1984 г. ноябрь—декабрь *т. 39, вып. 6(240*
УСПЕХИ МАТЕМАТИЧЕСКИХ НАУК

ПЕРВЫЕ 50 МИЛЛИОНОВ ПРОСТЫХ ЧИСЕЛ [1])

Дон Цагер

Мне хотелось бы рассказать вам сегодня о предмете, которым я сам хотя и не занимался, но который всегда чрезвычайно привлекал меня и который пленяет математиков, начиная с незапамятных времен вплоть до настоящего времени, а именно, о вопросе распределения простых чисел.

Вы, безусловно, все знаете, что простым числом является всякое натуральное число, большее чем 1, которое не делится ни на одно из натуральных чисел, кроме 1. По крайней мере такое определение дают специалисты в области теории чисел; специалисты в других областях математики дают иногда свое определение простых чисел, отличное от вышеприведенного. Так, например, специалисты в области теории функций определяют простое число как целочисленный корень аналитической функции

$$1-\frac{\sin\frac{\pi\Gamma(s)}{s}}{\sin\frac{\pi}{s}};$$

для алгебраистов простое число — это

«характеристика некоторого конечного поля»,

либо

«точка в Spec $\mathbb{Z}$»;

либо

«неархимедова метрика».

специалисты в области комбинаторики дают индуктивное определение простых чисел с помощью рекуррентной формулы (1) [2])

$$P_{n+1}=\left[1-\log_2\left(\frac{1}{2}+\sum_{r=1}^{n}\sum_{1\leqslant i_1<\ldots<i_z\leqslant n}\frac{(-1)^r}{2^{p_{i_1}\ldots p_{i_z}}-1}\right)\right]$$

([x] — наибольшее целое $\leqslant x$);

и, наконец, в последнее время специалисты в области математической логики стали определять простые числа как положительные значения

---

[1]) Настоящая статья является исправленным вариантом иногуральной лекции автора, прочитанной 5 мая 1975 г. в Боннском университете. Дополнительные замечания и ссылки на литературу помещены в конце. Оригинальный немецкий вариант опубликован в Beihefte zu Elemente der Mathematik № 15, Birkhäuser Verlag, Basel/ Пер. с англ. Г. П. Бабенко.

[2]) В круглых скобках даны номера замечаний, помещенных в конце статьи.

полинома (2)

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

Но я надеюсь, что вас вполне удовлетворяет первое из приведенных мной определений.

Распределение простых чисел характеризуется двумя особенностями, о которых я предполагаю рассказать настолько убедительно, что вы постоянно будете помнить о них. Во-первых, несмотря на простое определение простых чисел и скромную роль «кирпичиков» для построения натуральных чисел, простые числа принадлежат к в высшей степени случайным пренебрегающим всеми правилами объектам, изучаемым математиками: они подобно сорной траве появляются среди натуральных чисел, не подчиняясь, кажется, никаким законам, только случаю, и никто не может заранее предсказать, где даст росток следующее простое число. Вторая особенность еще более удивительна, поскольку здесь имеет место совсем противоположный факт, а именно, простые числа проявляют ошеломляющую регулярность, существуют законы, определяющие их поведение, и подчиняются они этим законам почти с воинской дисциплинированностью.

Доказательство первого из этих утверждений я позволю себе начать с демонстрации списков простых и составных чисел в пределах 100 (где, за исключением 2, я перечисляю только нечетные числа)

Простые числа			Составные числа		
2	29	67	9	49	81
3	31	71	15	51	85
5	37	73	21	55	87
7	41	79	25	57	91
11	43	83	27	63	93
13	47	89	33	65	95
17	53	97	35	69	99
19	59		39	75	
23	61		45	77	

и списков простых чисел, имеющих место среди 100 чисел, непосредственно предшествующих 10 000 000, и 100 чисел, следующих сразу за 10 000 000:

Простые числа, лежащие между 9 999 900 и 10 000 000	
9 999 901	9 999 943
9 999 907	9 999 971
9 999 929	9 999 973
9 999 931	9 999 991
9 999 937	

