно также легко вывести, что если все натуральные числа выписывать последовательно в строчки по n чисел в n-й строке, т. е. если составить бесконечную треугольную таблицу

1				
2	3			
4	5	6		
7	8	9	10	
11	12	13	14	15
.	.	.	.	.

то в каждой строке этой таблицы, начиная со второй, найдется по крайней мере одно простое число. Мы не знаем, справедливо ли это утверждение.

17. Теорема Лагранжа

Теорема 13. *Если p — простое число и*

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

есть многочлен степени $n \geqslant 1$ с целыми коэффициентами, где коэффициент a_0 при высшей степени x не делится на p, то среди чисел

$$x = 0,\ 1,\ 2,\ 3,\ \ldots,\ p-1 \qquad (2)$$

существует не более чем n таких, для которых число $f(x)$ делится на p.

Доказательство. Теорема справедлива для многочленов степени 1. В самом деле, если бы среди чисел (2) было по меньшей мере два различных числа x_1 и $x_2 > x_1$ таких, что $p|f(x_1)$ и $p|f(x_2)$, то мы имели бы $p|f(x_2) - f(x_1)$, а так как $f(x) = a_0x + a_1$, то мы имели бы $p|a_0(x_2 - x_1)$, где $x_2 - x_1$, будучи разностью двух различных чисел последовательности (2) и, значит, меньших p, не делится на p. Следовательно, p было бы делителем произведения двух натуральных чисел, не делящихся на p, что противоречит теореме 7.

Пусть теперь n — некоторое натуральное число >1. Предположим, что теорема справедлива для многочленов степени $n-1$, и допустим при этом, что для некоторого многочлена (1) степени n теорема Лагранжа неверна, т. е. что существует набор целых чисел $x_1, x_2, \ldots, x_{n+1}$, где $0 \leqslant x_1 < x_2 < \ldots < x_{n+1} < p$, таких, что $p|f(x_i)$ для $i = 1, 2, \ldots, n+1$.

Имеем $f(x) - f(x_1) = a_0(x^n - x_1^n) + a_1(x^{n-1} - x_1^{n-1}) + \ldots + a_{n-1}(x - x_1)$. Отсюда, так как $x^k - x_1^k = (x - x_1) \times (x^{k-1} + x_1x^{k-2} + \ldots + x_1^{k-2}x + x_1^{k-1})$ для $k = 2, 3, \ldots, n$, то мы легко найдем, что

$$f(x) - f(x_1) = (x - x_1)f_1(x), \qquad (3)$$

где $f_1(x)$ — многочлен степени $n-1$ с целыми коэффициентами (зависящими от $a_0, a_1, \ldots, a_n$ и x_1), причем коэффициентом при x^{n-1} будет a_0, т. е. число, не делящееся на p.

На основании тождества (3), мы получим

$$f(x_i) - f(x_1) = (x_i - x_1)f_1(x_i) \qquad (4)$$

для $i = 2, 3, \ldots, n+1$.

Но из того, что $p|f(x_i)$ для $i = 1, 2, \ldots, n+1$, следует, что

$$p|f(x_i) - f(x_1) \text{ для } i = 2, 3, \ldots, n+1;$$

значит, согласно (4), имеем:

$$p|(x_i - x_1)f_1(x_i) \text{ для } i = 2, 3, \ldots, n+1,$$

а так как числа $x_i - x_1$ для $i = 2, 3, \ldots, n+1$ не делятся на p, то, в силу теоремы 7, должно быть

$$p|f_1(x_i) \text{ для } i = 2, 3, \ldots, n+1,$$

вопреки предположению, что теорема справедлива для многочленов степени $n-1$.

Следствие. *Если p есть простое число, а* (1) — *многочлен степени n с целыми коэффициентами, и если существует более чем n натуральных чисел $x < p$, для которых $f(x)$ делится на p, то все коэффициенты многочлена* (1) *делятся на p.*

Доказательство. Предположим, что многочлен (1) удовлетворяет условию следствия, но не все коэффициенты его делятся на p. Пусть a_{n-k} есть первый по порядку коэффициент, не делящийся на p. Предположим, что $k > 0$. Для каждого натурального x, для которого $f(x)$ делится на p, очевидно,

$$g(x) = a_{n-k}x^k + a_{n-k+1}x^{k-1} + \ldots + a_n$$

также делится на p. Таким образом, для многочлена $g(x)$ степени k существует более чем n и, так как $k \leqslant n$, более чем k натуральных чисел $x < p$, для которых $p|g(x)$, что противоречит теореме Лагранжа (применимой, так как a_{n-k} не делится на p). Итак, предположим, что $k=0$, т. е. что все коэффициенты многочлена (1), кроме a_n, делятся на p. Но тогда, поскольку существует число x, для которого $f(x)$ делится на p, мы, исходя из формулы (1), должны будем заключить, что $p|a_n$. Таким образом, предположение, что наше следствие несправедливо, в каждом случае приводит к противоречию.

18. Теорема Вильсона

Дадим теперь одно важное применение доказанного в § 17 следствия. Пусть p — простое число и пусть

$$f(x) = (x-1)(x-2)\ldots(x-p+1) - x^{p-1} + 1$$

есть многочлен степени $p-2$ с целыми коэффициентами. Для $x=1, 2, \ldots, p-1$, согласно теореме Ферма, мы имеем $p|x^p-x=x(x^{p-1}-1)$, откуда $p|x^{p-1}-1$.

Но для $x=1, 2, \ldots, p-1$ мы, очевидно, также имеем

$$p|(x-1)(x-2)\ldots(x-p+1),$$

так как для таких x один из сомножителей рассматриваемого произведения равен нулю. Учитывая, что разность двух чисел, делящихся на p, делится на p, мы заключаем, что $p|f(x)$ для $x=1, 2, \ldots, p-1$.

Таким образом, согласно следствию теоремы Лагранжа (для $n=p-2$), мы можем заключить, что все коэффициенты нашего многочлена, а значит, и его свободный член делятся на p.

Но для нечетных p (так как $(-1)^{p-1}=1$) свободным членом многочлена $f(x)$ является число $1\cdot 2\cdot 3\ldots\ldots(p-1)+1$ или $(p-1)!+1$. Следовательно, если p есть простое нечетное число, то $p|(p-1)!+1$, что, впрочем, справедливо и для $p=2$, так как $1!+1=2$. Таким образом, доказаиа

Теорема 14 (Вильсона). *Для каждого простого числа p число $(p-1)!+1$ делится на p.*

Следует заметить, что если для натурального числа $n>1$ число $(n-1)!+1$ делится иа n, то n должно быть простым числом. Действительно, если бы n было составным, то в силу того, что $n=ab$, где a и b — натуральные числа >1 и $<n$, число a было бы одним из сомножителей произведения $1\cdot 2\ldots(n-1)$ и, следовательно, число $(n-1)!+1$ при делении иа a давало бы в остатке 1, между тем как, делясь иа n, оно и подавно должно делиться на a. Полученное противоречие доказывает, что число n должио быть простым.

Итак, *для того чтобы натуральное число $n>1$ было простым, необходимо и достаточно, чтобы число $(n-1)!+1$ делилось на n.*

Таким образом, теоретически мы можем при помощи только одного деления выяснить, является данное число простым нли нет. Однако практически пользоваться этим способом неудобно, так как уже для трехзначных n число $(n-1)!+1$ имеет более чем сто цифр.

В связи с теоремой Вильсона возникает вопрос, возможны ли такие простые числа p, для которых $(p-1)!+1$ делится на p^2. Оказывается, для $p \leqslant 30\,000$ имеется три таких числа: 5, 13 и 563. Мы не знаем, существует ли бесконечно много таких чисел p.

Теоремы Ферма и Вильсона можно соединить в одну следующую теорему:

Если p — простое число, то для любого целого числа a число $a^p + (p-1)!a$ делится на p.

В самом деле, если p — простое и a — произвольное целое число, то, согласно теореме Ферма, число $a^p - a$ делится на p, а так как, согласно теореме Вильсона, число $a + (p-1)!a = [1 + (p-1)!]a$ делится на p, то и сумма этих чисел, т. е. число $a^p + (p-1)!a$ также делится на p. С другой стороны, если $a^p + (p-1)!a$ делится на p при любом целом a, то при $a = 1$ мы получаем отсюда теорему Вильсона, из которой следует, что при любом целом a $p \mid (p-1)!a + a$, а так как $p \mid a^p + (p-1)!a$, то $p \mid a^p + (p-1)!a - [(p-1)!a + a]$, т. е. $p \mid a^p - a$, что дает теорему Ферма.

Легко также доказать, что теоремы Ферма и Вильсона можно соединить и в следующую теорему:

Если p — простое число, a — целое число, то число $(p-1)!a_p + a$ делится на p (Лео Мозер).

Из теоремы Вильсона вытекает

Теорема 15 (Лейбница). *Для того чтобы натуральное число $p > 2$ было простым, необходимо и достаточно, чтобы число $(p-2)! - 1$ делилось на p.*

Доказательство. Если число $p > 2$ является простым, то, согласно теореме Вильсона, число $(p-1)! + 1$ делится на p. Учитывая, что $(p-1)! = (p-2)!(p-1)$, мы имеем $(p-1)! + 1 = (p-2)!p - [(p-2)! - 1]$, откуда видно, что число $(p-2)! - 1$ делится на p.

С другой стороны, если $p \mid (p-2)! - 1$, то $p \mid (p-1)! - (p-1)$ и поэтому $p \mid (p-1)! + 1$, откуда (напомним, что $p > 2$), как было уже доказано выше, следует, что p должно быть простым числом. Таким образом, теорема Лейбница доказана.

Если p есть простое число >3, то $(p-1)! > p$, ибо тогда $(p-1)! \geqslant 2(p-1) = p + (p-2) > p$. Поэтому число $(p-1)! + 1$, как число, большее p и, согласно

теореме Вильсона, делящееся на p, является числом составным.

Итак, если $p > 3$ есть простое число, то $(p-1)! + 1$ есть число составное. Отсюда следует, что существует бесконечное множество натуральных чисел n, для которых число $n! + 1$ является составным. Существует ли бесконечное множество натуральных n, для которых число $n! + 1$ является простым, мы не знаем.

Простыми являются числа $1! + 1 = 2$, $2! + 1 = 3$, $3! + 1 = 7$; следующим простым числом того же вида является $11! + 1 = 39\,916\,801$. Мы не знаем, является ли простым число $27! + 1$.

На основании теоремы Лейбница можно легко заключить, что существует бесконечное множество натуральных чисел n, для которых число $n! - 1$ является составным. Но мы не знаем, существует ли бесконечное множество натуральных n, для которых число $n! - 1$ является простым (простыми являются числа $3! - 1 = 5$, $4! - 1 = 23$, $6! - 1 = 719$). Мы не знаем также, существует ли среди чисел каждого из видов $p! + 1$ и $p! - 1$, где p — простое число, бесконечное множество составных чисел.

Мы не знаем ответа на вопрос, существует ли бесконечное множество натуральных n, для которых число $p_1 p_2 \dots p_n + 1$ является простым (p_n есть n-е простое число), а также на вопрос, существует ли бесконечное множество таких натуральных чисел n, для которых число $p_1 p_2 \dots p_n + 1$ является составным.

Числа $p_1 + 1 = 3$, $p_1 p_2 + 1 = 7$, $p_1 p_2 p_3 + 1 = 31$, $p_1 p_2 p_3 p_4 + 1 = 211$, $p_1 p_2 p_3 p_4 p_5 + 1 = 2311$ являются простыми, но числа $p_1 p_2 \dots p_n + 1$ для $n = 6$, 7 и 8 являются составными, делящимися соответственно на 59, 19 и 347.

Докажем еще (следуя идее А. Шинцеля), что для натуральных $n > 3$ произведение Q_n всех простых чисел, меньших n, будет больше чем n.

Допустим, что при некотором натуральном $n > 3$ $Q_n \leqslant n$. Тогда мы имели бы $Q_n - 1 < n$. Число $Q_n - 1$ не делится ни на одно простое число $< n$ (так как такие числа являются делителями Q_n), поэтому, учитывая, что $n \geqslant 4$, мы заключаем, что число $Q_n - 1 \geqslant Q_4 - 1 = 5 > 1$ имеет простой делитель p, который должен быть $\geqslant n$. Но тогда $Q_n - 1 \geqslant n$, что приводит

к противоречию. Таким образом, $Q_n > n$ для $n > 3$, что и требовалось доказать.

Относительно произведения P_n всех простых чисел $\leqslant n$ можно доказать, что для натуральных n имеет место неравенство $P_n < 4^n$, а для натуральных $n \geqslant 29$ неравеиство $P_n > 2^n$.

Доказано также, что для натуральных $n > 2$ сумма всех простых чисел $\leqslant n$ будет $> n$.

