DAUGAVPILS PEDAGOĢISKAIS INSTITŪTS

MATEMĀTIKAS MĀCĪŠANAS JAUTĀJUMI

3. laidiens

IZDEVNIECĪBA «ZVAIGZNE»
RĪGA 1976

ДАУГАВПИЛССКИЙ ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ

ВОПРОСЫ ПРЕПОДАВАНИЯ МАТЕМАТИКИ

Выпуск 3

ИЗДАТЕЛЬСТВО «ЗВАЙГЗНЕ»
РИГА 1976

Искомые функции имеют следующий вид:

$$h(x) = \begin{cases} x, & \text{если } 0 \leqslant x < 1; \\ 2, & \text{если } 1 \leqslant x \leqslant 2. \end{cases}$$

$$S(x) = \begin{cases} \dfrac{x^2}{2}, & \text{если } 0 \leqslant x < 1; \\ \dfrac{1}{2} + 2(x-1), & \text{если } 1 \leqslant x \leqslant 2. \end{cases}$$

Рассмотрение таких упражнений даст более полное представление о функции и подготовит учащихся к лучшему восприятию понятия непрерывности.

В заключение отметим, что много интересных задач, связанных с построением графиков разнообразных функций, можно рассматривать на факультативных занятиях и в кружковой работе. Для этого можно использовать пособия [5], [6], [7].

ЛИТЕРАТУРА

1. Алгебра. Учебное пособие для 6-го класса средней школы. Под ред. А. И. Маркушевича. М., «Просвещение», 1973. 224 с.

2. Алгебра. Учебное пособие для 7-го класса средней школы. Под ред. А. И. Маркушевича. М., «Просвещение», 1974. 256 с.

3. Алгебра. Учебное пособие для 8-го класса средней школы. Под ред. А. И. Маркушевича. М., «Просвещение», 1973. 256 с.

4. *Кудрявцев С. В.* Дидактические материалы по алгебре для 8-го класса. М., «Просвещение», 1973. 240 с.

5. *Гурский И. П.* Функции и построение графиков. М., Учпедгиз, 1961. 216 с.

6. *Сивашинский И. Х.* Элементарные функции и графики. М., «Наука», 1968. 280 с.

7. *Гельфанд М. Б., Шейнцвит Р. П.* Построение графиков функций, связанных с целой и дробной частью действительного числа. — «Математика в школе», 1970, № 3, с. 68—72.

Ш. Х. Михелович

О простых и составных числах

(Материалы для бесед с учащимися)

I. ПРОСТЫЕ ЧИСЛА. ОСНОВНОЙ ЗАКОН АРИФМЕТИКИ.

1) Каждое натуральное число делится на 1 и на себя.

$$a|1 \text{ и } a|a.$$[1]

Но существуют числа (мы будем подразумевать только натуральные числа), которые, кроме указанных делителей, других не имеют. Все такие числа, кроме 1, называются простыми, остальные — составными.

Простыми числами являются:

$$2, 3, 5, 7, 11, \ldots$$

Составными числами являются, например,

$$4=2\cdot2;\ 6=2\cdot3;\ 8=2\cdot4;\ 9=3\cdot3 \text{ и др.}$$

Число 1 занимает особое положение: оно имеет единственный делитель 1 и этот делитель совпадает с самим числом. Поэтому оказывается удобным число 1 не считать ни простым, ни составным.

Таким образом, 2 является наименьшим простым числом, в то же время число 2 является единственным четным простым числом, потому что все остальные четные числа больше двух и делятся на 2.

2) Как можно было бы простые и составные числа охарактеризовать иначе, чем это сделано в п. 1?

Простые числа — это натуральные числа, которые имеют два

[1] Если a делится на b, то будем это записывать так: $a|b$, если не делится — $a \nmid b$.

и только два различных делителя, а составные числа — это такие, которые имеют более двух различных делителей.

При таком определении число 1 автоматически выпадает из множества как простых, так и составных чисел.

3) Простые и составные числа можно охарактеризовать следующими записями:

а) p — простое, если $p>1$ и из $p|n \Rightarrow$[1] $n=1$ или $n=p$;

б) a — составное, если существует n, $1<n<a$, причем $a|n$.

4) Простые числа имеют большое значение, так как они являются как бы кирпичиками, при помощи которых умножением можно построить все остальные числа, кроме 1. Поэтому эти остальные числа и называются составными. Примеры: $6=2\cdot 3$, $15=3\cdot 5$.

5) Покажем, что каждое составное число можно действительно получить умножением простых чисел. Иначе этот факт выражают так: каждое составное число можно представить как произведение простых множителей, или каждое составное число можно разложить на простые множители.

Здесь надо обратить внимание на то, что наименьший делитель числа, отличный от 1, обязательно является простым. В самом деле, если бы этот делитель был составным, то он имел бы делитель, меньший, чем он сам, на который также делилось бы исходное число. Получилось бы противоречие.

Составное число можно разложить на простые множители, последовательно отделяя наименьший простой множитель.

Пример: $60=2\cdot 30$, $30=2\cdot 15$, $15=3\cdot 5$; таким образом,

$$60=2\cdot 2\cdot 3\cdot 5,$$

или

$$60=2^2\cdot 3\cdot 5.$$

Разложение на простые множители в последней форме называют также каноническим представлением.

В общем случае каноническое представление числа N имеет вид

$$N=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}, \qquad (1)$$

где $p_1, p_2, \dots, p_k$ — различные простые числа.

О простом числе говорят также, что оно разложимо на простые множители (при этом допускается, что в выражении (1) k может быть равно 1 и $\alpha_1=1$). Получается, что каждое натуральное число можно представить в канонической форме, если $N>1$.

[1] Знак $\Rightarrow$ означает: следует, вытекает, влечет за собой.

В выражении (1) можно изменить порядок сомножителей, но выделить из числа N, имеющего каноническое разложение (1), другие простые множители, кроме $p_1, p_2, \dots, p_k$, или изменить показатели степеней $\alpha_1, \alpha_2, \dots, \alpha_k$ невозможно. В этом смысле говорят, что натуральное $N>1$ имеет единственное разложение на простые множители. Этот так называемый основной закон арифметики мы доказывать не будем, но на частных примерах легко проверить его справедливость. Так, например, из 60 нельзя выделить другие простые множители, кроме 2, 3 и 5; нельзя также найти для 60 каноническое разложение, в котором простые множители 2, 3 и 5 имели бы иные показатели степени, чем в указанном выше разложении.

С другой стороны, нетрудно указать на числовые системы, для которых однозначная разложимость на простые множители не имеет места. Рассмотрим, например, числовую систему:

$$E=\{1, 2, 4, 6, 8, \dots\}.$$

Если в E считать «простыми» числа 2, 6, 10, ..., которые больше 1 и делятся в E только на 1 и самих себя, то легко убедиться, что в E основной закон нарушен.