Простые числа, лежащие между 10 000 000 и 10 000 100
10 000 019
10 000 079

Я думаю, вы согласитесь, что явных объяснений, почему одно число является простым, а другое нет, не существует. Даже, наоборот, глядя на эти числа, возникает такое чувство, что перед тобой одна из необъяснимых тайн мироздания. Тот факт, что даже математикам не удается постичь эту тайну, возможно наиболее убедительно доказывается тем рвением, с которым они отыскивают все большие и большие простые числа, оперируя с регулярно возрастающими числами, подобно квадратам или степеням двух. Никто и никогда не станет утруждать себя поисками и регистрацией результатов, превосходящих уже известные, но, когда речь заходит о простых числах, люди, доставляя себе массу трудностей, поступают именно таким образом. Например, в 1876 г. Лукас доказал, что число $2^{127} - 1$ является простым, и в течение 75 лет этот результат оставался непревзойденным, что, возможно, и не удивительно, если представить себе это число

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

И только в 1951 г., когда появились ЭВМ, были открыты последующие простые числа. В приводимой ниже таблице представлены последовательные простые числа с указанием имен ученых, впервые их открывших (3). В настоящее время самой большой удачей является 6002-значное число $2^{19937} - 1$ (которое мне не хотелось бы здесь выписывать); если вы мне не верите, можете посмотреть это число в книге рекордов Гиннесса [1]).

Самые большие из известных простых чисел

Простое число p	Число знаков	Год открытия	Первооткрыватель
$2^{127}-1$	39	1876	Лукас
$\frac{1}{17}(2^{148}+1)$	44	1951	Феррье
$114(2^{127}-1)+1$	41	1951	Миллер + Уилер + EDSAC 1
$180(2^{127}-1)^2+1$	79		
$2^{521}-1$	157	1952	Лемер + Робинсон + SWAC
$2^{607}-1$	183		
$2^{1279}-1$	386		
$2^{2203}-1$	664		
$2^{2281}-1$	687		
$2^{3217}-1$	969	1957	Ризел + BESK
$2^{4253}-1$	1281	1961	Гурвиц + Селфридж + IBM 7090
$2^{4423}-1$	1332		
$2^{9689}-1$	2917	1963	Джиллис + JLIAC 2
$2^{9941}-1$	2993		
$2^{11213}-1$	3376		
$2^{19937}-1$	6002	1971	Тукерман + IBM 360 [2])

Однако более интересен вопрос о законах, определяющих поведение простых чисел. Я уже показывал вам список простых чисел в пределах первых 100 чисел. А сейчас вы увидите те же данные, но представленные графически. Функция, обозначенная нами через $\pi(x)$ (о которой я буду постоянно говорить в дальнейшем), указывает число простых чисел, не превосходящих x; таким образом, первое значение $\pi(x)$ равно 0 и в каждой точке, соответствующей простому (рис. 1) числу 2, 3, 5 и т. д., она увеличивается на 1. Уже на этом графике видно, что, за исключением небольших колебаний, $\pi(x)$, в общем, возрастает вполне регулярно. Когда же я расширил область значений

[1]) В 1983 г. открыто новое, 39571-значное, простое число (*Прим. перев.*)

[2]) В 1978—1983 гг. найдены четыре новых простых числа Мерсена $M_p = 2^p - 1$ для простых p, заключенных в интервале [21 000, 132 049]. Последнее из них $2^{132049} - 1$ имеет 39751 цифру (*Прим. перев.*)

x от 100 до 50000, то эта регулярность стала поразительно четкой, поскольку график в этом случае имеет вид, показанный на рис. 2. Мне кажется, что гладкость, с которой данная кривая возрастает, является одним из наиболее удивительных фактов, известных в математике. Но где бы природа ни обнаруживала образец совершенства, можно быть уверенным, что найдутся ученые, которые постараются объяснить его. Наблюдаемая регулярность возникновения простых чисел не является исключением из этого правила. Нетрудно вывести эмпирическую формулу, которая дала бы хорошее описание роста простых чисел. Среди первых 100 чисел мы имеем 25 простых чисел, т. е. одну четвертую часть от общего количества чисел; среди первых 1000 чисел мы имеем 168 простых чисел, что составляет примерно одну шестую часть; среди первых 10 000 чисел мы имеем 1229 простых чисел, т. е. примерно одну восьмую часть.