19. Разложение простого числа на сумму двух квадратов

Пусть теперь p обозначает простое число вида $4k + 1$. Принимая во внимание четность числа $\frac{p-1}{2} = 2k$, найдем, что число

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

при делении на p дает, очевидно, такой же остаток, как число

$$(p-1)(p-2) \ldots \left(p - \frac{p-1}{2}\right).$$

Но последнее число, если его сомножители записать в обратиом порядке, можно представить в виде

$$\frac{p+1}{2}\left(\frac{p+1}{2} + 1\right) \ldots (p-2)(p-1),$$

поэтому, если мы его умножим на $\left(\frac{p-1}{2}\right)!$ и заметим, что $\frac{p+1}{2} = \frac{p-1}{2} + 1$, то найдем, что получившееся число $(p+1)!$ дает при делении на p такой же остаток, как $\left(\frac{p-1}{2}\right)!^2$. А так как $(p-1)! + 1$, согласно теореме Вильсона, делится на p, то и число $\left(\frac{p-1}{2}\right)!^2 + 1$ также делится на p. Таким образом, доказана

Теорема 16. *Если p есть простое число вида $4k + 1$, то число $\left(\frac{p-1}{2}\right)!^2 + 1$ делится на p.*

Для вывода следствия из этой теоремы нам понадобится следующая

Лемма. *Если p — простое число и a — целое число, не делящееся на p, то существуют натуральные числа $x < \sqrt{p}$ и $y < \sqrt{p}$ такие, что при соответствующем знаке + или — число $ax \pm y$ делится на p.*

Доказательство. Пусть p — данное простое число и пусть m обозначает наибольшее натуральное число $\leqslant \sqrt{p}$, так что $m+1 > \sqrt{p}$ и, следовательно, $(m+1)^2 > p$. Рассмотрим целые числа $ax - y$, где x и y принимают значения 0, 1, 2, ..., m. Таких чисел имеется $(m+1)^2 > p$, а так как при делении их на p различных остатков может быть не более чем p, то при двух разных системах чисел x_1, y_1 и x_2, y_2, где, например, $x_1 \geqslant x_2$, числа $ax_1 - y_1$ и $ax_2 - y_2$ должны при делении на p давать одинаковые остатки и, значит, число $ax_1 - y_1 - (ax_2 - y_2) = a(x_1 - x_2) - (y_1 - y_2)$ должно делиться на p. Равенство $x_1 = x_2$ здесь исключено, так как в этом случае число $y_1 - y_2$ делилось бы на p, что, ввиду $0 \leqslant y_1 \leqslant m \leqslant \sqrt{p} < p$ и аналогично $0 \leqslant y_2 < p$, невозможно, поскольку системы x_1, y_1 и x_2, y_2 предполагаются разными. Исключено также и равенство $y_1 = y_2$, так как в этом случае число $a(x_1 - x_2)$ делилось бы на p, откуда, согласно определению числа a, следовало бы, что число $x_1 - x_2$ делится на p, а это невозможно (в последнем убеждаемся так же, как и в случае разности $y_1 - y_2$). Далее, так как $x_1 \geqslant x_2$ и $x_1 \neq x_2$, то число $x_1 - x_2$ является натуральным, число же $y_1 - y_2$ целое, отличное от нуля, следовательно, при соответствующем знаке, число $y = \pm(y_1 - y_2)$ также является натуральным. Теперь замечаем, что $x = x_1 - x_2 \leqslant x_1 \leqslant m \leqslant \sqrt{p}$, следовательно, $x < \sqrt{p}$, ибо равенство $x^2 = p$ невозможно, поскольку p — простое число. Аналогично $y < \sqrt{p}$. При этом число $ax \pm y$, которое при соответствующем знаке равно числу $a(x_1 - x_2) - (y_1 - y_2)$, делится на p. Таким образом, лемма доказана.

Пусть теперь p — простое число вида $4k+1$ и пусть $a = \left(\frac{p-1}{2}\right)!$ есть число, не делящееся на p (согласно следствию теоремы 7, как произведение нескольких натуральных чисел, меньших p). Тогда, в силу нашей леммы, существуют натуральные числа $x < \sqrt{p}$, $y <$

$< \sqrt{p}$ такие, что при соответствующем знаке + или — число $ax \pm y$ делится на p. Таким образом, в любом случае число $a^2x^2 - y^2 = (ax + y)(ax - y)$ будет делиться на p. Но, на основании теоремы 16, число $a^2 + 1$ делится на p, следовательно, и число $a^2x^2 + x^2$ делится на p. Поскольку же числа $a^2x^2 + x^2$ и $a^2x^2 - y^2$ делятся на p, то и их разность $x^2 + y^2$ делится на p и, следовательно, $x^2 + y^2 = kp$, где k — натуральное число. Так как $x < \sqrt{p}$ и $y < \sqrt{p}$, то $x^2 + y^2 < 2p$, или $kp < 2p$, откуда $k < 2$, а так как k — натуральное число, то $k = 1$, т. е. $x^2 + y^2 = p$. Таким образом, доказана

Теорема 17 (Ферма). *Каждое простое число вида* $4k + 1$ *есть сумма двух квадратов натуральных чисел.*

Так, например, $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$, $29 = 2^2 + 5^2$, $37 = 1^2 + 6^2$, $41 = 4^2 + 5^2$, $53 = 2^2 + 7^2$, $61 = 5^2 + 6^2$, $73 = 3^2 + 8^2$.

Докажем теперь, что разложение простого числа на сумму двух квадратов натуральных чисел единственно, если не обращать внимания на порядок слагаемых. Впрочем, мы докажем даже более общее предложение.

Теорема 18. *Пусть* a *и* b *— данные натуральные числа, тогда ни одно простое число* p *нельзя представить двумя различными способами в форме* $p = ax^2 + by^2$, *где* x *и* y *— натуральные числа, если в случае* $a = b = 1$ *не обращать внимания на порядок слагаемых.*

Доказательство. Предположим, что простое число p допускает два разложения:

$$p = ax^2 + by^2 = ax_1^2 + by_1^2,$$

где x, y, x_1, y_1 — натуральные числа. Отсюда получаем $p^2 = (axx_1 + byy_1)^2 + ab(xy_1 - yx_1)^2 = (axx_1 - byy_1)^2 + ab(xy_1 + yx_1)^2$.

Но $(axx_1 + byy_1)(xy_1 + yx_1) = (ax^2 + by^2)x_1y_1 + (ax_1^2 + by_1^2)xy = p(x_1y_1 + xy)$. Таким образом, по крайней мере один из сомножителей левой части должен делиться на простое число p.

Если $p \mid axx_1 + byy_1$, то из первого выражения для p^2 следует, что должно быть $xy_1 - yx_1 = 0$ и, следовательно, $xy_1 = yx_1$, $p = axx_1 + byy_1$, $px = (ax^2 + by^2)x_1 = px_1$, откуда $x = x_1$, а значит, и $y = y_1$.

Если же $p \mid xy_1 + yx_1$, то из второго выражения для p^2 следует, что $axx_1 - byy_1 = 0$ и $p^2 = ab(xy_1 + yx_1)^2$,

причем последнее, если учесть, что числа x, y, x_1 и y_1 являются натуральными, возможно только тогда, когда $a = b = 1$. Поэтому имеем $p = xy_1 + yx_1$ и $xx_1 - yy_1 = 0$, что дает нам равенство $px = (x^2 + y^2)y_1 = py_1$, откуда $x = y_1$ и, следовательно (принимая во внимание, что $p = x^2 + y^2 = x_1^2 + y_1^2$), $y = x_1$. Таким образом, наши разложения отличаются одно от другого только порядком слагаемых. Теорема 18 доказана.

Из теоремы 18 тотчас же следует, что если натуральное число n можно представить хотя бы двумя способами в виде суммы двух квадратов натуральных чисел (при условии, что два разложения, отличающиеся только порядком слагаемых, не считаются различными), то n не является простым числом. Поэтому, например, из того что $2501 = 1^2 + 50^2 = 10^2 + 49^2$, мы заключаем, что число 2501 не является простым.

Пусть m и n — натуральные числа. Имеем $m^4 + 4n^4 = (m^2)^2 + (2n^2)^2 = (m^2 - 2n^2)^2 + (2mn)^2$.

Если $m = n$ или $m = 2n$, то наши разложения на суммы квадратов одинаковы, но тогда мы имеем либо $m^4 + 4n^4 = 5n^4$, что является простым числом только для $m = n = 1$, либо $m^4 + 4n^4 = 20n^4$, что является числом составным. Если же $m \neq n$ и $m \neq 2n$, то, как легко доказать, наши разложения отличаются друг от друга не только порядком слагаемых, и, значит, число $m^4 + 4n^4$ — составное. Следовательно,

Если m и n — натуральные числа, из которых по крайней мере одно отлично от единицы, то число $m^4 + 4n^4$ является составным.

В частности (для $m = 1$), отсюда следует, что *все числа вида $4n^4 + 1$, где n — натуральное число > 1, являются составными.*

Если мы имеем два разложения данного натурального числа на суммы двух квадратов (отличающиеся друг от друга не только порядком слагаемых), то нетрудно показать, что можно найти представление этого числа в виде произведения двух натуральных чисел, больших единицы.

В частности, совершенно элементарно можно получить следующее разложение на множители

$$m^4 + 4n^4 = (m^2 + 2mn + 2n^2)(m^2 - 2mn + 2n^2),$$

Заметим, однако, что если натуральное число допускает только одно разложение на сумму двух квадратов натуральных чисел, то отсюда еще не следует, что оно должно быть простым числом. Например, как легко убедиться, числа 10, 18, 45 дают каждое только одно разложение: $10 = 1^2 + 3^2$, $18 = 3^2 + 3^2$, $45 = 3^2 + 6^2$.

Но можно доказать, что если натуральное нечетное число n дает только одно разложение на сумму двух квадратов целых чисел $\geqslant 0$ (если не считать различными разложения, отличающиеся только порядком слагаемых), причем в этом разложении слагаемые не имеют общего делителя >1, то n является простым числом. Основываясь на этом, при помощи электронной вычислительной машины ЕМС, находящейся в Варшавском политехническом институте, удалось показать, что число $2^{39} - 7$ есть простое; произведенное исследование показало, что существует только одно разложение этого числа на сумму двух квадратов, именно

$$2^{39} - 7 = 64\,045^2 + 738\,684^2,$$

причем в этом разложении слагаемые не имеют общего делителя >1.

О числах $2^n - 7$ для $n = 4, 5, \ldots, 38$ известно, что они являются составными. В 1956 г. П. Эрдеш поставил вопрос, все ли числа $2^n - 7$ для натуральных $n > 3$ составные. Ответ на этот вопрос, как мы видим, отрицателен.

Числа $2^n - 7$ являются составными для $n = 40, 41, \ldots, 50$, ибо они, как это было подтверждено, делятся соответственно на 3, 5, 3, 107, 3, 5, 3, 11, 3, 61, 3. Таким образом, среди чисел $2^n - 7$ для натуральных n, где $3 < n \leqslant 50$, имеется только одно простое (для $n = 39$).

Легко доказать, что среди чисел $2^p - 7$, где p — простое число, имеется бесконечно много составных. Действительно, согласно теореме 10, существует бесконечно много простых чисел вида $4k + 1$, а для каждого такого простого числа p, в силу того, что $5 | 2^4 - 1$, имеем $5 | 2^{4k} - 1$, откуда $5 | 2^{4k+1} - 2$, а значит, также $5 | 2^p - 7$.

Мы не знаем, существует ли бесконечное множество натуральных чисел n, для которых число $2^n - 7$ является простым.

В связи с теоремой 17 напрашивается вопрос, что можно сообщить о разложениях других простых чисел на суммы двух квадратов.

Число 2 имеет, очевидно, только одно представление в виде суммы двух квадратов натуральных чисел: $2 = 1^2 + 1^2$. Таким образом, остается еще исследовать простые числа вида $4k + 3$ (где $k = 0, 1, 2, \ldots$). Легко доказать, что ни одно натуральное число этого вида не может быть представлено в виде суммы двух квадратов целых чисел. Действительно, поскольку это число нечетное, то в случае $4k + 3 = x^2 + y^2$ целые числа x и y не могли бы быть оба четными или же нечетными. Таким образом, одно из них должно быть четным, а другое нечетным. Но квадрат четного числа при делении на 4 дает в остатке нуль, квадрат же нечетного — единицу. Следовательно, сумма $x^2 + y^2$ при делении на 4 дала бы в остатке 1, в то время как число $4k + 3$ дает в остатке 3. Формула $4k + 3 = x^2 + y^2$, таким образом, оказывается невозможной при целых k, x и y.

Итак, *среди простых чисел только число 2 и простые числа вида* $4k + 1$ *разлагаются на суммы двух квадратов натуральных чисел, причем каждое из них дает только одно такое разложение* (если не считать различными разложения, отличающиеся только порядком слагаемых).