Действительно, здесь, например,

$$36=6\cdot 6=2\cdot 18,$$

причем числа 2, 6, 18 являются «простыми».

6) Для нахождения канонического разложения числа N можно начать с отделения наименьшего простого множителя. С этой целью испытываем, не подходит ли в качестве делителя одно из простых чисел возрастающей последовательности 2, 3, 5, ... Спрашивается, как долго следует продолжать испытания?

Замечаем, что при увеличении делителя неполное частное уменьшается.

Так, например, для $N=131$ имеем:

$$131=2\cdot 65+1;$$
$$131=3\cdot 43+2;$$
$$131=5\cdot 26+1;$$
$$131=7\cdot 18+5;$$
$$\underline{131=11\cdot 11+10;}$$
$$131=13\cdot 10+1.$$

Нетрудно понять, что как только неполное частное становится меньше делителя, испытания можно прекратить. В самом деле, если бы в дальнейшем оказалось, что для некоторого простого числа p $131=pa$, где $1<a<13<p$, то это означало бы, что число 131 имеет делитель a $(a>1)$, меньший числа 13; следовательно, оно имело бы и простой делитель, меньший 13, но при составлении таблицы мы ведь убедились в том, что 131 не имеет простых делителей, меньших 13.

Если указанные испытания прошли безрезультатно, то этим одновременно устанавливается, что N — простое число. Так, например, составленная выше таблица показывает, что 131 — простое число.

Простоту числа можно проверить иначе. Пусть p — наименьший простой делитель составного N. Тогда $N=pa$, где $a\geqslant p$. Отсюда $pa\geqslant p^2$, так что $N\geqslant p^2$, а $p\leqslant\sqrt{N}$.

Таким образом, наименьший простой делитель составного N не превосходит $\sqrt{N}$.

Например: простыми числами, не превосходящими $\sqrt{131}$, являются 2, 3, ..., 11, но они не делят 131, поэтому это число является простым.

7) Естественно, возникает вопрос, сколько имеется всего простых чисел. На этот вопрос ответил уже древнегреческий ученый Евклид (III в. до н. э.). В своем знаменитом труде «Начала» он доказал, что ряд простых чисел не ограничен, т. е. продвигаясь по бесконечному ряду натуральных чисел, мы будем снова и снова встречаться с простыми числами.

Как он это доказал? Коротко можно сказать: Евклид доказал, что для каждого простого числа существует другое простое, большее первого.

Покажем, например, что существует простое число, которое больше 7 (для других простых чисел рассуждения по существу не отличаются).

Для этого составим число

$$2\cdot3\cdot5\cdot7+1=211,$$

т. е. произведение простых чисел до семи плюс один.

Число $2\cdot3\cdot5\cdot7=210$ делится на каждое из чисел 2, 3, 5 и 7, но следующее за ним число 211 ни на одно из них делиться не может, всегда остается остаток 1. Отсюда следует, что 211 либо само простое число, либо имеет простой делитель, который больше 7. Во всяком случае, существует простое число, большее 7.

8) Древнегреческий ученый Эратосфен, который жил несколько позже Евклида, изобрел способ, как найти простые числа от 1 до N. Этот способ, напоминающий действие решета, получил название решета Эратосфена.

Рассмотрим, как с помощью этого способа можно найти простые числа, например, до 60.

С этой целью выписываем все натуральные числа от 2 до 60. Из них вычеркиваем каждое второе число после простого числа 2. Первым незачеркнутым числом остается простое число 3; теперь вычеркиваем каждое третье число после 3 (причем считаем и те числа, которые вычеркнуты ранее). Первым незачеркнутым числом теперь оказывается число 5. Это число простое. Даже если бы мы этого заранее не знали, мы могли бы это утверждать. В самом деле, если бы это число было составным, то оно было бы кратным некоторому предшествующему простому числу, но кратные предшествующим простым числам 2 и 3 уже исключены.

Число 5 оставляем нетронутым, но вычеркиваем каждое пятое число после 5 (причем опять считаем и те числа, которые зачеркнуты ранее) и т. д.

После вычеркивания всех кратных 7 в таблице остаются все простые числа до 60. Нет надобности искать в таблице кратные 11 (первому незачеркнутому числу после 7), так как $11\cdot7>60$, а меньшие кратные 11 уже исключены раньше.

Следует вообще заметить, что первое число после простого числа p, которое приходится исключать, равно квадрату этого числа. Так, например, первое число, которое мы исключаем после нахождения простого числа 7, — это 49. Дело в том, что предыдущие кратные 7 (например, 35) являются кратными меньшим простым числам и как таковые уже исключены раньше.

Для $N=60$ решето Эратосфена имеет вид:

$$\begin{array}{cccccccccccccccc}
 & 2 & 3 & \overline{4} & 5 & \overline{6} & 7 & \overline{8} & \overline{9} & \overline{10} & 11 & \overline{12} & 13 & \overline{14} & \overline{15} \\
\overline{16} & 17 & \overline{18} & 19 & \overline{20} & \overline{21} & \overline{22} & 23 & \overline{24} & \overline{25} & \overline{26} & \overline{27} & \overline{28} & 29 & \overline{30} \\
31 & \overline{32} & \overline{33} & \overline{34} & \overline{35} & \overline{36} & 37 & \overline{38} & \overline{39} & \overline{40} & 41 & \overline{42} & 43 & \overline{44} & \overline{45} \\
\overline{46} & 47 & \overline{48} & \overline{49} & \overline{50} & \overline{51} & \overline{52} & 53 & \overline{54} & \overline{55} & \overline{56} & \overline{57} & \overline{58} & 59 & \overline{60}.
\end{array}$$

9) Присматриваясь к последовательности простых чисел, очень трудно заметить какую-либо закономерность в их следовании. Прошли тысячелетия со времен Евклида, пока кое-какие закономерности были обнаружены.

Сначала, можно сказать, в последовательности простых чисел бросаются в глаза не закономерности, а странности. Между некоторыми простыми числами имеются довольно большие промежутки, между другими расстояние уменьшается до двух, и только в одном случае простые числа стоят рядом — это 2 и 3. (Кроме этих двух чисел, никакие другие простые числа рядом стоять не могут, потому что каждое второе число после двух — число четное — составное.)

Нетрудно убедиться в том, что промежутки между простыми числами могут быть сколь угодно большими; в самом деле, если возьмем последовательные натуральные числа

$$11!^{1}+2,\ 11!+3,\ 11!+4,\ \ldots,\ 11!+11, \qquad (1)$$

то первое из них делится на 2 (так как $11!|2$, $2|2$, а следовательно, и $11!+2|2$), второе — на $3, \ldots, 11!+11$ — на 11, так что получается 10 рядом стоящих составных чисел. Таким же образом можно указать даже 1000 и более последовательных натуральных чисел, которые все являются составными.