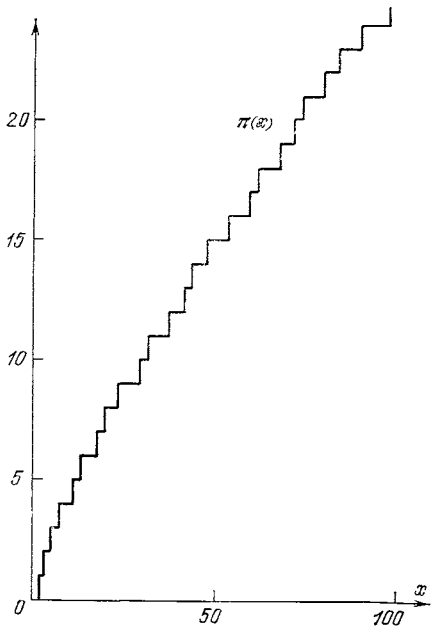

Рис. 1

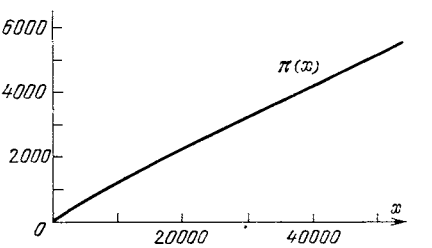

Рис. 2

Если продолжить этот список, вычисляя отношение простых чисел к общему числу натуральных чисел среди первых 100 000, 1 000 000 и т.д. чисел, то мы получим следующую таблицу (в которой за каждым значе-

x	$\pi(x)$	$x/\pi(x)$
10	4	2,5
100	25	4,0
1 000	168	6,0
10 000	1 229	8,1
100 000	9 592	10,4
1 000 000	78 498	12,7
10 000 000	664 579	15,0
100 000 000	5 761 455	17,4
1 000 000 000	50 847 534	19,7
10 000 000 000	455 052 512	22,0

нием функции $\pi(x)$, столь бесстрастно представленным здесь, стоят тысячи часов утомительных вычислений). Из этой таблицы видно, что всякий раз, когда мы переходим от одной степени 10 к последующей, отношение $x/\pi(x)$ увеличивается примерно на 2,3. Математики сразу же отождествили число 2,3 с логарифмом 10 (разумеется, по основанию e). Итак, мы пришли к выводу, что

$$\pi(x) \sim \frac{x}{\log x},$$

где знак $\sim$ означает, что $\pi(x)/(x/\log x) \to 1$, если $x \to \infty$. Это соотношение (получившее доказательство лишь в 1896 г.) известно как *асимптотический закон распределения простых чисел*. Гаусс, величайший математик мира, открыл его в пятнадцатилетнем возрасте, изучая таблицы простых чисел, помещенные в подаренной ему годом раньше книге логарифмов. В течение всей своей жизни Гаусс увлеченно занимался изучением вопроса распределения простых чисел, в связи с чем ему пришлось выполнить массу вычислений. В одном из писем к Энке (4) он пишет, как он «довольно часто, имея свободными минут пятнадцать, занимался просчитыванием очередной тысячи (т. е. интервала в 1000 чисел)», пока, наконец, не перечислил все простые числа вплоть до 3 000 000 (!) и не сравнил их распределение с результатами, полученными с помощью выведенной им формулы.

Закон распределения простых чисел утверждает, что $\pi(x)$ асимптотически (т. е. с относительной ошибкой, равной 0%) равно $x/\log x$. Но если сравнить график функции $x/\log x$ с графиком функции $\pi(x)$, можно видеть, что,