Труднее ответить на вопрос, какие натуральные числа являются суммами двух квадратов натуральных чисел. Можно доказать, что для того чтобы натуральное число n было суммой двух квадратов натуральных чисел, необходимо и достаточно, чтобы в его разложении на простые сомножители сомножители вида $4k + 3$, если они встречаются, входили в степенях с четными показателями и, кроме того, чтобы либо число 2 входило с нечетным показателем, либо число n имело по крайней мере один простой делитель вида $4k + 1$.

Исследован также вопрос, сколько данное натуральное число n дает разложений на суммы двух квадратов натуральных чисел. Оказывается, это зависит от разложения числа n на простые сомножители. Можно доказать, что существуют натуральные числа, дающие произвольно много разложений на суммы двух квадратов натуральных чисел. Число 65 дает два разложения на суммы двух квадратов: $65 = 1^2 + 8^2 = 4^2 + 7^2$; чис-

ло 1105 дает четыре таких разложения: $1105 = 4^2 + 33^2 = 9^2 + 32^2 = 12^2 + 31^2 = 23^2 + 24^2$.

20. Разложение простого числа на разность двух квадратов и другие разложения

Напрашивается вопрос, какие простые числа и сколькими способами могут быть представлены в виде разности двух квадратов натуральных чисел.

Предположим, что простое число p разлагается на разность двух квадратов натуральных чисел: $p = x^2 - y^2$, где x и y — натуральные числа, причем, очевидно, $x > y$. Отсюда $p = (x - y)(x + y)$ и, значит, $x - y$ и $x + y$ являются натуральными делителями числа p, причем первый меньше второго. Но так как p — простое число, то $x - y = 1$, $x + y = p$ и, следовательно, $x = \frac{p+1}{2}$, $y = \frac{p-1}{2}$. Таким образом, число p должно быть нечетным, и в этом случае мы имеем единственное разложение

$$p = \left(\frac{p+1}{2}\right)^2 - \left(\frac{p-1}{2}\right)^2.$$

Итак, доказана

Теорема 19. *Каждое нечетное простое число представимо в виде разности двух квадратов натуральных чисел и притом только одним способом.*

Легко доказать, что для того чтобы натуральное число $n > 1$ было разностью двух квадратов натуральных чисел, необходимо и достаточно, чтобы при делении на 4 оно не давало в остатке 2.

Можно доказать, что существуют числа, допускающие достаточно большое число разложений на разность двух квадратов. Из теоремы 19 следует, что натуральное число, допускающее более чем одно разложение на разность двух квадратов натуральных чисел, не является простым.

Впрочем, легко также доказать, что если нечетное число имеет только одно разложение на разность двух квадратов целых чисел, то оно является простым. В самом деле, предположим, что нечетное число

n — составное и, значит, $n = ab$, где a и b — натуральные числа > 1. Очевидно, имеем

$$n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2 = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2,$$

причем если, например, $a \geqslant b$, то $n - 1 = ab - 1 > a - b$ (так как $b > 1$), и, следовательно, наши разложения являются различными.

Таким образом, нечетное составное число дает по крайней мере два различных разложения на разность двух квадратов целых чисел. Заметим, однако, что имеются нечетные составные числа, представимые единственным способом в виде разности двух квадратов натуральных чисел, например число 9. (Можно доказать, что такими числами являются квадраты простых нечетных чисел.)

Перейдем теперь к вопросу о разложении простых чисел на суммы трех квадратов натуральных чисел.

Можно доказать, что существует бесконечно много простых чисел, являющихся суммами трех квадратов натуральных чисел, а также бесконечно много простых чисел, не являющихся такими суммами. Среди простых чисел <100 суммами трех квадратов натуральных чисел являются только следующие:
$3 = 1^2 + 1^2 + 1^2$, $11 = 1^2 + 1^2 + 3^2$, $17 = 2^2 + 2^2 + 3^2$, $19 = 1^2 + 3^2 + 3^2$, $29 = 2^2 + 3^2 + 4^2$, $41 = 1^2 + 2^2 + 6^2 = 3^2 + 4^2 + 4^2$, $43 = 3^2 + 3^2 + 5^2$, $53 = 1^2 + 4^2 + 6^2$, $59 = 1^2 + 3^2 + 7^2$, $61 = 3^2 + 4^2 + 6^2$, $67 = 3^2 + 3^2 + 7^2$, $73 = 1^2 + 6^2 + 6^2$, $83 = 1^2 + 1^2 + 9^2 = 3^2 + 5^2 + 7^2$, $89 = 2^2 + 2^2 + 9^2 = 2^2 + 6^2 + 7^2 = 3^2 + 4^2 + 8^2$, $97 = 5^2 + 6^2 + 6^2$.

Мы видим также, что существуют простые числа, имеющие более чем одно разложение на сумму трех квадратов натуральных чисел, например числа 41, 83 и 89.

Легко доказать, что каждое целое число можно представить бесконечным числом способов в виде $x^2 + y^2 - z^2$, где x, y, z — натуральные числа. Для этого достаточно заметить, что для целых k и t имеют место тождества:

$$2k - 1 = (2t)^2 + (k - 2t^2)^2 - (k - 2t^2 - 1)^2,$$
$$2k = (2t + 1)^2 + (k - 2t^2 - 2t)^2 - (k - 2t^2 - 2t - 1)^2.$$

Что же касается разложений простых чисел на суммы четырех квадратов натуральных чисел, то можно доказать, что такие разложения имеют все простые числа, за исключением чисел: 2, 3, 5, 11, 17, 29 и 41.

Можно также доказать, что единственными простыми числами, которые не представимы в виде суммы пяти квадратов натуральных чисел, являются числа 2, 3 и 7 и что для каждого натурального числа $m > 3$ существует только конечное число простых чисел, не являющихся суммами m квадратов натуральных чисел.

И. Човла высказал предположение, что если число 1 считать простым (как это прежде иногда делали), то каждое натуральное число является суммой восьми или меньшего числа квадратов простых чисел. Это проверено для натуральных чисел $\leqslant 288\,000$.

В связи с теоремой 17 напрашивается вопрос, какие простые числа могут быть представлены в форме $x^2 + 2y^2$, или в форме $x^2 + 3y^2$, где x и y — натуральные числа. Здесь имеет место следующая теорема.

Для того чтобы простое число p можно было представить в виде $x^2 + 2y^2$, где x и y — натуральные числа, необходимо и достаточно, чтобы p было вида $8k + 1$ или $8k + 3$. Каждое простое число этих видов дает только одно разложение вида $x^2 + 2y^2$ (что вытекает из теоремы 18).

Так, например,

$$3 = 1^2 + 2 \cdot 1^2,\ 11 = 3^2 + 2 \cdot 1^2,\ 17 = 3^2 + 2 \cdot 2^2,\ 19 = 1^2 + 2 \cdot 3^2.$$

Высказано предположение, что существует бесконечно много простых чисел p вида $8k + 1$ и также вида $8k + 3$ таких, что $p = 1^2 + 2y^2$, где y — натуральное число, а также бесконечно много таких, что $p = x^2 + 2 \cdot 1^2$, где x — натуральное число. Например, $73 = 1^2 + 2 \cdot 6^2$, $83 = 9^2 + 2 \cdot 1^2$.

Для того чтобы простое число p можно было представить в виде $x^2 + 3y^2$, где x и y — натуральные числа, необходимо и достаточно, чтобы p было вида $6k + 1$. Каждое простое число этого вида дает только одно разложение вида $x^2 + 3y^2$.

Так, например, $7 = 2^2 + 3 \cdot 1^2$, $13 = 1^2 + 3 \cdot 2^2$, $19 = 4^2 + 3 \cdot 1^2$, $31 = 2^2 + 3 \cdot 3^2$, $37 = 5^2 + 3 \cdot 2^2$. Высказано предположение, что существует бесконечно много простых чисел p вида $6k + 1$ таких, что $p = 1^2 + 3y^2$, где

y — натуральное число, а также бесконечно много таких, что $p = x^2 + 3 \cdot 1^2$, где x — натуральное число. Имеем, например, $67 = 8^2 + 3 \cdot 1^2$, $103 = 10^2 + 3 \cdot 1^2$, $109 = 1^2 + 3 \cdot 6^2$.

Из теоремы 17 непосредственно следует, что *для того чтобы простое число p можно было представить в виде $x^2 + 4y^2$, где x и y — натуральные числа, необходимо и достаточно, чтобы p было вида $4k + 1$.*

Доказана также следующая теорема:

Для того чтобы простое нечетное число p можно было представить в виде $x^2 - 2y^2$, где x и y — натуральные числа, необходимо и достаточно, чтобы p было числом одного из видов: $8k + 1$ или $8k + 7$ [1]).

Займемся теперь вопросом, какие простые числа являются суммами двух кубов натуральных чисел. На этот вопрос можно легко дать ответ. Действительно, если простое число p является суммой двух кубов натуральных чисел, $p = x^3 + y^3$, то $x + y | p$, и если хотя бы одно из чисел x, y оказалось бы больше единицы, то было бы $x + y < x^3 + y^3 = p$, т. е. число p имело бы натуральный делитель $x + y$, больший единицы и меньший p, что невозможно. Таким образом, должно быть $x = y = 1$ и, следовательно, $p = 2$.

Итак, *ни одно простое число, кроме числа $2 = 1^3 + 1^3$, не является суммой двух кубов натуральных чисел.*

Какие же простые числа являются разностями двух кубов натуральных чисел? Если p — простое число и $p = x^3 - y^3$, где x и y — натуральные числа, то $x > y$, и имеем $p = x^3 - y^3 = (x - y)(x^2 + xy + y^2)$. Так как здесь второй сомножитель больше первого, то должно быть $x - y = 1$ и $x^2 + xy + y^2 = p$, откуда $p = x^3 - (x - 1)^3 = 3x^2 - 3x + 1$.

Таким образом, простое число p является разностью двух кубов натуральных (и притом последовательных) чисел тогда и только тогда, когда оно имеет вид $3x(x - 1) + 1$, где x — натуральное число, большее единицы.

Высказано предположение, что таких простых чисел существует бесконечно много. Для $x = 2, 3, 4, 5$ мы получаем здесь простые числа $7 = 2^3 - 1^3$, $19 = 3^3 - 2^3$,

---

[1]) См. W. Sierpiński, Teoria liczb, II, Warszawa, 1959, str. 338, 446.

$37 = 4^3 - 3^3$, $61 = 5^3 - 4^3$; для $x = 6$ получаем составное число $91 = 7 \cdot 13$; для $x = 7$ — простое число $127 = 7^3 - 6^3$; для $x = 8$ и $x = 9$ — составные числа $169 = 13^2$ и $217 = 7 \cdot 31$; для $x = 10, 11, 12$ — простые числа $271 = 10^3 - 9^3$, $331 = 11^3 - 10^3$, $397 = 12^3 - 11^3$; для $x = 13$ — составное число $469 = 7 \cdot 67$; для $x = 14$ и 15 — простые числа $547 = 14^3 - 13^3$ и $631 = 15^3 - 14^3$; для $x = 16$ и $x = 17$ — составные числа $721 = 7 \cdot 103$ и $817 = 19 \cdot 43$; для $x = 18$ — простое число $919 = 18^3 - 17^3$.

Итак, все простые числа < 1000, являющиеся разностями двух кубов натуральных чисел, суть следующие: 7, 19, 37, 61, 127, 271, 331, 397, 547, 631 и 919.

Легко можно доказать, что существует бесконечное множество простых чисел, не являющихся разностями двух кубов натуральных чисел. В самом деле, мы доказали, что каждое простое число, являющееся разностью двух кубов натуральных чисел, есть число вида $3x(x-1)+1$, где x — натуральное число > 1. Но из двух последовательных натуральных чисел $x-1$ и x одно всегда четное. Следовательно, наше простое число должно быть вида $6k+1$. Но, согласно теореме 12, существует бесконечно много простых чисел вида $6k+5$, ни одно из которых, очевидно, не является числом вида $6k+1$ и, следовательно, не является разностью двух кубов натуральных чисел. Заметим, однако, что имеются составные числа вида $6k+5$, являющиеся разностями двух кубов натуральных чисел, например число $215 = 6 \cdot 35 + 5 = 6^3 - 1^3$. Можно также доказать, хотя это было бы труднее, что существует бесконечно много простых чисел вида $6k+1$, не являющихся разностями двух кубов натуральных чисел. Таковыми будут, например, простые числа 31, 67, 103, 139, 157.

Высказано предположение, что простых чисел, являющихся суммами трех кубов натуральных чисел, существует бесконечно много. Высказано даже более сильное предположение, что уже простых чисел вида $x^3 + 2 = x^3 + 1^3 + 1^3$, где x — натуральное число, имеется бесконечно много. Таковы, например, простые числа $3 = 1^3 + 2$, $29 = 3^3 + 2$, $127 = 5^3 + 2$, $24\,391 = 29^3 + 2$. Можно доказать, что существует бесконечно много простых чисел, не являющихся суммами трех кубов целых чисел.