Итак, промежутки между последовательными простыми числами могут быть сколь угодно большими.

Надо, конечно, учесть, что такие последовательности составных чисел, как например (1), расположены сравнительно далеко от начала натурального ряда; и чем длиннее указанная последовательность становится, тем дальше она отодвигается от начала.

Подсчитайте, с какого числа начинается последовательность (1).

$$11!+2=2\cdot3\cdot4\cdot5\cdot6\cdot7\cdot8\cdot9\cdot10\cdot11+2=39\,916\,802.$$

10) Вы, конечно, хотели бы теперь узнать, как обстоит дело с теми простыми числами, между которыми разность всего 2. Такие простые числа получили название простых чисел — «близнецов», их можно записать в виде p и $p+2$. Сведения, которые мы имеем о них, куда более скромные, а именно: простые числа — «близнецы» обнаружены среди весьма больших чисел. Такими числами являются, например, 8 004 119 и 8 004 121; 10 006 427 и 10 006 429; 1 000 000 009 649 и 1 000 000 009 651. Самая далекая из известных таких пар следующая: 1 000 000 000 149 341 и 1 000 000 000 149 343. До сих пор неизвестно, существует ли простых чисел — «близнецов» бесконечно много или их число ограничено.

11) Согласно п. 9 мы знаем, что на некоторых участках натурального ряда можно найти неимоверные расстояния без того, чтобы встретиться с новым простым числом, на некоторых участках они бывают почти рядом. Вероятно, возникает вопрос, нельзя ли предсказать, каково простое число, следующее за p. (Мы ведь можем сказать наперед, что четное число, следующее за 1000, — это 1002, за $2n$ — $2n+2$.)

[1] 11! означает $1\cdot2\cdot3\ldots11$, а вообще $n!$ означает $1\cdot2\ldots n$.

К сожалению, этого сказать еще никто не может.

Поставим поэтому более скромный вопрос, нельзя ли хотя бы указать промежуток, в котором обязательно встретится новое простое число.

Один такой промежуток можно выявить, исходя из доказательства Евклида о неограниченности ряда простых чисел, а именно: в п. 7 мы фактически обнаружили, что простое число, следующее за 7, не превосходит $2\cdot3\cdot5\cdot7+1=211$. Аналогичное можно утверждать относительно простого числа p.

Этот результат кажется не очень блестящим, если вспомнить, что фактически следующее за 7 простое число — это 11.

Но для начала и таким результатом следует довольствоваться: предсказание слабое, но все же вполне определенное.

12) Обнаружив один промежуток, естественно спросить, нельзя ли сузить границы промежутка, в пределах которого после любого простого числа p можно с уверенностью ожидать встречу с новым простым числом.

Этим вопросом занимались многие ученые. Один из наиболее блестящих результатов получен великим русским математиком П. Л. Чебышевым (1821—1894). В середине прошлого века он доказал, что для $n>3$ между n и $2n-2$ всегда содержится хотя бы одно простое число, например,

между	4 и 6	$(=8-2)$	расположено простое число 5;
„	5 и 8	$(=10-2)$	„ „ „ 7;
„	6 и 10	$(=12-2)$	„ „ „ 7;
„	7 и 12	$(=14-2)$	„ „ „ 11;
„	20 и 38	$(=40-2)$	расположены простые числа 23, 29, 31, 37.

В связи с открытием этой и других закономерностей, касающихся расположения простых чисел, Чебышев настолько прославился, что его стали называть победителем простых чисел.

В настоящее время удалось еще более сузить границы упомянутого промежутка: доказано, что для натуральных чисел $n>5$ между n и $2n$ содержатся по крайней мере 2 простых числа. Так, например,

между	6 и 12	расположены простые числа 7 и 11;
„	7 и 14	„ „ „ 11 и 13;
„	8 и 16	„ „ „ 11 и 13.

13) Поскольку предсказания относительно отдельных простых чисел очень трудны, неплохо бы выяснить, как часто в

среднем простые числа встречаются на участках натурального ряда. (Мы не можем, например, сказать, какова будет погода 13 августа 1978 года, но мы можем с некоторой уверенностью предсказать, какова будет средняя температура в августе — это величина довольно постоянная для определенного географического места.) С этой целью введем предварительно обозначение для числа простых чисел, не превосходящих данное число x, а именно $\pi(x)$.

Нетрудно найти, что

$$\pi(1)=0;\ \pi(2)=1;\ \pi(3)=2;\ \pi(4)=2;\ \pi(5)=3;$$

$$\pi(6)=3;\ \pi(7)=4;\ \pi(8)=4;\ \pi(9)=4;\ \pi(10)=4.$$

Оказывается, что

$$\pi(100)=25;\ \pi(1000)=168;\ \pi(10\,000)=1229;$$

$$\pi(1\,000\,000)=78\,498.$$

Из последних данных видно, что число простых чисел в среднем убывает: в самом деле, до 100 мы имеем 25 простых чисел, до 1000 — на каждую сотню $168:10\approx17$, до 10 000 — $1\,229:100\approx\approx13$, до 1 000 000 — $78\,498:10\,000\approx8$.

Оказывается, что и в дальнейшем число простых чисел на каждую сотню натуральных чисел продолжает в среднем убывать и становится ничтожно малым, так что, хотя простых чисел в натуральном ряду имеется бесконечно много, все же, по сравнению со всем натуральным рядом, их ничтожно мало.

И это свойство впервые строго доказал П. Л. Чебышев.

14) Вы уже знаете, что натуральное число (>1) либо является простым, либо его можно представить как произведение простых чисел. Относительно выражения натуральных чисел через сумму простых чисел чрезвычайно интересное предположение высказал петербургский академик Х. Гольдбах (в письме к великому петербургскому математику Л. Эйлеру (1707—1783) в 1742 г., а именно: каждое натуральное число $N>5$ можно представить в виде суммы трех простых чисел.

Проверьте утверждение Гольдбаха для $N=20$, 35, 40. Имеем например,

$$20=2+\ 7+11;$$

$$35=5+13+17;$$

$$40=2+19+19.$$

Л. Эйлер ответил Гольдбаху, что он не сомневается в том, что каждое четное число, которое больше 2, есть сумма двух простых.

Проверьте утверждение Эйлера для $N=20$, 40. Имеем, например,

$$20=\ 7+13;$$

$$40=17+23.$$

В течение почти двух столетий не было никакого сдвига в решении этой проблемы, которая по своему содержанию столь проста. И это несмотря на то, что указанной проблемой занимались крупнейшие математики и что опытная проверка к началу XX века была выполнена до 9 миллионов.