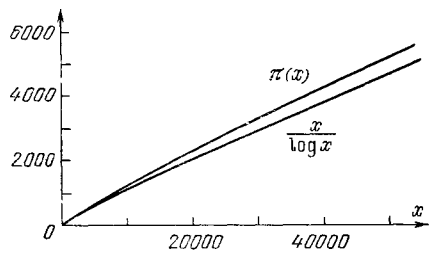

Рис. 3

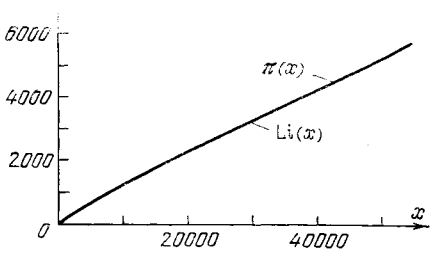

Рис. 4

несмотря на то, что функция $x/\log x$ качественно отображает поведение функции $\pi(x)$, она, безусловно, не вполне соответствует функции $\pi(x)$, чтобы объяснить гладкость последней (рис. 3). Поэтому вполне естественно искать более хорошие приближения. Если еще раз посмотреть на таблицу отношений $x/\pi(x)$, можно увидеть, что это соотношение почти точно соответствует $\log x - 1$. Проведя более тщательные вычисления и получив более подробные данные относительно функции $\pi(x)$, Лежандр (5) в 1808 г. установил, что для того чтобы получить особенно хорошее приближение, из $\log x$ нужно вычитать не 1, а 1, 08366, т. е.

$$\pi(x) \approx \frac{x}{\log x - 1{,}08366}.$$

Исходя из установленного эмпирическим путем факта, что плотность простых чисел в окрестности некоторого очень большого числа x почти равна $1/\log x$, можно получить еще одно хорошее приближение к функции $\pi(x)$, которое впервые было предложено Гауссом. А именно, число простых чисел, не превосходящих x, приближенно определяется *логарифмической суммой*

$$Ls(x) = \frac{1}{\log 2} + \frac{1}{\log 3} + \ldots + \frac{1}{\log x}$$

либо, что в сущности одно и то же (6), *логарифмическим интегралом*

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\log t}\, dt.$$

Если теперь сравнить график функции $\mathrm{Li}(x)$ с графиком функции $\pi(x)$ рис. 4, то можно видеть, что в пределах принятой нами точности эти графики совершенно совпадают. Я не вижу смысла приводить здесь также график приближения Лежандра, поскольку в пределах данного графика оно является даже лучшим приближением к функции $\pi(x)$. Имеется еще одно приближе-

ние, о котором мне хотелось бы сказать здесь несколько слов. Занимаясь исследованиями в области простых чисел, Риман пришел к выводу, что вероятность того, что некоторое большое число x будет простым, будет ближе к $1/\log x$, если считать не только простые числа, но также и *степени* простых чисел, считая квадрат простого числа как половину простого числа, куб простого числа — как третью часть простого числа и т. д. В результате получаем следующее приближение (7):

$$\pi(x) + \frac{1}{2}\pi(\sqrt{x}) + \frac{1}{3}\pi(\sqrt[3]{x}) + \ldots \approx \mathrm{Li}(x)$$

или

$$\pi(x) = \mathrm{Li}(x) - \frac{1}{2}\mathrm{Li}(\sqrt{x}) - \frac{1}{3}\mathrm{Li}(\sqrt[3]{x}) - \ldots$$

Функцию в правой части этой формулы обозначим в честь Римана через $R(x)$. Как показывают результаты, приведенные в нижеследующей таблице, эта функция является поразительно удачным приближением к $\pi(x)$:

x	$\pi(x)$	$R(x)$
100 000 000	5 761 455	5 761 552
200 000 000	11 078 937	11 079 090
300 000 000	16 252 325	16 252 355
400 000 000	21 336 326	21 336 185
500 000 000	26 355 867	26 355 517
600 000 000	31 324 703	31 324 622
700 000 000	36 252 931	36 252 719
800 000 000	41 146 179	41 146 248
900 000 000	46 009 215	46 009 949
1 000 000 000	50 847 534	50 847 455

Для тех, кто хоть немного знаком с теорией функций, могу добавить, что $R(x)$ — целая функция $\log x$, задаваемая быстро сходящимся степенным рядом

$$R(x) = 1 + \sum_{n=1}^{\infty} \frac{1}{n\zeta(n+1)} \frac{(\log x)^n}{n!},$$

где $\zeta(n+1)$ — ζ-функция Римана (8).