Легко доказать, что ни одно простое число >2 не является суммой двух n-х степеней натуральных чисел, где n есть нечетное число, большее единицы (доказательство аналогично изложенному выше для случая $n=3$). Заметим еще, что К. Ф. Рот в 1951 г. доказал, что каждое достаточно большое натуральное число является суммой восьми кубов натуральных чисел, из которых по крайней мере семь — кубы простых чисел.

21. Квадратичные вычеты

Если p — простое число, то квадратичным вычетом для числа p называется каждое целое число r, для которого существует целое число x такое, что число $x^2 - r$ делится на p. Другими словами, целое число r называется квадратичным вычетом для p, если существует квадрат целого числа, дающий при делении на p такой же остаток, как и r. Целые числа, не являющиеся квадратичными вычетами для p, называются квадратичными невычетами для p.

Для числа 2, очевидно, каждое целое число является квадратичным вычетом, так как если r — нечетное число, то $2|1^2 - r$, если же r — четное число, то $2|0^2 - r$.

Пусть теперь p — простое нечетное число. Выясним, сколько в последовательности 1, 2, 3, ..., $p-1$ имеется квадратичных вычетов для p.

Обозначим через r_x остаток от деления числа x^2 на p. Для целых x числа r_x будут, очевидно, всеми квадратичными вычетами для p (так как $p|x^2 - r_x$). Значит, в частности, квадратичным вычетом для p будет каждое из чисел

$$r_1, r_2, \ldots, r_{\frac{p-1}{2}} \qquad (1)$$

(число $\frac{p-1}{2}$ — натуральное, так как мы предположили, что p является простым нечетным числом). Числа последовательности (1), очевидно, отличны от нуля (так как ни одно из чисел $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ не делится на p) и, следовательно, являются числами последовательности 1, 2, 3, ..., $p-1$. Покажем, что они все различные. Предположим, что для некоторых натуральных i и j, где $i < j \leqslant \frac{p-1}{2}$, мы имеем $r_i = r_j$. Это означает,

что числа i^2 и j^2 дают при делении на p одинаковые остатки и, следовательно, число $j^2 - i^2 = (j-i)(j+i)$ делится на p. Но, в силу неравенства для i и j, числа $j-i$ и $j+i$ являются натуральными, причем оба они меньше p (так как $j+i<2j\leqslant p-1<p$). Таким образом, число p должно быть делителем произведения двух натуральных чисел, меньших p, что невозможно.

Итак, мы доказали, что $r_i \neq r_j$ для $i<j\leqslant\frac{p-1}{2}$. Следовательно, среди чисел последовательности 1, 2, ..., $p-1$ мы имеем по крайней мере $\frac{p-1}{2}$ квадратичных вычетов для p. Докажем теперь, что в этой последовательности никаких других квадратичных вычетов для p, кроме чисел (1), не содержится. Предположим для доказательства, что r есть число из последовательности 1, 2, ..., $p-1$, являющееся квадратичным вычетом для p. Тогда существует целое число a такое, что $p|a^2-r$. Отсюда следует, что $p|(a^2)^{\frac{p-1}{2}}-r^{\frac{p-1}{2}}$, т. е. $p|a^{p-1}-r^{\frac{p-1}{2}}$.

Далее, так как число r не делится на p, то и число a не делится на p. Поэтому, согласно теореме Ферма, имеем $p|a^{p-1}-1$. Следовательно, $p|(a^{p-1}-1)-\left(a^{p-1}-r^{\frac{p-1}{2}}\right)$, т. е. $p|r^{\frac{p-1}{2}}-1$. Таким образом, имеем $p|r_i^{\frac{p-1}{2}}-1$ для $i=1, 2, \ldots, \frac{p-1}{2}$. Но, согласно теореме Лагранжа, многочлен $x^{\frac{p-1}{2}}-1$ не может делиться на p для более чем $\frac{p-1}{2}$ различных значений x из последовательности 0, 1, 2, ..., $p-1$. Отсюда следует, что, кроме $\frac{p-1}{2}$ чисел (1), в последовательности 1, 2, ..., $p-1$ нет других чисел r, для которых $p|r^{\frac{p-1}{2}}-1$, т. е. в этой последовательности нет других квадратичных вычетов для p. Таким образом, доказана

Теорема 20. *Если p есть простое нечетное число, то в последовательности 1, 2, 3, ..., $p-1$ мы имеем точно $\frac{p-1}{2}$ квадратичных вычетов для p (и, очевидно, столько*

же квадратичных невычетов для p, так как $p-1-\frac{p-1}{2}=\frac{p-1}{2}$).

Из доказательства теоремы непосредственно следует, что для получения всех чисел последовательности 1, 2, ..., $p-1$, являющихся квадратичными вычетами для простого нечетного числа p, достаточно определить остатки от деления на p чисел

$$1^2,\ 2^2,\ 3^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2.$$

Таким путем мы найдем, например, что всеми квадратичными положительными вычетами для 13, меньшими 13, являются числа 1, 4, 9, 3, 12, 10 и, следовательно, невычетами для 13 (среди чисел >0 и <13) будут числа 2, 5, 6, 7, 8 и 11.

Как мы уже доказали выше, число r из последовательности 1, 2, ..., $p-1$ является квадратичным вычетом для простого нечетного p тогда и только тогда, когда число $r^{\frac{p-1}{2}}-1$ делится на p. Таким образом, если число a из указанной последовательности является квадратичным невычетом для p, то число $a^{\frac{p-1}{2}}-1$ не делится на p. Но, согласно теореме Ферма, число $a^{p-1}-1$ делится на p, а так как $a^{p-1}-1=\left(a^{\frac{p-1}{2}}-1\right)\times\left(a^{\frac{p-1}{2}}+1\right)$, причем первый сомножитель правой части ие делится на p, то должен делиться второй сомножитель, т. е. $p\mid a^{\frac{p-1}{2}}+1$. Следовательно, число a из последовательностн 1, 2, ..., $p-1$ является квадратичным вычетом для простого нечетного числа p, если $p\mid a^{\frac{p-1}{2}}-1$, н невычетом, если $p\mid a^{\frac{p-1}{2}}+1$.

Заметим, что для составных чисел дело обстоит иначе. Напрнмер, для $n=15$ среди натуральных чисел <15 только пять (следовательно, меньше чем $\frac{n-1}{2}=7$) являются квадратичными вычетами для числа 15, именно числа 1, 4, 6, 9 и 10, а остальные 9 чисел являются квадратичными невычетами для числа 15. Среди натуральных чисел <8 только два, именно числа 1 и 4 являются квадратичными вычетами для числа 8.

Заметим еще, что А. Вале Винс нашел теорему, согласно которой *нечетное число n является простым тогда и только тогда, когда ни одно из чисел* $2^2, 3^2, 4^2, \ldots, \left(\frac{n-1}{2}\right)^2$ *при делении на n не дает в остатке ни* 0, *ни* 1.

Для простых чисел изучены также вычеты кубические, биквадратичные и высших степеней. Можно доказать, что для каждого нечетного числа n существует бесконечно много простых чисел p, для которых каждое целое число является вычетом n-й степени. Так, например, для чисел 5 и 11 каждое целое число является кубическим вычетом, для чисел же 5 и 7 каждое целое число является вычетом 5-й степени.

Доказательство того, что каждое целое число является вычетом 5-й степени для простого числа 7, вытекает непосредственно из следующих формул, которые легко можно проверить:

$$7|0^5-0,\quad 7|1^5-1,\quad 7|4^5-2,\quad 7|5^5-3,\quad 7|2^5-4,$$
$$7|3^5-5,\quad 7|6^5-6.$$

Можно доказать, что для простых чисел 5 и 17 каждое целое число является вычетом любой нечетной степени. Можно также доказать, что для того чтобы для простого числа p каждое целое число было вычетом любой нечетной степени, необходимо и достаточно, чтобы простое число p было вида $2^{2^k}+1$, т. е. чтобы оно было простым числом Ферма.

22. Числа Ферма

Числами Ферма называются числа вида $F_k = 2^{2^k}+1$, где $k = 0, 1, 2, \ldots$ Знаменитый математик XVII века П. Ферма предполагал, что все такие числа являются простыми. Это справедливо для $k = 0, 1, 2, 3, 4$, но Л. Эйлер в 1732 г. обнаружил, что число

$$F_5 = 2^{2^5}+1 = 4\,294\,967\,297,$$

имеющее 10 цифр, является составным: оно делится на 641. В настоящее время мы знаем уже 37 составных чисел F_k, именно для $k = 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18, 23, 36, 38, 39, 55, 58, 63, 73, 77, 81, 117, 125, 144, 150, 207, 226, 228, 260, 267, 268, 284, 316, 452, 1945$.

Среди этих 37 составных чисел F_k имеются такие, для которых нам известны их разложения на простые сомножители (например, F_5 и F_6), имеются такие, для которых мы не знаем этих разложений, но знаем разложения в произведения двух целых чисел >1 (например, F_{1945}), наконец, имеются и такие, для которых мы не знаем ни одного разложения в произведение двух целых чисел >1, хотя и знаем, что такое разложение существует (F_7, F_8, F_{13} и F_{14}).

Начнем с наибольшего из известных составных чисел Ферма, т. е. с числа F_{1945}. Оно имеет более чем 10^{582} цифр, и поэтому все их невозможно выписать. Однако, как уже было сказано ранее (§ 8), мы знаем наименьший простой делитель этого числа: $m = 5 \cdot 2^{1947} + 1$. Напрашиваются здесь два вопроса: 1) как найден этот делитель и 2) как можно убедиться, что число m, имеющее 587 цифр, является делителем числа F_{1945}, все цифры которого невозможно выписать.

Мы здесь, очевидно, не будем ни производить деления числа F_{1945} на число m, ни находить частное от этого деления. Совершенно иным путем мы убедимся, или, скорее всего, выясним, как можно убедиться в том, что число F_{1945} при делении на m дает в остатке нуль.

Обозначим для целого числа t через $\bar{t}$ остаток от деления t на m. Из определения числа $\bar{t}$ следует, что для каждого целого числа t будет $m \mid t - \bar{t}$. Определим теперь последовательность r_k ($k = 1, 2, \ldots$) посредством условий

$$r_1 = 2^2, \quad r_{k+1} = \overline{r_k^2} \quad \text{для} \quad k = 1, 2, \ldots \tag{1}$$

Докажем при помощи индукции, что

$$m \mid 2^{2^k} - r_k \quad \text{для} \quad k = 1, 2, \ldots \tag{2}$$

Формула (2), очевидно, справедлива для $k = 1$, так как $2^{2^1} - r_1 = 0$. Предположим, что она справедлива для некоторого натурального числа k. В таком случае, согласно (2), и подавно $m \mid 2^{2^{k+1}} - r_k^2$. Учитывая же, что $m \mid t - \bar{t}$ для $t = r_k^2$, имеем $m \mid r_k^2 - \overline{r_k^2}$. Затем находим $m \mid 2^{2^{k+1}} - \overline{r_k^2}$. Следовательно, согласно (1), $m \mid 2^{2^{k+1}} - r_{k+1}$. Итак, формула (2) доказана посредством индукции. Для $k = 1945$ имеем

$$m \mid F_{1945} - r_{1945} - 1,$$

откуда следует, что число F_{1945} при делении на m дает такой же остаток, как и число $r_{1945}+1$. Поэтому, чтобы исследовать, делится ли число F_{1945} на m, достаточно исследовать, делится ли на m число $r_{1945}+1$. Осмыслим теперь, какие действия нужно будет выполнить, чтобы подсчитать число r_{1945}. Из формул (1) следует, что числа $r_2, r_3, \ldots$ как остатки от деления на m все будут меньше m, так что каждое из них имеет не более чем 587 цифр. Таким образом, из формул (1) вытекает, что для вычисления числа r_{1945} необходимо осуществить 1944 возвышений в квадрат чисел, имеющих не более чем 587 цифр, и столько же делений этих квадратов (следовательно, чисел, имеющих не более чем 1175 цифр) на число m, имеющее 587 цифр. Это — действия, которые современные электронные машины в состоянии выполнить. Таким путем было подтверждено, что число F_{1945} делится на $m=5\cdot 2^{1947}+1$, а так как $F_{1945}>m$, что легко можно проверить, то заключаем, что число F_{1945} является составным.

Перейдем теперь к вопросу, как можно найти простой делитель m числа F_{1945}. Известна теорема, согласно которой каждый натуральный делитель числа F_n должен иметь вид $2^{n+2}k+1$, где k — целое неотрицательное число. Для $n=1945$ отсюда следует, что делителями числа F_{1945} могут быть только числа, принадлежащие арифметической прогрессии $2^{1947}k+1$, где $k=0, 1, 2, \ldots$ Для $k=0$ мы получаем тривиальный делитель 1. Для $k=1$ число $2^{n+2}+1=2^{1947}+1$ не является простым, так как, очевидно, делится на 3. Для $k=2$ число $2^{n+2}\cdot 2+1=2^{1948}+1=(2^4)^{487}+1$ делится на 2^4+1 и, следовательно, не является простым. Для $k=3$ число $2^{n+2}\cdot 3+1=2^{1947}\cdot 3+1$ является составным, делящимся на 5. В самом деле, $5|2^4-1$, откуда $5|2^{1944}-1$. Умножив правую часть последней формулы на $2^3\cdot 3$, найдем, что $5|2^{1947}\cdot 3-24$, откуда также $5|2^{1947}\cdot 3+1$. Для $k=4$ число $2^{n+2}\cdot 4+1=2^{1949}+1$ делится на 3, следовательно, является составным.