Впервые успеха в решении этой проблемы добился молодой советский математик Л. Г. Шнирельман (1905—1938). В 1930 г. он доказал, что существует постоянное число C, такое, что всякое натуральное число $N>1$ есть сумма не более C простых.

К настоящему времени методом, восходящим к Шнирельману, доказано, что каждое достаточно большое N можно представить как сумму не более 10 простых чисел. (Это значит, что должно существовать такое натуральное число N_0, что все натуральные числа, большие, чем это натуральное число, можно будет представить как сумму не более 10 простых чисел.)

Результат Шнирельмана был в свое время воспринят математиками с большим восторгом, потому что до этого проблема Гольдбаха считалась вообще неприступной.

Крупнейший специалист по теории чисел Э. Ландау в связи с открытием Шнирельмана писал: «Работа Шнирельмана содержит одно из величайших достижений в теории чисел, до которого мне удалось дожить».

Но еще куда более значительных успехов добился крупнейший советский ученый в области теории чисел, всемирно известный математик И. М. Виноградов (род. в 1891 г.). В 1937 г. он доказал, что каждое достаточно большое нечетное число можно представить в виде суммы трех простых чисел. Мы даже знаем такое число a $(a=3^{3^{16}})$, что каждое нечетное число, которое больше a, является суммой трех простых нечетных чисел.

Что касается предположения Эйлера, что всякое четное число представимо в виде суммы двух простых чисел, то оно до настоящего времени не доказано и не опровергнуто.

Известно лишь, что каждое достаточно большое четное число можно представить в виде суммы простого числа и произведения не более трех простых чисел. Это в 1965 г. доказал советский математик А. А. Бухштаб (род. в 1905 г.).

II. НЕКОТОРЫЕ ЗАМЕЧАТЕЛЬНЫЕ ПРОСТЫЕ И СОСТАВНЫЕ ЧИСЛА

1) Свойства чисел с древних времен привлекали внимание людей, правда, иногда они связывались с некоторыми суевериями. Уже в школе древнегреческого математика Пифагора (VI в. до н. э.) рассматривались различные категории чисел, например простые, составные, совершенные, дружественные, квадратные.

Совершенные числа — это такие числа, сумма собственных делителей которых (т. е. делителей за исключением самого числа) равна этому же числу. Совершенными числами являются, например, 6 и 28:

$$6=1+2+3;\ 28=1+2+4+7+14.$$

Древним грекам были также известны совершенные числа 496 и 8 128.

Если сумму делителей числа n обозначим через $s(n)$, то для совершенных чисел $s(n)-n=n$, или $s(n)=2n$.

2) Чтобы поближе ознакомиться с совершенными числами, рассмотрим, как определяется сумма делителей числа n.

Постараемся выяснить это сначала для степени простого числа p^α. Делители такого числа следующие:

$$1, p, p^2, \dots, p^\alpha,$$

а их сумма равна

$$1+p+p^2+\dots+p^\alpha.$$

Чтобы найти эту сумму, вспомним некоторые формулы:

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

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

Нетрудно убедиться в том, что наблюдаемая закономерность имеет общий характер, т. е. что

$$(a^3+a^2+a+1)(a-1)=a^4-1;$$

$$(a^4+a^3+a^2+a+1)(a-1)=a^5-1 \text{ и т. д.}$$

Проверим, например, эту закономерность для произведения

$$(a^5+a^4+\dots+1)(a-1).$$

Находим:

$$(a^5+a^4+a^3+a^2+a+1)(a-1)=$$
$$\begin{array}{l}=a^6+a^5+a^4+a^3+a^2+a+\\ \quad -a^5-a^4-a^3-a^2-a-1\\ \hline =a^6 \qquad\qquad\qquad\qquad -1.\end{array}$$

Процесс умножения подтверждает верность указанной закономерности. Итак, (если $a\neq 1$),

$$a^5+a^4+a^3+a^2+a+1=\frac{a^6-1}{a-1}$$

и вообще

$$p^\alpha+p^{\alpha-1}+\dots+p+1=\frac{p^{\alpha+1}-1}{p-1}.$$

3) Упражнение.

Найти сумму делителей: а) 3^5, б) 2^6, в) 5^3.

Ответ.

а) $s(3^5)=\dfrac{3^6-1}{3-1}=364;$

б) $s(2^6)=\dfrac{2^7-1}{2-1}=127;$

в) $s(5^3)=\dfrac{5^4-1}{5-1}=156.$

4) Подумаем, как можно было бы найти сумму всех делителей числа $p_1^{\alpha_1}p_2^{\alpha_2}$.

Рассмотрим сначала способ составления всех делителей такого числа, например $2^3\cdot3^2$. Во-первых, расположим в два ряда делители множителей 2^3 и 3^2. Получим ряды:

$$1,\ 2,\ 2^2,\ 2^3;$$
$$1,\ 3,\ 3^2.$$

Теперь надо составить всевозможные произведения этих чисел. По-видимому, они появляются как слагаемые в произведении

$$(1+2+2^2+2^3)(1+3+3^2).$$

Таким образом, это произведение является суммой всех делителей числа $2^3 \cdot 3^2$. В общем случае имеем в отдельности для $p_1^{\alpha_1}$ и $p_2^{\alpha_2}$ (p_1 и p_2 — различные простые числа) делители:

$$1, \quad p_1, \quad p_1^2, \quad \ldots, \quad p_1^{\alpha_1};$$
$$1, \quad p_2, \quad p_2^2 \quad \ldots, \quad p_2^{\alpha_2},$$

а их всевозможные произведения, которые суть делители $p_1^{\alpha_1}p_2^{\alpha_2}$, исчерпываются слагаемыми произведения

$$(1+p_1+\ldots+p_1^{\alpha_1})(1+p_2+\ldots+p_2^{\alpha_2}).$$

Поэтому последнее произведение и является суммой всех делителей $p_1^{\alpha_1}p_2^{\alpha_2}$. Поскольку значение каждой скобки нам уже известно, то имеем

$$s(p_1^{\alpha_1}p_2^{\alpha_2})=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\,\frac{p_2^{\alpha_2+1}-1}{p_2-1}.$$

По-видимому, присоединяя к $p_1^{\alpha_1}p_2^{\alpha_2}$ еще третий множитель $p_3^{\alpha_3}$ (p_3 — простое число, $\neq p_1$ и $\neq p_2$), можно будет сумму всех делителей произведения получить в виде произведения

$$(1+p_1+\ldots+p_1^{\alpha_1})(1+p_2+\ldots+p_2^{\alpha_2})(1+p_3+\ldots+p_3^{\alpha_3}),$$

что приводит нас к формуле

$$s(p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3})=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\,\frac{p_2^{\alpha_2+1}-1}{p_2-1}\,\frac{p_3^{\alpha_3+1}-1}{p_3-1}.$$

Эту формулу можно распространить на общий случай, когда

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}.$$

5) Евклид установил, что если число n имеет вид $n=2^{k-1}(2^k-1)$, $k>1$, и при этом $2^k-1=p$ — число простое, то n — число совершенное.