Здесь мне хотелось бы подчеркнуть, что приближения Гаусса и Лежандра были получены исключительно эмпирически и что даже Риман, хотя и пришел к функции $R(x)$ в результате теоретических рассуждений, не доказал асимптотического закона распределения простых чисел. Впервые эта теорема была доказана в 1896 г. Адамаром и (независимо) Валле Пусеном; доказательства этих авторов основывались на работе Римана. Рассматривая вопрос о предсказуемости простых чисел, мне хотелось бы привести еще несколько числовых примеров. Как уже говорилось выше, вероятность того, что число x является простым, равна приблизительно $1/\log x$, т. е. число простых чисел на интервале a, лежащем в окрестности числа x, должно быть равно примерно $a/\log x$; безусловно, интервал этот должен быть достаточно велик, чтобы статистика имела смысл, и в то же время мал по сравнению с x. Например, можно ожидать, что на интервале между 100 000 000 и 100 000 000 + + 150 000 имеется 8142 простых числа, поскольку

$$\frac{150\,000}{\log(100\,000\,000)} = \frac{150\,000}{18\,427\ldots} \approx 8142.$$

И соответственно вероятность того, что два произвольных числа в окрестности x оба будут простыми, равна приблизительно $1/(\log x)^2$. Отсюда следует, что число простых чисел-двойников (т. е. пар простых чисел, отличающихся

друг от друга на 2, как, например, 11 и 13, 59 и 61) на интервале между x и $x + a$, по всей вероятности, будет равно приблизительно $a/(\log x)^2$. В действительности их может быть несколько больше, поскольку тот факт, что n — уже простое число, в некоторой степени изменяет вероятность того, что $n + 2$ — простое число (в этом случае $n + 2$ — несомненно, нечетное число). Простым эвристическим рассуждением получаем, что ожидаемое число простых чисел-двойников на интервале $[x, x + a]$ должно быть равно $C \cdot a/(\log x)^2$, где C — константа, равная приблизительно 1,3 (точнее C — 1, 3203236316...). Таким образом, на интервале между 100 000 000 и 100 000 000 + 150 000 должно быть

$$(1{,}32\ \ldots)\frac{150\,000}{(18\,427)^2} \approx 584$$

пары простых чисел-двойников. В нижеследующей таблице приведены результаты, полученные Джоунсом, Лалом и Бландоном (10), показывающие точное число простых чисел и простых чисел-двойников на этом интервале, а также на интервалах такой же длины, но взятых в окрестностях более высоких степеней 10:

Интервал	Простые числа		Простые числа-двойники	
	предполагаемое количество	фактическое количество	предполагаемое количество	найдено
100 000 000— 100 150 000	8142	8154	584	601
1 000 000 000— 1 000 150 000	7238	7242	461	466
10 000 000 000— 10 000 150 000	6514	6511	374	389
100 000 000 000— 100 000 150 000	5922	5974	309	276
1 000 000 000 000— 1 000 000 150 000	5429	5433	259	276
10 000 000 000 000— 10 000 000 150 000	5011	5065	221	208
100 000 000 000 000— 100 000 000 150 000	4653	4643	191	186
1 000 000 000 000 000— 1 000 000 000 150 000	4343	4251	166	161

Как можно заметить, соответствие с теорией исключительное, что особенно удивительно в случае простых чисел-двойников, поскольку пока еще даже не доказано, что таких пар существует бесконечное множество, не говоря уже о том, что они распределяются согласно этому гипотетическому закону.

И наконец, в связи с проблемой предсказуемости простых чисел мне хотелось бы рассмотреть еще один вопрос, а именно, вопрос об интервалах между простыми числами. Просматривая таблицы простых чисел, можно иногда встретить необыкновенно большие интервалы между ними, например между 113 и 127, совершенно свободные от простых чисел. Пусть $g(x)$ — величина наибольшего свободного от простых чисел интервала или «пробела» среди чисел, не превосходящих x. Например, наибольшим интервалом в пределах 200 является вышеупомянутый интервал между 113 и 127, следовательно $g(200) = 14$. Естественно, число $g(x)$ растет неравномерно, но в результате

эвристических рассуждений мы получаем асимптотическую формулу $g(x) \sim (\log x)^2$. На нижеследующем графике можно видеть, насколько хорошо, несмотря на свою исключительную нерегулярность, функция $g(x)$ следует предполагаемому поведению (рис. 5).