Таким образом, разыскивая простой делитель числа F_{1945}, мы должны делить его на $2^{1947}\cdot 5+1=m$. Как уже отмечалось, деление выполняется без остатка, и так как m — наименьшее целое число >1, являющееся делителем числа F_{1945}, то m — число простое.

Подобным образом можно исследовать другие числа Ферма. Исследование десятизначного числа F_5, относительно которого Ферма был убежден, что оно является простым, выполняется весьма просто. Делители числа F_5, как мы знаем, должны быть вида $2^7 \cdot k + 1$, или $128k + 1$. Для $k = 1$ мы получаем число 129, делящееся на 3, и следовательно, составное; для $k = 2$ получаем простое число 257, которое не является делителем числа F_5, в чем легко можно убедиться непосредственным делением. Для $k = 3$ мы получаем число 385, делящееся на 5 и, стало быть, составное. Для $k = 4$ получаем число $513 = 2^9 + 1$, делящееся на 3 и, следовательно, также составное. (Иначе, число $2^{32} = 4^{16} = (3 + 1)^{16} = (5 - 1)^{16}$ при делении и на 3, и на 5 дает в остатке 1, а значит, число F_5 дает в остатке 2, т. е. число F_5 не делится ни на 3, ни на 5 и поэтому не делится также ни на одно из чисел 129, 385 и 513.) Для $k = 5$ получаем простое число 641, относительно которого непосредственным делением легко можно убедиться, что оно является делителем числа F_5. Таким образом, только при помощи двух делений мы убеждаемся, что 641 является наименьшим простым делителем числа F_5.

Разделив число $F_5 = 4\,294\,967\,297$ на 641, мы получим в частном 6 700 417. Делители этого числа, будучи делителями числа F_5, должны быть вида $2^7k + 1$. Если это число составное, то оно имеет простой делитель, не больший, чем корень квадратный из него, и, значит, < 2600. Таким образом, для k мы имеем здесь неравенство $128k + 1 < 2600$, откуда $k < 21$, а с другой стороны, мы знаем, что должно быть $k > 4$, ибо наименьшим простым делителем числа F_5 является 641. Таким путем при помощи немногих делений подтверждено, что число 6 700 417 является простым, и, следовательно, получено разложение числа F_5 в произведение двух различных простых сомножителей.

Для числа F_6 найден делитель $2^8 \cdot 1071 + 1$ и, таким образом, подтверждено, что оно является составным.

Разыскать простой делитель числа F_n среди чисел арифметической прогрессии $2^{n+2}k + 1$ практически возможно только в том случае, если число F_n обладает не слишком большим простым делителем. В противном случае, подставляя вместо k даже очень много последовательных натуральных чисел, мы не натолкнемся на

такой делитель. Это имеет место, например, для чисел F_7 и F_8, из которых первое содержит 39, а второе 78 цифр. Мы не знаем ни одного простого делителя этих чисел, а также ни одного разложения их в произведения двух натуральных чисел, бо́льших единицы. Однако Дж. К. Морхед в 1905 г. доказал, что число F_7 является составиым, а в 1909 г. он же и А. Е. Вестерн доказали, что число F_8 также является составным. Доказательство основывалось иа следующей теореме.

Теорема 21. *Если число F_n является простым, то число $3^{2^{2^n-1}}+1$ делится на F_n.*

Докажем вначале следующее предложение.

Лемма. *Если k есть целое неотрицательное число и если число $p=12k+5$ является простым, то число $3^{6k+2}+1$ делится на p.*

Доказательство. Лемма, очевидно, справедлива для $k=0$, поэтому далее мы можем считать, что k является числом натуральным. Пусть $p=12k+5$. Возьмем произведение первых $6k+2$ натуральных чисел, делящихся на 3, и разобьем сомножители этого произведения на три группы, отнеся к первой группе первые $2k$ сомножителей, ко второй — следующие $2k+1$ сомножителей и к третьей — остальные $2k+1$ сомножителей.

Сомножители первой группы дают произведение $3\cdot 6\cdot 9\ldots 6k$.

Сомножители второй группы, если записать их в порядке убывания, дают произведение

$$(12k+3)\cdot 12k\cdot(12k-3)\ldots(6k+6)(6k+3),$$

которое, учитывая, что $p=12k+5$, можно написать в виде

$$(p-2)(p-5)(p-8)\ldots[p-(6k+2)].$$

Так как число сомножителей здесь нечетное $(2k+1)$, то последнее произведение после развертывания и объединения слагаемых, делящихся на p, даст нам число $pu-2\cdot 5\cdot 8\ldots(6k+2)$, где u есть некоторое целое число.

Сомножители третьей группы дают произведение

$$(12k+6)(12k+9)(12k+12)\ldots(18k+6)=$$
$$=(p+1)(p+4)(p+7)\ldots(p+6k+1)=$$
$$=pv+1\cdot 4\cdot 7\ldots(6k+1),$$

где v — натуральное число.

Таким образом, имеем $3 \cdot 6 \cdot 9 \ldots (18k+6) = 3 \cdot 6 \cdot 9 \ldots 6k \cdot [pu - 2 \cdot 5 \cdot 8 \ldots (6k+2)][pv + 1 \cdot 4 \cdot 7 \ldots (6k+1)] = pw - 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \ldots (6k+1) \cdot (6k+2) = pw - (6k+2)!$, где w — целое число.

Но $3 \cdot 6 \cdot 9 \ldots (18k+6) = (6k+2)!3^{6k+2}$. Отсюда мы заключаем, что число pw делится на $(6k+2)!$, следовательно, $pw = (6k+2)!t$, где t есть целое число. Но $6k+2 < 12k+5 = p$, и поэтому число $(6k+2)!$ не делится на p. Поскольку же произведение $(6k+2)!t$ делится на p, то t должно делиться на p, $t = ps$, откуда $w = (6k+2)!s$, где s есть целое число. Таким образом, имеем $3^{6k+2} = ps - 1$, откуда следует, что число $3^{6k+2} + 1$ делится на p, что и требовалось доказать.

Перейдем теперь к доказательству теоремы 21.

Доказательство. Пусть n есть некоторое натуральное число. Тогда имеем $2^n = 2m$, где m — натуральное число, $F_n - 1 = 4^m$, откуда следует, что число $F_n - 5$ делится на 4. С другой стороны, имеем $F_n - 1 = 4^m = (3+1)^m = 3t + 1$, где t — натуральное число. Отсюда $F_n - 5 = 3(t-1)$, так что число $F_n - 5$, делясь на 4, оказывается делящимся и на 3, следовательно, это число делится на 12, и поэтому $F_n = 12k + 5$, где k — целое число. Таким образом, согласно нашей лемме, если число F_n простое, то число $3^{6k+2} + 1 = 3^{(F_n-1)/2} + 1 = 3^{2^{n}-1} + 1$ делится на F_n.

Итак, теорема 21 доказана. Заметим попутно (хотя далее это нам и не понадобится), что можно доказать и теорему, обратную теореме 21.

Воспользуемся теперь теоремой 21 для доказательства того, что число F_7 является составным. Для этой цели достаточно показать, что число $3^{2^{127}} + 1$ не делится на число $F_7 = 340\,282\,366\,920\,938\,463\,463\,374\,607\,431\,768\,211\,457$.

Значит, достаточно вычислить остаток от деления числа $3^{2^{127}}$ на F_7. Число $3^{2^{127}}$ столь велико, что мы не можем выписать все его цифры, однако, чтобы подсчитать остаток, который оно дает при делении на F_7, можно поступить следующим образом. Число 3^{27} имеет 61 цифру, следовательно, его мы можем написать и подсчитать остаток r, который получается при делении этого числа на F_7 (теперь это уже нетрудно сделать, если прибегнуть к помощи электронной вычислительной машины, но для Морхеда в 1905 г. это было очень трудно, хотя

и возможно). Остаток r_1 от деления числа r^2 на число F_7 есть, очевидно, остаток от деления числа 3^{28} на число F_7. Подобным же образом остаток r_2 от деления числа r_1^2 на число F_7 есть остаток от деления числа 3^{2^2} на F_7. Продолжая этот процесс далее, дойдем до остатка r_{120} от деления числа $3^{2^{127}}$ на F_7. Таким путем найдем, что $r_{120} \neq F_7 - 1$, откуда следует, что число $3^{2^{127}} + 1$ не делится на F_7 и, значит, согласно теореме 21, число F_7 не является простым.

Аналогичным образом убеждаемся, что и число F_8 не является простым. Для каждого же из чисел F_n ($n = 9, 10, 11$ и 12), которые являются составными, мы знаем их простые делители, именно:

$$2^{16} \cdot 37 + 1 \mid F_9, \quad 2^{12} \cdot 11131 + 1 \mid F_{10}, \quad 2^{13} \cdot 39 + 1 \mid F_{11},$$
$$2^{14} \cdot 7 + 1 \mid F_{12}.$$

На основании теоремы 21, при помощи электронных вычислительных машин доказано, что F_{13}, имеющее 2467 цифр, и F_{14}, имеющее 4933 цифры, являются числами составными. Никаких простых делителей этих чисел мы не знаем.

Доказано, что числа F_{15} и F_{16} также составные, причем найдены их простые делители: $2^{21} \cdot 573 + 1 \mid F_{15}$, $2^{18} \cdot 3150 + 1 \mid F_{16}$.

Число F_{17} имеет более 30 тысяч цифр. Существующие же в настоящее время вычислительные машины не в состоянии выполнять десятки тысяч делений чисел, имеющих несколько десятков тысяч цифр, на числа, имеющие более 30 тысяч цифр. Таким образом, мы пока все еще лишены возможности применить теорему 21 к исследованию чисел F_{17} и F_{19}.

В 1953 г. для числа F_{16} был найден наименьший простой делитель $2^{18} \cdot 3150 + 1$ и тем самым была опровергнута гипотеза, согласно которой все числа бесконечной последовательности

$$2+1, \quad 2^2+1, \quad 2^{2^2}+1, \quad 2^{2^{2^2}}+1, \quad 2^{2^{2^{2^2}}}+1, \ldots$$

являются простыми (составное число F_{16} — пятый член этой последовательности). Мы не знаем, однако, имеется ли в этой последовательности бесконечно много простых чисел, а также имеется ли в ней бесконечно много составных чисел.

Заметим, что ни одно из чисел $2^{2^n+1}+1$, где n — натуральное, не является простым, так как оно больше 3 и делится на 3.

23. Простые числа видов n^n+1, $n^{n^n}+1$ и некоторых других видов

В связи с числами Ферма напрашивается вопрос, сколько существует простых чисел вида n^n+1, где n — натуральное число. Предположим, что n — натуральное и что число n^n+1 является простым. Каждое натуральное n есть, как известно, число вида $n=2^k m$, где k — целое число $\geqslant 0$, а m — нечетное. Если бы m оказалось числом, большим единицы, то число $n^n+1=(n^{2^k})^m+1$ было бы $>n^{2^k}+1$ и делящимся на $n^{2^k}+1$ и, следовательно, было бы составным. Таким образом, должно быть $m=1$, а значит, $n=2^k$.

Если $k=0$, то $n=1$, и число $n^n+1=2$ является простым. Если же $k>0$, то $k=2^r s$, где r есть целое число $\geqslant 0$, а s — нечетное. Если бы было $s>1$, то число $n^n+1=2^{2^r sn}+1=(2^{2^r n})^s+1$ как число, большее чем $2^{2^r n}+1$ и делящееся на это число, было бы составным. Таким образом, должно быть $s=1$, следовательно, $k=2^r$, $n=2^{2^r}$ и, значит, $n^n+1=2^{2^r\cdot 2^{2^r}}+1=2^{2^r+2^r}+1=F_{r+2^r}$.

Итак, число n^n+1, где n — натуральное число >1, тогда и только тогда является простым, когда $n=2^{2^r}$, где r — целое число $\geqslant 0$, и F_{r+2^r} есть простое число.

Для $r=0$, так как число $F_1=5$ есть простое, мы получаем простое число $2^2+1=5$. Для $r=1$, так как число $F_3=257$ есть простое, получаем простое число $4^4+1=257$. Для $r=2$, так как F_6, как известно, есть число составное, делящееся на $2^8\cdot 1071+1$, мы не получим простого числа. Для $r=3$ мы также не получим простого числа, ибо F_{11} является числом составным, делящимся на $2^{13}\cdot 39+1$. Таким образом, если кроме чисел 2, 5 и 257 существует еще простое число вида n^n+1, то оно должно быть $\geqslant F_{20}>2^{2^{20}}>2^{10^6}>10^{3\cdot 10^5}$, т. е. должно быть числом, имеющим более чем триста тысяч цифр.