Проверим это.

Поскольку $n=2^{k-1}p$, то по указанной формуле для $s(n)$ находим

$$s(n)=\frac{2^k-1}{2-1}\,\frac{p^{1+1}-1}{p-1}=(2^k-1)(p+1)=p2^k=2\cdot 2^{k-1}p=2n.$$

Среди чисел $k\leqslant 7$ условие, чтобы 2^k-1 было простым числом, выполняется для $k=2, 3, 5, 7$. Мы получаем простые числа 3, 7, 31

и 127, которым соответствуют упомянутые выше совершенные числа.

6) После открытия Евклида возник, конечно, вопрос о том, нет ли других совершенных чисел. Только через 2 тысячи лет Л. Эйлер доказал, что четных совершенных чисел другого вида не существует, но это доказать труднее, чем теорему Евклида о совершенных числах.

Что же касается нечетных совершенных чисел, то до сих пор не доказано, что таких не существует, но имеется предположение, что это именно так. Во всяком случае известно, что нечетные совершенные числа, если они существуют, превышают 10^{50}.

7) Был поставлен вопрос о нахождении простых чисел вида 2^k-1, так как каждому такому простому числу соответствует совершенное число. До сих пор неизвестно, имеется ли бесконечно много таких простых чисел. При поисках таких простых чисел были обнаружены наибольшие из известных простых чисел вообще.

Нетрудно убедиться в том, что при $k=k_1k_2$, т. е. когда k — составное, 2^k-1 не может быть простым числом. В самом деле, если, например, $k=3\cdot 4$, то имеем $2^{3\cdot 4}-1=(2^3)^4-1$, что делится на 2^3-1. С другой стороны, в случае простого показателя k нельзя еще утверждать, что 2^k-1 — число простое. Так, например, при $k=11$ имеем $2^{11}-1=2047=23\cdot 89$.

8) Простые числа вида $M_p=2^p-1$, где p — простое число, получили название простых чисел Мерсенна. О них французский математик М. Мерсенн вел переписку с великим французским математиком П. Ферма (1601—1665), с именем которого связан расцвет теории чисел в новое время (после средних веков, в период которых теория чисел мало развивалась). До Эйлера было известно 7 совершенных чисел, соответствующих простым числам Мерсенна при $p=2, 3, 5, 7, 13, 17, 19$. Эйлер доказал, что $2^{31}-1$ также простое число. Число Эйлера считалось наибольшим из известных простых чисел до 1883 г., когда талантливый русский вычислитель И. М. Первушин доказал, что $2^{61}-1$ есть простое число.

К настоящему времени установлена еще простота чисел вида 2^p-1 для показателей $p=89$, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937.

Начиная с $p=521$ простота чисел M_p была установлена при помощи электронных вычислительных машин (1952).

Простота числа $2^{19937}-1$ (имеет 6002 цифры) была установлена в 1971 г. Это вообще наибольшее из известных до 1971 г. простых чисел.

9) Если сумма собственных делителей числа a равна b и

наоборот, то такие числа называются дружественными числами (это название возникло еще в Древней Греции). Для них $s(a)-a=b$, $s(b)-b=a$, так что $s(a)=s(b)=a+b$.

В Древней Греции была известна лишь одна пара дружественных чисел: 220 и 284 (проверьте это). Эйлер нашел 65 пар дружественных чисел. Одна из них 17 296 и 18 416. Общая формула для них не найдена до сих пор.

(Проверьте, что $1184=2^5\cdot 37$ и $1210=2\cdot 5\cdot 11^2$ являются дружественными числами.)

10) Пифагорейцы изображали числа при помощи точек, группируемых в виде геометрических фигур. Это облегчало им изучать свойства чисел. В дальнейшем такие числа получили название фигурных чисел.

Простейшими среди фигурных чисел являются треугольные числа: 1, 3, 6, 10, ... (рис. 1). Им соответствуют треугольники, составленные из точек. При этом $a_1=1$; $a_2=1+2=3$; $a_3=1+2+3=6$; $a_4=1+2+3+4=10$ и т. д.

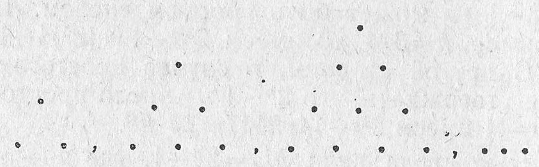

Рис. 1.

С другой стороны, нетрудно заметить, что

$$a_1=\frac{1\cdot 2}{2};\quad a_2=\frac{2\cdot 3}{2};\quad a_3=\frac{3\cdot 4}{2};\quad a_4=\frac{4\cdot 5}{2}\ \text{и т. д.}$$

Вообще n-е треугольное число

$$a_n=1+2+\ldots+n=\frac{n(n+1)}{2}.$$

Убедимся в том, что это так должно быть, например, для 15. Способ проверки подскажет нам, что эта закономерность имеет общий характер. Запишем 15 в следующих двух видах:

$$15=1+2+3+4+5;$$

$$15=5+4+3+2+1,$$

следовательно, $2\cdot 15=(1+5)+(2+4)+(3+3)+(4+2)+(5+1)=5\cdot 6$ и

$$15=\frac{5\cdot 6}{2}.$$

В общем случае можно будет воспользоваться таким же рассуждением.

Заметим, что великий немецкий математик К. Ф. Гаусс (1777—1855), который имеет большие заслуги в развитии теории чисел, будучи мальчиком лет четырех, сам додумался указанным выше способом сложить натуральные числа от 1 до 50.

Ферма высказал утверждение, что каждое натуральное число является треугольным числом, или суммой двух или трех таких чисел.

(Проверьте это на примерах).

11) Весьма простое строение имеют квадратные числа

$$1,\ 4,\ 9,\ \ldots,$$

т. е. квадраты натуральных чисел. Им соответствуют квадраты, составленные из точек (рис. 2).

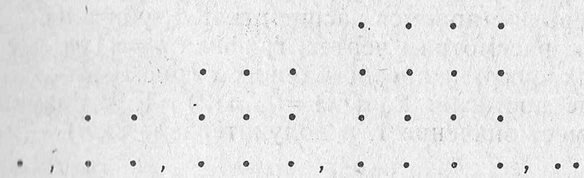

Рис. 2.

Французский математик Ж. Лагранж доказал, что каждое натуральное число можно выразить как сумму четырех квадратов целых чисел.

Так, например, $27=4^2+3^2+1^2+1^2$, $250=14^2+7^2+2^2+1^2$.