Пока я привел достаточные основания лишь моего утверждения относительно подчиненности простых чисел определенным законам и не пытался подкрепить доказательствами правоту утверждения относительно их недисциплинированности. Кроме того, я все еще не выполнил обещания, данного мной в названии настоящей статьи, познакомить вас с первыми 50 миллионами простых чисел, перечислив пока всего лишь несколько тысяч. Поэтому давайте сравним графики функции $\pi(x)$ и приближений Лежандра, Гаусса и Римана в пределах 10 миллионов (12). Поскольку эти четыре функции лежат настолько близко друг к другу, что их графики неразличимы для вооруженного глаза, что мы уже могли наблюдать на графиках, построенных для первых 50 000 чисел, я нанес на график лишь те участки, где эти функции разнятся между собой (рис. 6). Я думаю, на этом графике прекрасно показано, во что можно впутаться, приняв решение заниматься изучением теории чисел. Как можно видеть, для малых x (приблизительно вплоть до 1 000 000) приближение Лежандра

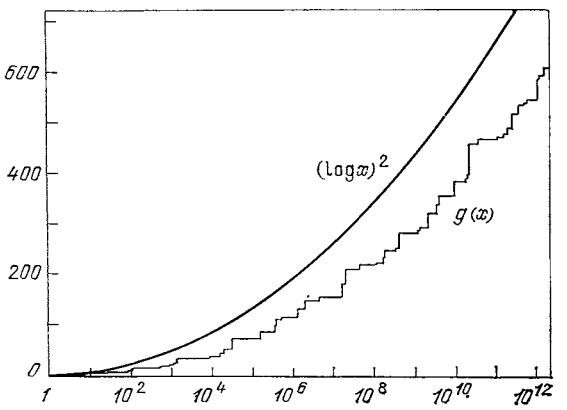

Рис. 5

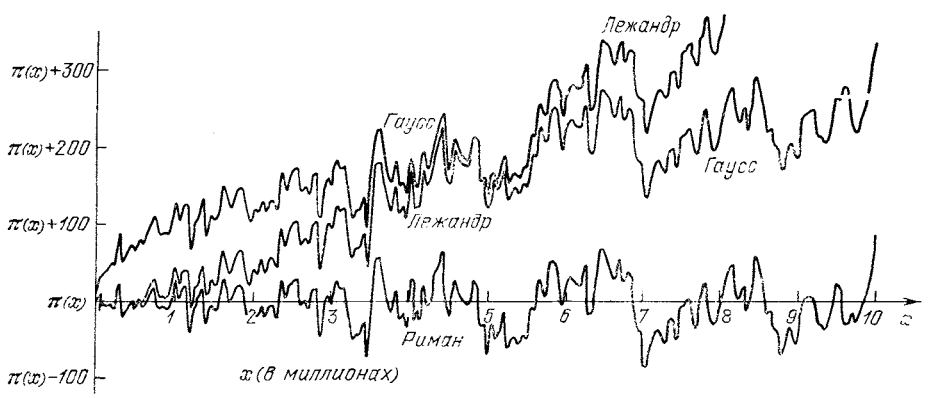

Рис. 6

$x(\log x - 1{,}08366)$ будет значительно лучше, чем гауссово приближение $\mathrm{Li}(x)$ но после 5 миллионов лучшим приближением будет $\mathrm{Li}(x)$, и можно показать, что по мере роста функция $\mathrm{Li}(x)$ будет оставаться лучшим приближением.