Следовательно, среди чисел вида $n^n + 1$ (где n — натуральное число), имеющих не более чем триста тысяч цифр, содержится только три простых числа: $1^1 + 1 = 2$, $2^2 + 1 = 5$ и $4^4 + 1 = 257$.

Принимая это во внимание, можно рискнуть высказать гипотезу о том, что не существует простых чисел вида $n^n + 1$, где n — натуральное число, кроме трех: 2, 5 и 257. Следует, однако, заметить, что из этой гипотезы вытекало бы, что существует бесконечно много чисел Ферма, являющихся составными: таковыми были бы числа F_{r+2^r} для $r = 4, 5, 6, \ldots$, т. е. числа F_{20}, F_{37}, F_{70}, F_{135}, F_{264}, F_{521}, F_{1034}, ... Ни об одном из этих чисел, однако, до сих пор не доказано, что оно является составным.

Рассмотрим теперь, что известно о простых числах вида $n^{n^n} + 1$. Имеем $1^{1^1} + 1 = 2$, $2^{2^2} + 1 = 17$. Легко доказать, что если число $n^{n^n} + 1$, где n — натуральное число > 1, является простым, то при некотором целом $r \geqslant 0$ должно быть $n = 2^{2^r}$, следовательно, $n^{n^n} + 1 = F_{r+2^r+2^{2^r}}$

Для $r = 0$ мы получаем простое число $F_2 = 17$, для $r = 1$ — число F_9, о котором известно, что оно является составным, делящимся на $2^{16} \cdot 37 + 1$. Для $r = 2$ получаем число F_{66}, которое, как легко можно доказать, имеет более чем 10^{18} цифр. Отсюда следует, что

Среди чисел, имеющих не более чем миллиард миллиардов цифр, существует только два простых числа вида $n^{n^n} + 1$, *где* n — *натуральное число, именно* 2 *и* 17.

Рассмотрим также, какие из чисел вида $n \cdot 2^n + 1$, где $n = 1, 2, 3, \ldots$, являются простыми (это так называемые числа Каллена). Кроме числа 3 (для $n = 1$), мы знаем еще только одно такое простое число для $n = 141$. Вопрос, сколько имеется таких простых чисел, остается открытым.

Легко доказать, что не существует других простых чисел вида $2^n + 1$, кроме простых чисел Ферма. Действительно, если $n = 2^r m$, где m — нечетное число > 1, то число $2^n + 1 = (2^{2^r})^m + 1$ делится на меньшее число $2^{2^r} + 1 > 1$ и, следовательно, является составным. Из простых чисел вида $2^n + 1$, где $n = 1, 2, \ldots$, мы знаем, таким образом, только пять, именно для $n = 1, 2, 4, 8, 16$,

наименьшее же число этого вида, о котором мы не знаем, простое оно или нет, есть число $2^{8192}+1$. Следовательно, мы знаем также только четыре простых числа вида $2\cdot 2^n+1$, где n — натуральное число, именно для $n=1, 3, 7$ и 15. Зато мы знаем 19 простых чисел вида $3\cdot 2^n+1$, именно для $n=1, 2, 5, 6, 8, 12, 18, 30, 36, 41, 66, 189, 201, 209, 276, 353, 408, 438, 534$. Простых чисел вида $4\cdot 2^n+1$, где $n=1, 2, \ldots$, мы знаем только три: для $n=2, 6$ и 14. Простых же чисел вида $5\cdot 2^n+1$, где $n=1, 2\ldots$, мы знаем 12: для $n=1, 3, 7, 13, 15, 25, 39, 55, 75, 85, 127, 1947$.

Для каждого натурального числа $k\leqslant 100$, за исключением $k=47$ и $k=94$, мы знаем по крайней мере одно натуральное число n такое, что число $k\cdot 2^n+1$ является простым. Однако можно доказать, что существует бесконечно много таких натуральных чисел k, для которых каждое из чисел $k\cdot 2^n+1$ ($n=1, 2, \ldots$) является составным.

Займемся теперь простыми числами вида 2^m+2^n+1, где m и n — натуральные числа, $m>n$. Такими числами являются, например, $2^2+2+1=7$, $2^3+2+1=11$, $2^3+2^2+1=13$, $2^4+2+1=19$.

Неизвестно, существует ли бесконечное множество таких простых чисел. Зато легко доказать, что существует бесконечно много составных чисел указанного вида. Это вытекает, например, тотчас же из равенства $2^{2n}+2^{n+1}+1=(2^n+1)^2$ для $n=2, 3, \ldots$, либо из замечания, что для $k=1, 2, \ldots$ число $2^{4k+1}+2+1$ всегда делится на 5, число же $2^{2k}+2^{2l}+1$ при натуральных k и l всегда делится на 3. Имеем также разложение $2^{4k}+2^{2k}+1=(2^{2k}+2^k+1)(2^{2k}-2^k+1)$.

А. Рихнер установил, что для $n<24$ числа 2^n+3 являются простыми только для $n=1, 2, 3, 4, 6, 7, 12, 15, 16, 18$. Легко доказать, что среди чисел $2^{2^{2n}}+3$ имеется бесконечно много составных, а именно числа $2^{2^{2(3k+1)}}+3$ для $k=0, 1, 2, \ldots$ все делятся на 19. Числа же $2^{2^{2k+1}}+3$ для $k=0, 1, 2, \ldots$ все делятся на 7.

Заметим также, что $13\mid 2^{2^{2k}}-3$ для $k=1, 2, 3, \ldots$, следовательно, и каждое из чисел

$$2^{2^2}-3,\quad 2^{2^{2^2}}-3,\ldots$$

делится на 13 и, значит, является составным.

Мы не знаем, имеется ли среди чисел

$$2+3,\quad 2^2+3,\quad 2^{2^2}+3,\quad 2^{2^{2^2}}+3,\ \ldots$$

только конечное число простых. Зато легко можно доказать, что среди чисел

$$2^{2^2}+5,\quad 2^{2^{2^2}}+5,\ \ldots$$

нет ни одного простого, так как каждое из этих чисел делится на 7. Действительно, для натуральных k число $2^{2k}=(3+1)^k$ при делении на 3 дает в остатке 1, следовательно, $2^{2k}=3t+1$, где t — натуральное число. Отсюда $2^{2^{2k}}+5=2^{3t+1}+5=(7+1)^t\cdot 2+5$, что, очевидно, делится на 7.

Неизвестно, существует ли такое натуральное число k, для которого имеется бесконечно много простых чисел вида $2^{n_1}+2^{n_2}+\ldots+2^{n_k}+1$, где $n_1,\ n_2,\ \ldots,\ n_k$ суть натуральные числа.

Мы не знаем также, существует ли бесконечно много простых чисел вида 2^n+n^2, где n — натуральное число. Четырьмя наименьшими такими простыми числами являются $3=2^1+1^2, 17=2^3+3^2, 593=2^9+9^2$ и $32\,993=2^{15}+15^2$.

Как заметил А. Монковский, существует только одно простое число, именно число 5, вида 4^n+n^4, где n — натуральное. В самом деле, если $n>1$, то n не может быть числом четным. Пусть $n=2k+1$, где k — натуральное. Но тогда $4^n+n^4=4(2^k)^4+n^4=(2\cdot 2^{2k}-2^{k+1}n+n^2)(2\cdot 2^{2k}+2^{k+1}n+n^2)$ есть число составное.

А. Шинцель доказал, что для всякого натурального числа a, где $2\leqslant a\leqslant 2^{27}$, существует по крайней мере одно натуральное число $n\leqslant 15$ такое, что число $a^{2^n}+1$ является составным. Если бы, опираясь на этот факт, мы рискнули высказать гипотезу, что для всякого натурального $a>1$ существует по крайней мере одно натуральное n такое, что число $a^{2^n}+1$ оказывается составным, то из этой гипотезы вытекало бы существование бесконечного множества составных чисел Ферма, ибо для $a=2^{2^k}$ (где $k=1, 2, \ldots$) имеем $a^{2^n}+1=F_{n+k}$. (Заметим, что для $a=2^{2^{1945}}$ эту гипотезу еще не удалось подтвердить).

Легко доказать, что существует бесконечное множество натуральных чисел a, для которых все числа $a^{2^n}+1$, где $n = 1, 2, \ldots$, являются составными. Таковы, например, все числа $a = b^m$, где b — натуральное число >1, а m — нечетное число >1.

С другой стороны, мы не знаем ни одного натурального числа $a > 1$, для которого мы могли бы доказать, что среди чисел $a^{2^n}+1 (n = 1, 2, \ldots)$ существует бесконечно много простых.

Из гипотезы Шинцеля (о которой речь будет идти в § 30) вытекает, что для всякого натурального числа m существует такое натуральное число $a > 1$, что все m чисел $a^{2^n}+1$, где $n = 1, 2, \ldots, m$, являются простыми. Для $m = 4$ можно взять $a = 2$. Но трудно было бы найти такое число $a > 1$ для $m = 5$.

24. Три ошибочных теоремы Ферма

П. Ферма в своем письме к Мерсенну от 1641 г. высказал следующие три теоремы:

1. *Ни одно из простых чисел вида* $12k+1$ *не является делителем ни одного из чисел вида* 3^n+1.

2. *Ни одно из простых чисел вида* $10k+1$ *не является делителем ни одного из чисел вида* 5^n+1.

3. *Ни одно из простых чисел вида* $10k-1$ *не является делителем ни одного из чисел вида* 5^n+1.

Доказано, что ни одна из этих трех теорем не является справедливой. Первая потому, что, например, $61 \mid 3^5+1$, $241 \mid 3^{60}+1$, вторая потому, что $521 \mid 5^5+1$, третья потому, что $29 \mid 5^7+1$. Для каждой из этих трех теорем, как доказал А. Шинцель, существует бесконечно много простых чисел, для которых они неверны.

Таким образом, здесь положение несколько иное по сравнению с теоремой Ферма о том, что каждое из чисел $2^{2^n}+1$ $(n=1, 2, \ldots)$ является простым, где мы знаем только конечное число примеров, опровергающих эту теорему.

Кроме приведенных выше теорем, Ферма в указанном письме к Мерсенну сформулировал также теорему о том, что *ни одно простое число вида* $12k-1$ *не является делителем ни одного из чисел вида* 3^n+1. Эта теорема позднее была доказана.

25. Числа Мерсенна

Числами Мерсенна называются числа вида $M_n = 2^n - 1$, где $n = 1, 2, 3, \ldots$ Они представляют интерес с двух точек зрения. Во-первых, наибольшие известные нам простые числа являются числами Мерсенна и, во-вторых, при помощи чисел Мерсенна мы находим все так называемые совершеиные четные числа. (Совершенным числом называется натуральиое число, равное сумме всех своих натуральных делителей, меньших самого числа.) n-е число Мерсенна можно определить также как сумму n первых члеиов геометрической прогрессии $1, 2, 2^2, 2^3, 2^4, \ldots$

Таким образом, имеем

$$M_1 = 1,\ M_2 = 3,\ M_3 = 7,\ M_4 = 15,\ M_5 = 31,\ M_6 = 63,$$
$$M_7 = 127, \ldots$$

Как легко доказать, если индекс n числа M_n есть число составное, то и число M_n является составным. В самом деле, если $n = ab$, где a и b — натуральиые числа >1, то $2^a - 1 > 1$ и $2^n - 1 = 2^{ab} - 1 > 2^a - 1$, следовательно, число $2^{ab} - 1$, делящееся на $2^a - 1$, является составным.

Итак, если число M_n, где $n > 1$, простое, то и число n должио быть простым, но ие обязательно наоборот, так как, например, $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$.

Доказано, что если p — простое число, то каждый натуральный делитель числа M_p должен быть вида $2kp + 1$, где k — целое число $\geqslant 0$. Поэтому, например, делителями числа M_{11} являются числа $22k + 1$, где $k = 0, 1, 4$ и 93.

Точно так же делители числа $M_{101} = 2^{101} - 1$ должны быть вида $202k + 1$. К сожалению, до сих пор не найдено ни одного простого делителя числа M_{101} (очевидно, число k здесь очень велико), хотя другим путем (о чем речь будет идти поздиее) доказано, что число M_{101} составное и является произведением двух различных простых чисел.

Доказано, что если q есть простое число вида $8k + 7$, то $q \mid M_{\frac{q-1}{2}}$. Это позволило показать, что средн

чисел M_p, где p — простое число, многие являются составными. Например,

$$47 \mid M_{23},\ 167 \mid M_{83},\ 263 \mid M_{131},\ 359 \mid M_{179},\ 383 \mid M_{191},\ 479 \mid M_{239}.$$

Высказано предположение (до сих пор не доказанное), что таких составных чисел существует бесконечно много.