Отметим, что факт, доказанный Лагранжем, является частным случаем известного предложения английского математика Э. Варинга (1770) о том, что каждое натуральное число N можно представить в виде ограниченной суммы n-ных степеней целых чисел, т. е. в виде

$$N=x_1^n+x_2^n+\ldots+x_r^n,$$

где $x_1, x_2, \ldots, x_r$ — целые числа, а r, т. е. число слагаемых, зависит от показателя степени n, но от N не зависит. Оказывается, что каждое натуральное число N можно представить как сумму не более 9 кубов, не более 30 четвертых степеней, не более 40 пятых степеней целых чисел.

В общем случае знаменитую проблему Варинга впервые решил крупнейший немецкий математик первой половины XX века Д. Гильберт (1862—1943). Но его доказательство получилось очень громоздким и оценка для r очень грубой. Обозримое доказательство и хорошую оценку для r дал академик И. М. Виноградов, что явилось большим достижением в области теории чисел. При этом И. М. Виноградов воспользовался новым методом, который имеет широкое применение и в других вопросах теории чисел. В частности, этим же методом, еще более усовершенствованным, академик Виноградов воспользовался при решении проблемы Гольдбаха для нечетного случая.

III. РАСПРЕДЕЛЕНИЕ ПРОСТЫХ ЧИСЕЛ В НАТУРАЛЬНОМ РЯДЕ И В ДРУГИХ ПОСЛЕДОВАТЕЛЬНОСТЯХ

1) Некоторые сведения о простых числах даны в предыдущих беседах. Теперь постараемся расширить и углубить их.

Во-первых, рассмотрим чертеж графика $y=\pi(x)$, где $\pi(x)$ — число простых чисел, не превосходящих x (рис. 3).

Пока x не достигает 2, $\pi(x)=0$; $\pi(2)=1$. В полуинтервале $[2,3)$ $\pi(x)$ имеет значение 1, в полуинтервале $[3,5)$ — значение 2 и т. д.

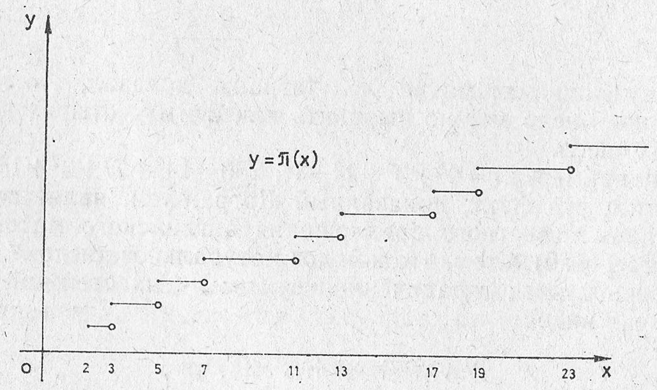

Рис. 3.

График функции $y=\pi(x)$ делает скачки; он состоит из ступеней (их первые концы графику не принадлежат); длина ступени в полуинтервале $[2,3)$ равна 1, в дальнейшем встречается много ступеней длины 2 (они соответствуют простым числам-«близнецам»), но мы не знаем, бесконечно ли число таких ступеней. Последняя из известных ступеней длины 2 начинается для $x=1\,000\,000\,000\,149\,341$. Имеются, с другой стороны, ступени сколь угодной длины, так как существуют интервалы любой длины, не содержащие простых чисел.

Теорему Евклида о бесконечности числа простых чисел в натуральном ряду можно при помощи функции $\pi(x)$ выразить следующим образом: при $x\to\infty$ $\pi(x)\to\infty$ или $\lim\limits_{x\to\infty}\pi(x)=\infty$.

2) На то, что простые числа с возрастанием натуральных чисел встречаются все реже, указал уже Эйлер. Это утверждение можно выразить следующим образом: отношение $\frac{\pi(x)}{x}$, так называемая средняя плотность простых чисел на отрезке от 1 до x, все время убывает. Эйлер впервые, хотя и не совсем строго, доказал, что при $x\to\infty$ $\frac{\pi(x)}{x}\to 0$, или что $\lim\limits_{x\to\infty}\frac{\pi(x)}{x}=0$.

Эйлер установил также, что простые числа в среднем в некотором смысле встречаются в натуральном ряду реже, чем квадраты натуральных чисел.

3) Отмеченные факты о распределении простых чисел дают только смутное представление об этом сложнейшем вопросе теории чисел.

Ученые начала XIX века поставили перед собой задачу найти для функции $\pi(x)$ приближающую ее функцию $f(x)$, которая была бы хорошо знакома и обладала бы тем свойством, что для бесконечно возрастающих значений x отношение $\frac{\pi(x)}{f(x)}$ стремилось бы к 1, т. е. чтобы было $\lim\limits_{x\to\infty}\frac{\pi(x)}{f(x)}=1$.

Иными словами, чтобы отношение соответствующих членов рядов

$$\pi(1),\ \pi(2),\ \pi(3),\ \ldots$$

и

$$f(1),\ f(2),\ f(3),\ \ldots$$

тем более приближалось к единице, чем дальше мы продвигаемся вперед в натуральном ряду чисел.

В 1808 г. Лежандр на основании исследования таблицы простых чисел (которая к тому времени была составлена до 400 000) опубликовал замечательную элементарную формулу для приближенного представления функции $\pi(x)$, а именно:

$$\pi(x) \approx \frac{x}{\ln x - 1{,}08\ldots},$$

где $\ln x$ — натуральный логарифм x[1]. Независимо от Лежандра Гаусс, подсчитывая количество простых чисел последовательно на каждую тысячу чисел натурального ряда, получил подобный же результат. Его можно выразить следующим образом:

$$\pi(x) \approx \int_2^x \frac{dt}{\ln t}.$$

Заметим, что при $x \to \infty$ имеем

$$\left(\frac{x}{\ln x - 1{,}08\ldots} : \int_2^x \frac{dt}{\ln t}\right) \to 1.$$

Но как результат Лежандра, так и результат Гаусса имели опытный характер и не могли дать указаний о поведении функции $\pi(x)$ за пределами известной в то время таблицы простых чисел.

4) Первым, кто после Евклида добился существенного продвижения в труднейшем вопросе о распределении простых чисел в натуральном ряду при помощи теоретических исследований, был П. Л. Чебышев.

Чебышев в середине прошлого века доказал, что для достаточно больших значений x

$$0{,}92\ldots < \pi(x) : \frac{x}{\ln x} < 1{,}05\ldots$$

---

[1] $\ln x$ — логарифм при основании e, где $e = \lim\limits_{n\to\infty}\left(1+\frac{1}{n}\right)^n = 2{,}71828\ldots$ — иррациональная константа, играющая в математике исключительно большую роль. Число e характеризует наращенное значение, получаемое из 1 через 1 год, если закон увеличения $\frac{1}{n}$ 100% за $\frac{1}{n}$ года и $n \to \infty$, т. е. при 100%-ном сложнопроцентном и непрерывном ее увеличении.