Среди первых 10 миллионов чисел мы имеем всего 600 000 простых чисел. Для того чтобы продемонстрировать вам обещанные 50 миллионов простых чисел, я должен перебрать не 10 миллионов, а целый миллиард чисел. На этом интервале график функции $R(x) - \pi(x)$ имеет вид, показанный на рис. 7. Амплитуда колебаний функции $R(x) - \pi(x)$ постепенно нарастает, но даже для этих почти непостижимо огромных значений x она никогда не выходит за пределы нескольких сотен. Здесь же следует упомянуть еще один

факт относительно числа простых чисел $\pi(x)$. На графике видно, что для 10 миллионов чисел приближение Гаусса всегда *превосходит* значения функции $\pi(x)$; и такое положение наблюдается вплоть до 1 миллиарда, что подтверждает нижеследующий график (где приведенные выше данные представлены в логарифмическом виде) (рис. 8). При виде этого графика создается впечатление, что если x возрастает, разность $\mathrm{Li}(x) - \pi(x)$ неуклонно стремится к бесконечности, т. е. логарифмический интеграл $\mathrm{Li}(x)$ постоянно завышает оценку числа простых чисел, не превосходящих x (это соответствовало бы нашему замечанию, что $R(x)$ — приближение, лучшее, чем $\mathrm{Li}(x)$, поскольку $R(x)$ всегда меньше, чем $\mathrm{Li}(x)$). Но это ошибочно: можно показать, что существуют такие точки, в которых амплитуда колебания функции $R(x) - \pi(x)$ настолько велика, что $\pi(x)$ фактически становится больше, чем $\mathrm{Li}(x)$. Пока еще ни одно из таких чисел найдено не было и, возможно, так и не будет найдено; но Литтлвуд доказал, что такие числа существуют, а Скью (14) доказал, что имеется подобное число, меньшее, чем

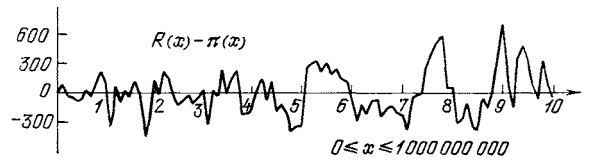

Рис. 7

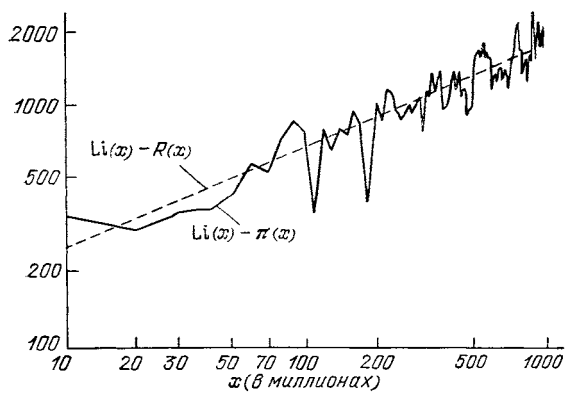

Рис. 8

$$10^{10^{10^{34}}}$$

(число, о котором Харди как-то сказал, что это, несомненно, наибольшее из всех чисел, служивших когда-либо каким-либо определенным целям в математике). Во всяком случае этот пример показывает, насколько опрометчивым может быть решение основывать свои выводы относительно простых чисел на численных данных.

В заключение своей лекции мне хотелось бы поговорить о некоторых теоретических результатах, полученных относительно $\pi(x)$, с тем чтобы у вас не осталось ощущения, что речь здесь шла исключительно об экспериментальной математике. Непосвященному может показаться, что свойство числа быть простым слишком уж малозначащее, чтобы можно было построить некоторую теорию. Это было опровергнуто еще 2200 лет тому назад Евклидом, который доказал существование бесконечно большого множества простых чисел. Его доказательство можно сформулировать одной фразой: если бы существовало конечное множество простых чисел, то, умножив их друг на друга и прибавив к результату 1, мы получили бы число, не делящееся ни на одно из простых чисел, а это невозможно. В 18 столетии Эйлер развил дальше теорию простых чисел, а именно, он доказал, что сумма величин, обратных простым числам, расходится, т. е. в конечном итоге превосходит любое первоначально заданное число. В своем, также очень простом, доказательстве Эйлер использовал функцию

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \ldots,$$

значение которой для изучения функции $\pi(x)$ было полностью осознано позднее, лишь с появлением работы Римана. Интересно заметить, что, несмотря на тот факт, что сумма обратных всех простых чисел расходится, эта сумма,

взятая по всем известным простым числам (скажем, первым 50 миллионам), будет меньше четырех (15).