Мы знаем пока только 20 простых чисел Мерсеина. Это числа M_n для $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253$ и 4423. Восемь наибольших простых чисел Мерсенна были найдены в последнее десятилетие при помощи электронных вычислительных машин.

Покажем теперь, каким путем было доказано, что эти весьма большие числа Мерсенна являются простыми. Это стало возможным благодаря следующей теореме, доказанной ранее.

Теорема Люка—Д. Х. Лемера. *Число M_p, где p — простое нечетное число, тогда и только тогда есть простое, когда M_p является делителем $(p-1)$-го члена последовательности u_n $(n = 1, 2, \ldots)$, определенной условиями:*

$$u_1 = 4, \quad u_{n+1} = u_n^2 - 2 \quad \text{для} \quad n = 1, 2, \ldots$$

(стало быть, последовательности, первыми членами которой являются числа 4, 14, 194, 37634, ...).

Легко доказать, что $M_p \mid u_{p-1}$ тогда и только тогда, когда M_p является делителем $(p-1)$-го члена последовательности $r_n (n = 1, 2, \ldots)$, зависящей от M_p и определенной условиями: $r_1 = 4$, r_{n+1} является остатком от деления числа $r_n^2 - 2$ на M_p.

Таким образом, при доказательстве того, что число M_p есть простое или составное, нам приходится иметь дело только с возвышением в квадрат и последующим делением на M_p чисел, меньших чем M_p. В частности, для доказательства того, что число M_{101}, имеющее 31 цифру, является простым, нужно было бы убедиться в том, что $M_{101} \mid r_{100}$. После выполнения необходимых здесь вычислений было установлено, что число r_{100} не делится на M_{101}. Следовательно, число M_{101} составное.

Чтобы доказать, что число M_{3217}, имеющее 969 цифр, является простым, нужно было установить, что $M_{3217} \mid r_{3216}$. Для этого потребовалось произвести несколько тысяч возвышений в квадрат и затем делений на

M_{3217} чисел, имеющих не более чем 969 цифр, что современные машины в состоянии выполнить [1]).

Высказано предположение, что если число Мерсенна M_n является простым, то и число M_{M_n} является простым. Это справедливо для четырех наименьших простых чисел Мерсенна, но уже для пятого простого числа $M_{13} = 8191$, как показал в 1953 г. Д. Ю. Уилер, это неверно: число $M_{M_{13}} = 2^{8191} - 1$ (имеющее 2466 цифр) является составным [2]). Заметим, что ни одного простого делителя числа $M_{M_{13}}$ мы не знаем.

В 1957 г. доказано, что хотя числа M_{17} и M_{19} простые, числа $M_{M_{17}}$ и $M_{M_{19}}$ являются составными, делящимися соответственно на $1768(2^{17} - 1) + 1$ и $120(2^{19} - 1) + 1$.

Высказано также предположение (до сих пор неопровергнутое), что числа q_0, q_1, q_2, ..., где $q_0 = 2$, а $q_{n+1} = 2^{q_n} - 1$ для $n = 0, 1, 2, \ldots$, являются все простыми. Это справедливо для чисел q_n, где $n \leqslant 4$, но уже для q_5, имеющего, как легко подсчитать, более чем 10^{37} цифр, мы не в состоянии решить вопрос, простое оно или составное.

Мы уже упоминали о связи чисел Мерсенна с совершенными четными числами. Еще Евклид указал следующий способ получения всех совершенных четных чисел. Вычисляем последовательно суммы членов геометрической прогрессии 1, 2, 2^2, 2^3, ... Если такая сумма окажется простым числом, то, умножив ее на последнее слагаемое, получим совершенное число.

С другой стороны, известно, что все совершенные четные числа являются числами вида $2^{p-1}M_p$, где M_p есть простое число Мерсенна. (Справедливость этой теоремы была доказана лишь в XVIII в. Л. Эйлером.) Отсюда следует, что мы знаем столько совершенных четных чисел, сколько мы знаем простых чисел Мерсенна, т. е. в настоящее время 20 чисел.

---

[1]) Для доказательства того, что число M_{3217} является простым, шведская электронная вычислительная машина БЕСК в 1957 г. затратила $5\frac{1}{2}$ часов.

[2]) Доказательство последнего факта (при помощи теоремы Люка—Лемера) потребовало ста часов работы электронной вычислительной машины.

Наименьшим совершенным числом является число $2M_2 = 6$, наибольшим известным совершенным числом — число $2^{4422}(2^{4423} - 1)$. Чисел совершенных нечетных мы не знаем. Известно только, что если они существуют, то являются весьма большими.

Упомянем еще об одной гипотезе, относящейся к числам Мерсенна. Ф. Якобчик высказал предположение, что если p — простое число, то число Мерсенна M_p не делится ни на один квадрат простого числа. А. Шинцель поставил вопрос, существует ли бесконечное множество чисел Мерсенна, являющихся произведениями различных простых чисел.

26. Простые числа в различных бесконечных последовательностях

Вопрос, содержит ли данная бесконечная последовательность, определенная даже несложным способом, бесконечно много простых чисел, вообще говоря, весьма труден. Как мы уже говорили, мы не знаем, содержат ли последовательности $n^2 + 1$, $n! + 1$, $n! - 1$, $2^n + 1$, $2^n - 1$ (для $n = 1, 2, \ldots$) бесконечно много простых чисел. Мы не знаем также, содержит ли бесконечное множество простых чисел последовательность 1, 11, 111, 1111, ... Также обстоит дело и в случае так называемой последовательности Фибоначчи u_n ($n = 1, 2, \ldots$), определенной условиями

$$u_1 = u_2 = 1, \quad u_{n+2} = u_n + u_{n+1} \quad (n = 1, 2, 3, \ldots).$$

Первыми членами этой последовательности являются числа $u_1 = 1$, $u_2 = 1$, $u_3 = 2$, $u_4 = 3$, $u_5 = 5$, $u_6 = 8$, $u_7 = 13$, $u_8 = 21$, ...

Доказано, что числа u_n являются простыми для $n = 3, 4, 5, 7, 11, 13, 17, 23, 29, 43, 47$. Других простых чисел u_n мы пока не знаем. Наибольшее известное простое число u_n есть число $u_{47} = 2\,971\,215\,073$, имеющее 10 цифр. Можно доказать, что если $n \neq 4$ и число u_n является простым, то и число n должно быть простым, но не обязательно наоборот, так как, например, $u_2 = 1$, $u_{19} = 4181 = 37 \cdot 113$, $u_{31} = 1\,346\,269 = 557 \cdot 2417$.

Мы не знаем, имеется ли среди чисел u_p, где p — простое число, бесконечно много составных.

Рассмотрим также последовательность v_n ($n = 1, 2, \ldots$), определенную условиями

$$v_1 = 1,\ v_2 = 3,\ v_{n+2} = v_n + v_{n+1}\ (n = 1, 2, \ldots),$$

первыми членами которой являются числа 1, 3, 4, 7, 11, 18, ... Числа v_n являются простыми для $n = 2, 4, 5, 7, 8, 11, 13, 17, 19, 31, 37, 41, 47, 53, 61, 71$. Наибольшее известное простое число v_n есть число $v_{71} = 688\,846\,502\,588\,399$. Мы не знаем, существует ли бесконечно много простых чисел v_n.

Укажем здесь еще одну последовательность, которой в последние годы занималось несколько математиков. При ее построении исходим из последовательности всех нечетных чисел: 1, 3, 5, 7, 9, 11, 13, 15, ... Положим $u_1 = 1$; наименьшее число последовательности, большее u_1, есть 3, его мы и примем за u_2. Вычеркнем из нашей последовательности каждое третье число (т. е. числа, находящиеся на местах третьем, шестом, девятом и т. д.). Таким путем мы получим новую последовательность: 1, 3, 7, 9, 13, 15, 19, 21, 25, 27, ... Наименьшее число этой последовательности, большее u_2, есть 7, его мы и примем за u_3. Вычеркнув теперь из последней последовательности каждое седьмое число, получим последовательность 1, 3, 7, 9, 13, 15, 21, 25, 27, ... Наименьшее число этой последовательности, большее u_3, есть 9, его мы примем за u_4. Из полученной последовательности будем вычеркивать теперь каждое девятое число. Поступая так далее, получим бесконечную последовательность $u_1, u_2, \ldots$, у которой членами, меньшими ста, будут числа: 1, 3, 7, 9, 13, 15, 21, 25, 31, 33, 37, 43, 49, 51, 63, 67, 69, 73, 75, 79, 87, 93, 99.

Числа нашей последовательности названы счастливыми. Мы не знаем, имеется ли среди них бесконечно много простых. Подсчитано, что среди счастливых чисел, меньших 98 600, имеется 715 простых чисел.

27. Решение уравнений в простых числах.

Мы знаем много простых уравнений (даже первой степени), относительно которых неизвестно, имеют ли они бесконечное множество решений в простых числах.

Таково, например, уравнение $x + y = z$. Легко доказать, что вопрос, имеет ли это уравнение бесконечно много решений в простых числах x, y, z, равносилен вопросу, существует ли бесконечно много пар простых чисел близнецов. В самом деле, если p, q и r — простые числа такие, что $p + q = r$, то числа p и q, очевидно, не могут быть оба нечетными (так как тогда сумма их была бы числом четным >2 и, следовательно, составным). Следовательно, одно из чисел p и q, например число q, должно быть четным и потому равно 2. Но тогда числа p и $r = p + 2$ составили бы пару простых чисел близнецов. С другой стороны, если числа p и $r = p + 2$ составляют пару простых чисел близнецов, то числа $x = p$, $y = 2$, $z = p + 2$ являются простыми и дают решение уравнения $x + y = z$.

Мы не знаем, имеет ли уравнение $2x + 1 = y$ или уравнение $2x - y = 1$ бесконечно много решений в простых числах x, y (такое предположение высказано), хотя и известно много таких решений. Например, для уравнения $2x + 1 = y$ $(x, y) = (2, 5)$, $(3, 7)$, $(5, 11)$, $(11, 23)$, для уравнения же $2x - 1 = y$ $(x, y) = (2, 3)$, $(3, 5)$, $(7, 13)$, $(19, 37)$.

Дж. Г. ван дер Корпут доказал, что уравнение $x + y + 1 = z$ имеет бесконечное множество решений в простых числах x, y, z (ср. стр. 19).

Доказано, что уравнение $x + y = z + t$ имеет бесконечное множество решений в различных простых числах x, y, z, t, так же как и уравнение $x^2 + y^2 = z^2 + t^2$. Например, $7^2 + 19^2 = 11^2 + 17^2$. Легко доказать, что уравнение $x^2 + y^2 + z^2 = t^2$ не имеет ни одного решения в простых числах x, y, z, t.

Мы не знаем, существует ли бесконечное множество прямоугольных треугольников таких, чтобы длины их сторон были натуральными числами, из которых два — простые. Можно доказать, что этот вопрос равносилен вопросу, имеет ли уравнение $p^2 = 2q - 1$ бесконечно много решений в простых числах p и q. Примерами таких треугольников являются треугольники со сторонами $(3, 4, 5)$, $(5, 12, 13)$, $(11, 60, 61)$, $(19, 180, 181)$, $(29, 240, 241)$, $(61, 1860, 1861)$.

Легко находятся все решения уравнения $x^2 - 2y^2 = 1$ в простых числах x, y. В самом деле, если натуральные числа x, y удовлетворяют уравнению $x^2 = 2y^2 +$

$+1$, то x, очевидно, число нечетное, $x = 2k + 1$, где k — целое число, откуда $x^2 = 4k^2 + 4k + 1$, а следовательно, $y^2 = 2k(k + 1)$ и, стало быть, y есть число четное. Поэтому, если y является простым числом, то $y = 2$, откуда следует, что наше уравнение имеет одно только решение в простых числах: $x = 3$, $y = 2$.

Мы не знаем, сколько решений в простых числах x, y имеет уравнение $x^2 - 2y^2 = -1$. Такие решения известны, например, $x = 7$, $y = 5$ или $x = 41$, $y = 29$.

Легко доказать, что если n — натуральное число > 1, то уравнение $p^n + q^n = r^n$ не имеет решений в простых числах p, q, r.

До сих пор не доказано предположение Ферма, согласно которому если p — простое нечетное число, то уравнение $x^p + y^p = z^p$ не имеет решений в натуральных числах x, y, z. (Это доказано для простых нечетных чисел $p < 4002$.)

28. Магические квадраты, составленные из простых чисел

Магическим квадратом (в широком смысле) с n строками мы называем таблицу, составленную из n^2 различных натуральных чисел, выписанных в n строк (и столько же столбцов), такую, что суммы чисел каждой строки, каждого столбца и чисел, находящихся на каждой из главных диагоналей, одинаковы. Известны магические квадраты с тремя и четырьмя строками, составленные из одних простых чисел. Например, квадраты

569	59	449
239	359	479
269	659	149

17	317	397	67
307	157	107	227
127	277	257	137
347	47	37	367

В первом из этих квадратов суммы, о которых идет речь, все равны 1077; во втором — 798.