Зная $\log x$ при основании 10, можно вычислить $\ln x$ по формуле $\ln x = \log x : M$, где $M = 0{,}4343\ldots$

Графически неравенства Чебышева означают, что для достаточно больших значений x график функции $\pi(x) : \frac{x}{\ln x}$ лежит между параллелями $y = 0{,}92\ldots$ и $y = 1{,}05\ldots$ (рис. 4). Из неравен-

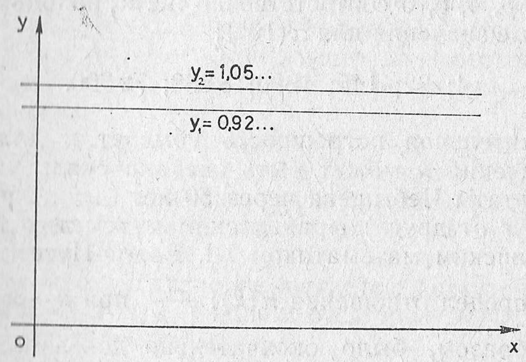

Рис. 4.

ства Чебышева следует, что для достаточно больших значений x

$$\frac{\pi(x)}{x} < \frac{1{,}05\ldots}{\ln x},$$

но так как $\ln x \to \infty$ при $x \to \infty$, то правая часть неравенства стремится к нулю и вместе с тем из этого следует, что $\frac{\pi(x)}{x} \to 0$ при $x \to \infty$. Таким образом, неравенства Чебышева подтверждают утверждение Эйлера о средней плотности простых чисел.

Результат Чебышева показывает, что приближенные формулы Лежандра и Гаусса применимы также за пределами эмпирически проверенных таблиц.

Из неравенств Чебышева вытекает, что для $n > 3$ между n и $2n-2$ всегда содержится хотя бы одно простое число.

Чебышев доказал, что если существует предел для выражения $\pi(x) : \frac{x}{\ln x}$ при $x \to \infty$, то он не может отличаться от 1.

Заметим, что при помощи приближенной формулы

$$\pi(x) \approx \frac{x}{\ln x}$$

очень удобно делать вычисления для $x=10^k$, так как

$$\pi(10^k)\approx\frac{10^k}{k\ln 10}=\frac{10^k\cdot 0{,}434}{k}.$$

При $k=1, 2, 3, 4, 5, 6$ соответственно легко находим следующие приближенные значения для $\pi(10^k)$:

$$4;\ 22;\ 145;\ 1090;\ 8\,680;\ 72\,300.$$

Их относительная погрешность убывает и для достаточно больших значений k может быть сделана сколь угодно малой.

5) Результаты Чебышева через 50 лет были дополнены (независимо друг от друга) французским математиком Ж. Адамаром и бельгийским математиком Ш. Валле-Пуссеном. Они доказали, что предел отношения $\pi(x):\frac{x}{\ln x}$ при $x\to\infty$ существует.

Таким образом, было окончательно доказано, что предел $\lim\limits_{x\to\infty}\left(\pi(x):\frac{x}{\ln x}\right)$ существует и равен 1. Этот факт называется основным законом распределения простых чисел.

Выражаясь более просто, можно сказать: если продвигаться все дальше и дальше в натуральном ряду чисел, то отношение соответствующих членов последовательностей

$$\pi(2),\ \pi(3),\ \pi(4),\ \pi(10),\ \pi(10^3),\ \pi(10^4),\ldots$$

и

$$\frac{2}{\ln 2},\ \frac{3}{\ln 3},\ \frac{4}{\ln 4},\ \frac{10}{\ln 10},\ \frac{10^3}{\ln 10^3},\ \frac{10^4}{\ln 10^4},\ldots$$

все более приближается к единице.

Из основного закона распределения простых чисел следует, что при $n\to\infty$ отношение n-го простого числа p_n к $n\ln n$ стремится к 1, другими словами, отношение соответствующих членов последовательностей

$$p_1,\ p_2,\ \ldots,\ p_n,\ \ldots$$

и

$$1\ln 1,\ 2\ln 2,\ \ldots,\ n\ln n,$$

стремится к единице.

В 1949 г. датский математик А. Сельберг и венгерский математик П. Эрдеш нашли элементарное доказательство основного закона распределения простых чисел, но и это доказательство является весьма сложным.

6) Существует бесконечно много простых чисел, но в то же время мы не в состоянии указать n-е простое число p_n. Мы также не в состоянии указать сколь угодно большое простое число.

Как было указано выше, наибольшее из известных простых чисел найдено среди простых чисел Мерсенна $M_p=2^p-1$, где p — простое число.

Ферма высказал предположение, что все числа вида 2^k+1, где $k=2^n$, являются простыми. Для $k>0$ условие $k=2^n$ является необходимой предпосылкой, так как в противном случае, когда $k=k_1\cdot k_2$ содержит нечетный множитель $k_1>1$, число $2^k+1=(2^{k_2})^{k_1}+1$ делится на $2^{k_2}+1$.

Однако указанное условие не является достаточным. В то время, как для $n=0, 1, 2, 3, 4$ получаются простые числа, так называемые простые числа Ферма

$$3,\ 5,\ 17,\ 257,\ 65537,$$

для $n\geqslant 5$ простые числа Ферма до сих пор не обнаружены. С другой стороны, показано, что числа Ферма $F_n=2^{2^n}+1$ являются составными для показателей

$n=5$, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18, 19, 23, 36, 38, 39, 55, 58, 63, 73, 77, 81, 117, 125, 144, 150, 207, 226, 228, 250, 267, 268, 284, 316, 452, 1945.

Для $n=5$ указанный факт был впервые доказан Эйлером. Большинство этих результатов установлено при помощи электронных вычислительных машин.

Нетрудно и нам убедиться в том, что $F_5|641$.

В самом деле, с одной стороны, $641=5\cdot 2^7+1$, $5\cdot 2^7\equiv -1 \pmod{641}$ и

$$5^4\cdot 2^{28}\equiv 1 \pmod{641}; \tag{1}$$

с другой стороны, $641=16+625=2^4+5^4$ и

$$2^4\equiv -5^4 \pmod{641}. \tag{2}$$

Почленным перемножением сравнений (1) и (2) получаем

$$2^{32}\equiv -1 \pmod{641};$$
$$2^{32}+1\equiv 0 \pmod{641},$$

т. е.

$$2^{2^5}+1 \mid 641.$$

Интересно отметить, что простые числа Ферма играют боль шую роль в геометрии, а именно: Гаусс доказал, что правильны p-угольники для простых $p>2$ можно построить циркулем и ли нейкой тогда и только тогда, когда p — простое число Ферма Поскольку неизвестно, существуют ли сколь угодно больши простые числа Ферма, то неизвестно также, существуют ли пра вильные p-угольники со сколь угодно большим количеством сто рон, которые можно было бы построить при помощи циркуля и линейки.