Высказано предположение, что для каждого натурального числа $n \geqslant 3$ существует бесконечно много магических квадратов (в широком смысле), составленных из n^2 различных простых чисел.

29. Несколько нерешенных задач, касающихся простых чисел

1. Мы не знаем, существует ли бесконечно много пар последовательных натуральных чисел, каждое из которых имеет только один простой делитель (как, например, пары 2 и 3, 3 и 4, 4 и 5, 7 и 8, 8 и 9, 16 и 17, 31 и 32). Нам известно только 26 таких пар, из которых наивысшей является пара $2^{4423} - 1$ и 2^{4423} (ср. далее 6).

Зато можно доказать, что уравнение $p^m - q^n = 1$, где p и q — простые числа, а m и n — натуральные числа >1, имеет только одно решение: $p = 3$, $q = 2$, $m = 2$, $n = 3$.

2. Мы не знаем, существует ли бесконечное множество троек последовательных натуральных чисел, каждое из которых является произведением двух различных простых чисел. (Примером такой тройки может служить тройка чисел: $33 = 3 \cdot 11$, $34 = 2 \cdot 17$, $35 = 5 \cdot 7$, а также тройка: $93 = 3 \cdot 31$, $94 = 2 \cdot 47$, $95 = 5 \cdot 19$.) Высказано предположение, что таких троек существует бесконечно много.

3. Мы не знаем, существует ли бесконечно много простых чисел p таких, что для каждого натурального $n < p - 1$ число 2^n при делении на p дает остаток, отличный от 1. (Такими являются, например, простые числа 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83.) Высказано предположение, что таких простых чисел p существует бесконечно много.

4. Мы не знаем, из каждого ли натурального числа $n \geqslant 10$ при изменении двух его цифр можно получить простое число. (Для двузначных чисел это очевидно. Для трехзначных чисел это вытекает, например, из того, что простыми являются числа 101, 211, 307, 401, 503, 601, 701, 809, 907.)

5. Мы не знаем, справедлива ли гипотеза А. Шинцеля, согласно которой для каждого вещественного числа $x \geqslant 117$ существует по крайней мере одно простое число p, содержащееся между x и $x+\sqrt{x}$. Эту гипотезу А. Шинцель проверил для всех чисел x таких, что $117 \leqslant x < 2 \cdot 10^7$.

6. Легко доказать, что среди любых шести последовательных натуральных чисел по крайней мере одно имеет хотя бы два различных простых делителя (так как всегда одно из них делится на 6 и, значит, имеет простыми делителями 2 и 3).

Можно также доказать, что среди каждых трех последовательных натуральных чисел >7 хотя бы одно имеет по крайней мере два различных простых делителя. Но мы не знаем, среди каждых ли двух достаточно больших последовательных натуральных чисел хотя бы одно имеет по крайней мере два различных простых делителя. Иными словами, мы не знаем, существует ли натуральное число m такое, что для $n \geqslant m$ хотя бы одно из натуральных чисел n и $n+1$ имеет по крайней мере два различных простых делителя. Мы знаем только, что если такое m существует, то должно быть $m \geqslant 2^{4423}$, ибо из чисел $2^{4423}-1$ и 2^{4423} каждое имеет только один простой делитель. Доказано, что если такое число m существует, то существует только конечное число простых чисел Ферма и только конечное число простых чисел Мерсенна.

30. Гипотеза А. Шинцеля

Многочлен от переменной x с целыми коэффициентами мы называем неприводимым, если он не является произведением двух многочленов с целыми коэффициентами, степени которых меньше степени рассматриваемого многочлена.

Относительно многочлена $f(x)$ с целыми коэффициентами напрашивается вопрос, когда такой многочлен при натуральных значениях x дает бесконечно много простых чисел. Легко доказать, что необходимым условием этого является требование, чтобы многочлен был неприводимым. Однако такое условие не является достаточным, ибо, как легко доказать, многочлен x^2+x+2

является неприводимым, но ни при одном натуральном значении x не дает простого числа: для каждого натурального x его значение есть число четное >2.

Легко также доказать, что кроме неприводимости многочлен $f(x)$ должен удовлетворять еще следующему условию: не существует ни одного натурального числа >1, которое являлось бы делителем числа $f(x)$ при каждом целом значении x.

Являются ли эти условия достаточными для того, чтобы многочлен с целыми коэффициентами, где коэффициент при наивысшей степени x положителен, давал бесконечно много простых чисел для натуральных x? В прошлом веке В. Я. Буняковский высказал предположение, что это так. Из данной гипотезы сейчас же следует, что существует бесконечно много простых чисел вида x^2+1, где x — натуральное число. Из нее же следует также, что существует бесконечно много натуральных чисел x, для которых x^2+x+41 является числом простым.

Из гипотезы А. Шинцеля, о которой речь идет ниже, следует, что для каждого натурального числа n существует бесконечно много натуральных чисел x, для которых все четыре числа $x^{2^n}+1$, $x^{2^n}+3$, $x^{2^n}+7$, $x^{2^n}+9$ простые.

А. Шинцель высказал следующую общую гипотезу **P**.

Если s — натуральное число, $f_1(x)$, $f_2(x)$, ..., $f_s(x)$ — многочлены с целыми коэффициентами, имеющие при наивысших степенях x положительный коэффициент, неприводимые и удовлетворяющие следующему условию **S**: *не существует натурального числа >1, которое являлось бы делителем произведения $f_1(x)f_2(x)\dots f_s(x)$ для каждого целого значения x, — то существует бесконечно много натуральных чисел x, для которых каждое из чисел $f_1(x)$, $f_2(x)$, ..., $f_s(x)$ является простым.*

Пусть, в частности, $s=2$, $f_1(x)=x$, $f_2(x)=x+2k$, где $2k$ — данное натуральное четное число. Имеем здесь

$$f_1(1)f_2(1)=1+2k,\quad f_1(-1)f_2(-1)=1-2k.$$

Если бы существовало натуральное число $d>1$ такое, что $d\mid f_1(x)f_2(x)$ для каждого целого числа x, то должно было бы быть $d\mid 2k-1$ и $d\mid 2k+1$, что невоз-

можно, ибо, как известно, два последовательных нечетных числа $2k - 1$ и $2k + 1$ не имеют ни одного общего делителя, большего единицы. Таким образом, условие **S** здесь выполнено, и из гипотезы **P** следует, что существует бесконечно много натуральных чисел x таких, что числа $f_1(x)$ и $f_2(x)$ являются простыми, стало быть, $x = p$, $x + 2k = q$, где p и q — простые числа, откуда $2k = q - p$. Поэтому из гипотезы **P** следует, что каждое натуральное четное число может быть представлено бесконечным числом способов в виде разности двух простых чисел. В частности, для $k = 1$ отсюда следует существование бесконечного множества пар простых чисел близнецов.

Из гипотезы **P** А. Шинцеля можно вывести еще много других теорем о простых числах, которые до сих пор не доказаны.

ИМЕННОЙ УКАЗАТЕЛЬ

Адамар (Hadamard J.) 29

Бейкер (Baker C. L.) 16
Бертран (Bertrand J.) 14
Бнджер (Beeger N. G. W. H.) 38
Бреднхин Б. М. 34
Буняковский В. Я. 86

Вале Винс А. 65
Валле-Пуссен (Vallée Poussin de la Ch.) 29
Ван дер Корпут (Van der Corput J. G.) 19, 82
Вестерн (Western A. E.) 44, 69
Вильсон (Wilson J.) 47—51
Виноградов И. М. 18
Вороной Г. Ф. 7

Гарди (Hardy G. H.) 20
Гильбрайт (Gilbreath N. L.) 21, 22
Голашевский (Gołaszewski S.) 18
Голубев В. А. 32, 35
Гольдбах Хр. 18, 19
Горжелевский (Gorzelewski A.) 44
Грунберггер (Gruenberger F. J.) 16

Джуга (Giuga G.) 39
Дирихле (Dirichlet P. G. Lejeune) 42

Евклид 13, 79

Каллен (Cullen J.) 73
Кантор (Cantor M.) 35
Крайчик (Kraitchik M.) 27
Кулик (Kulik J. F.) 16

Лагранж (Lagrange J. L.) 45—48, 63
Ландау (Landau E.) 30
Лейбниц (Leibniz G. W.) 49, 50
Лемер Д. Н. (Lehmer D. N.) 16
Лемер Д. Х. (Lehmer D. H.) 38, 44, 78, 79
Линник Ю. В. 20
Литтлвуд (Littlewood J. E.) 20, 41
Лич (Leech J.) 41
Лохер-Эрнст (Locher-Ernst L.) 29
Лузин Н. Н. 8
Люка (Lucas) 78, 79

Мазуркевич (Mazurkiewicz S.) 8
Мерсенн (Mersenne M.) 76—80, 85
Мозер (Moser L.) 28, 49
Монковский (Mąkowski A.) 19, 75.
Морхед (Morehead J. C.) 69, 70

Ньютон (Newton I.) 36

Полетти (Poletti L.) 16
Портер (Porter R. J.) 16

Рихерт (Richert H. E.) 28
Рихнер (Richner A.) 74

Робинзон (Robinson R. M.) 14
Рот (Roth K. F.) 62

Серпинский (Sierpiński W.) 7—9, 10, 14, 27, 29, 44, 45, 60
Скуля (Skula L.) 45

Туран (Turán P.) 31

Уилер (Wheeler D. J.) 79

Ферма (Fermat P.) 35, 39, 40, 48, 49, 53, 63—66, 68, 72, 73, 75, 76, 83, 85
Ферье (Ferrier A.) 32
Фибоначчи (Fibonacci L.) 80

Чебышев П. Л. 14, 44
Човла (Chowla I.) 59

Шерк (Scherk H. J.) 30
Шинцель (Schinzel A.) 9, 18, 31, 38, 44, 50, 75, 76, 80, 85—87.

Эйлер Л. 33, 65, 79
Эратосфен 15
Эрдеш (Erdös P.) 31, 55

Якобчик (Jakóbczyk F.) 80
Янишевский (Janiszewski Z.) 8

ОГЛАВЛЕНИЕ

И. Г. Мельников. Вацлав Серпинский (*к восьмидесятилетию со дня рождения*) 7
От переводчика 9

Предисловие 10

1. Что такое простые числа? 11
2. Простые делители натуральных чисел 12
3. Сколько существует простых чисел? 13
4. Как можно найти все простые числа, меньшие данного числа? 15
5. Простые числа близнецы 16
6. Гипотеза Гольдбаха 18
7. Гипотеза Гильбрайта 21
8. Разложение натурального числа на простые сомножители . . 22
9. Какими цифрами могут начинаться и заканчиваться простые числа? 27
10. Число простых чисел, не превосходящих данное число . . 28
11. Некоторые свойства n-го по порядку простого числа . . . 30
12. Многочлены и простые числа 32
13. Арифметические прогрессии, образованные из простых чисел 34
14. Малая теорема Ферма 35
15. Доказательство теорем, согласно которым имеется бесконечно много простых чисел каждого из видов $4k+1$, $4k+3$ и $6k+5$ 40
16. Некоторые гипотезы относительно простых чисел 43
17. Теорема Лагранжа 45
18. Теорема Вильсона 47
19. Разложение простого числа на сумму двух квадратов . . . 51
20. Разложение простого числа на разность двух квадратов и другие разложения 57
21. Квадратичные вычеты 62

22. Числа Ферма 65
23. Простые числа видов n^n+1, $n^{n^n}+1$ и некоторых других видов 72
24. Три ошибочных теоремы Ферма 76
25. Числа Мерсенна 77
26. Простые числа в различных бесконечных последовательностях 80
27. Решение уравнений в простых числах 81
28. Магические квадраты, составленные из простых чисел . . . 83
29. Несколько нерешенных задач, касающихся простых чисел 84
30. Гипотеза А. Шинцеля 85
Именной указатель 88

Вацлав Серпинский

Что мы знаем и чего не знаем
о простых числах

Л., Физматгиз, 1963 г., *92* стр. с *илл.*

Редактор *Н. М. Розенгауз*

Техн. редактор *А. А. Лукьянов*

Корректор *Л. А. Любович*

Сдано в набор 9/V 1963 г. Подписано к печати 3/IX 1963 г. Бумага $84\times108^{1}/_{32}$. Физ. печ. л. 2,875. Усл. печ. л. 4,72. Уч.-изд. л. 4,71. Тираж 100 000 экз. Цена книги 14 коп. Заказ № 1390.

Государственное издательство
физико-математической литературы
Москва, В-71, Ленинский проспект, 15

Типография № 2 им. Евг. Соколовой
УЦБ и ПП Леисовнархоза.
Ленинград, Измайловский пр., 29.