7) Многие математики старались найти такую элементарную функцию $f(x)$, которая для всех целых x (или, по крайней мере для бесконечной последовательности таких x) давала бы различ ные простые числа. При помощи такой функции можно было бы вычислить сколь угодно много простых чисел и сколь угодно большие простые числа, если только имелась бы возможност найти $f(x)$ для каждого x.

Эйлер нашел сравнительно длинные последовательности про стых чисел, пользуясь квадратичными функциями. Так, напри мер, выражение x^2+x+17 при $x=0, 1, 2, \ldots, 15$, а x^2-x+41 — при $x=0, 1, \ldots, 40$ дают только простые числа. Аналогичны свойством обладают многочлены $2x^2+29$ при $x=0, 1, \ldots, 28$ x^2+x+41 при $x=0, 1, \ldots, 39$, $x^2-79x+1601$ при $x=0, 1, \ldots, 79$

Найдены также другие многочлены $f(x)$, которые при $x=$ $=0, 1, \ldots, k$ принимают значения простых чисел.

В то же время легко доказать теорему, которую впервые вы сказал Х. Гольдбах: никакая целая рациональная функция от с целыми коэффициентами, отличная от константы, не может дл всякого натурального x принимать значения, равные просты числам.

Доказательство. Пусть

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n \quad \text{и} \quad f(a)=p,$$

где p — простое число. Рассмотрим $f(a+pt)$, где t — любое це лое число. Так как $a+pt\equiv a \pmod p$, то $f(a+pt)\equiv f(a) \pmod p$ Но $f(a)=p$, так что $f(a)\equiv 0 \pmod p$. Поэтому и $f(a+pt)\equiv$ $\equiv 0 \pmod p$, т. е. $f(a+pt) \mid p$ для любого t.

Так как при возрастающем t многочлен $f(a+pt)$ не може оставаться неизменным, то из делимости $f(a+pt)$ на p следует что $f(a+pt)$ не может принимать лишь простые значения. Тео рема доказана.

Однако в 1972 г. молодой ленинградский математик Ю. В. Матиясевич построил многочлен 21-й степени от 21 переменной, множество положительных значений которого есть в точности множество всех простых чисел.

В заключение отметим, что хотя доказано существование действительного числа α, такого, что $[\alpha^{3^n}]$ простое число для любого натурального n, все же задача нахождения простого числа, большего любого заданного, остается до сих пор практически нерешенной. Дело в том, что известны лишь немногие знаки α, так что по указанной формуле действительно можно вычислить лишь немногие простые числа. Найдены и другие формулы для вычисления бесчисленного множества простых чисел, но они имеют аналогичный недостаток. Это замечание относится также к многочлену, который построил Ю. В. Матиясевич.

8) Проблема распределения простых чисел в натуральном ряду получает дальнейшее развитие в вопросе распределения простых чисел в арифметических прогрессиях и других числовых последовательностях.

В 1837 г. немецкий математик Л. Дирихле доказал, что в каждой арифметической прогрессии

$$l,\ l+k,\ l+2k, \ldots,$$

где k и l — целые, взаимно простые числа, содержится бесконечное множество простых чисел (другими словами: при указанных условиях относительно k и l существует бесконечно много простых чисел вида $kn+l$).

Доказательство Дирихле для общего случая является весьма сложным.

Для отдельных случаев, например, для чисел вида $4n-1$, $4n+1$ теорема Дирихле доказывается значительно проще, с помощью рассуждений, аналогичных рассуждениям Евклида.

Докажем, что существует бесконечно много простых чисел вида $4n-1$.

Пусть $q_1, q_2, \ldots, q_r$ — первые r простых чисел вида $4n-1$. Число $N=4q_1q_2\ldots q_r-1$ также является числом вида $4n-1$, а его делители имеют вид $4n-1$ или $4n+1$. Только вида $4n+1$ они быть не могут, так как произведение двух чисел вида $4n+1$ снова является числом того же вида, между тем N имеет вид $4n-1$. Поэтому N имеет простой делитель вида $4n-1$. Но поскольку ни одно из чисел $q_1, q_2, \ldots, q_r$ для этого не подходит, то указанный делитель должен быть больше q_r. Итак, наибольшего простого числа вида $4n-1$ быть не может, значит существует бесконечно много простых чисел такого вида.

Доказательство для случая $4n+1$ также элементарно, но для настоящего изложения оно затруднительно.

Отметим в заключение, что исследования относительно представления простых чисел в виде квадратичной функции, даже для случая n^2+1, где n пробегает все натуральные значения, до сих пор остаются безуспешными.

ЛИТЕРАТУРА

1. *Виноградов И. М.* Основы теории чисел. М., «Наука», 1972. 167 с.
2. *Михелович Ш. Х.* Теория чисел. М., «Высшая школа», 1967. 336 с.
3. *Михелович Ш. Х.* Материалы для факультативных занятий по дополнительным вопросам арифметики, ч. 1. Даугавпилс, 1973. 178 с.

Ш. Х. Михелович

К решению задач с помощью сравнений

I.

До недавней реформы школьного математического образования учащиеся, как правило, сравнениями не пользовались, а о малой теореме Ферма (МТФ) узнавали лишь как о следствии бинома Ньютона.

В настоящее время положение изменилось. Изучение сравнений предусматривается на факультативных занятиях в VII—VIII классах. Материал этот, как известно, доступен для понимания учащихся и воспринимается ими с интересом.

Согласно программам факультативных курсов сравнения явно не включаются в «Дополнительные вопросы арифметики целых чисел» для VII класса. Однако ряд учителей старается применять сравнения как можно раньше. Это и понятно, так как сравнения весьма эффективны при решении многих задач теории делимости.

В наиболее распространенном пособии для факультативных занятий по данной тематике [1] сравнения вводятся в § 5—6 сразу же после теоремы о делении с остатком в § 4.

Из свойств сравнений указываются следующие:

1) $a\equiv b\,(m)\longleftrightarrow a-b\,|\,m$[1];

2—3) сравнения можно почленно складывать и умножать.

Приводятся следствия:

1) $a\equiv b\,(m)\rightarrow a^n\equiv b^n\,(m)$;

2) для многочлена $f(x)$ с целыми коэффициентами

$$a\equiv b\,(m)\Rightarrow f(a)\equiv f(b)\,(m).$$

Простое, но часто употребляемое свойство, что в сравнении можно заменять слагаемые и множители сравнимыми числами по данному модулю, не выделено.

[1] Символом $a|b$ будем обозначать, что a делится на b, а символом $a\nmid b$ — что a не делится на b.