Первый выдающийся результат на пути к обоснованию асимптотического закона был получен Чебышёвым (16) в 1850 г., который показал, что для достаточно большого x

$$0{,}89\frac{x}{\log x} < \pi(x) < 1{,}11\frac{x}{\log x},$$

т. е. асимптотический закон корректен с относительной ошибкой, не превышающей 11 %. В своем доказательстве Чебышёв использовал биномиальные коэффициенты, само же доказательство настолько красиво, что я не могу не привести его (с некоторыми заслуживающими внимания константами), хотя бы в краткой и упрощенной форме.

С одной стороны, докажем, что

$$\pi(x) < 1{,}7\frac{x}{\log x}.$$

Это неравенство справедливо для $x < 1200$. Предположим по индукции, что наше неравенство справедливо для $x < n$, и рассмотрим средний биномиальный коэффициент

$$\binom{2n}{n}$$

Поскольку

$$2^{2n} = (1+1)^{2n} = \binom{2n}{0} + \binom{2n}{1} + \ldots + \binom{2n}{n} + \ldots + \binom{2n}{2n},$$

этот коэффициент не превышает 2^{2n}. С другой стороны,

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \frac{(2n)\times(2n-1)\times\ldots\times 2\times 1}{(n\times(n-1)\times\ldots\times 2\times 1)^2}$$

В числителе мы имеем все простые числа p, меньшие, чем $2n$, в знаменателе же ни одно из простых чисел не может быть больше n. Следовательно, $\binom{2n}{n}$ делится на любое простое число, лежащее в интервале от n до $2n$:

$$\prod_{n<p\leqslant 2n} p \,\Big|\, \binom{2n}{n}.$$

Но произведение имеет $\pi(2n) - \pi(n)$ множителей, каждый из которых больше, чем n, поэтому мы получаем

$$n^{\pi(2n)-\pi(n)} \leqslant \prod_{n<p\leqslant 2n} p \leqslant \binom{2n}{n} < 2^{2n}$$

или, логарифмируя,

$$\pi(2n) - \pi(n) < \frac{2n\log 2}{\log n} < 1{,}39\frac{n}{\log n}.$$

По индукции эта теорема справедлива для n, следовательно $\pi(n) < 1{,}7\times$ $\times(n/\log n)$. Складывая эти соотношения, мы получаем

$$\pi(2n) < 3{,}09\frac{n}{\log n} < 1{,}7\frac{2n}{\log(2n)},$$

откуда следует, что данная теорема справедлива также и для $2n$. И, наконец, поскольку

$$\pi(2n+1) \leqslant \pi(2n) + 1 < 3{,}09\frac{n}{\log n} + 1 \leqslant 1{,}7\frac{2n+1}{\log(2n+1)}, \qquad n > 1200,$$

она будет справедлива также и для $2n+1$.

Для доказательства левого неравенства воспользуемся одной простой леммой, легко доказываемой с помощью формулы для степени простого числа p, на которую делится $n!$ (17).

Лемма. *Пусть p — простое число. Если p^{ν_p} — наибольшая степень числа p, на которую делится $\binom{n}{k}$, то*

$$p^{\nu_p} \leqslant n.$$

Следствие. *Каждый биномиальный коэффициент $\binom{n}{k}$ удовлетворяет соотношению*

$$\binom{n}{k} = \prod_{p \leqslant n} p^{\nu_p} \leqslant n^{\pi(n)}.$$

Сложив неравенства этого следствия для всех биномиальных коэффициентов $\binom{n}{k}$ с заданным n, мы имеем

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} \leqslant (n+1) \cdot n^{\pi(n)}.$$

Прологарифмировав последнее соотношение, получаем, что

$$\pi(n) \geqslant \frac{n \log 2}{\log n} - \frac{\log (n+1)}{\log n} > \frac{2}{3} \frac{n}{\log n}, \qquad n > 200.$$

В заключение мне хотелось бы сказать несколько слов о работе Римана. Несмотря на то, что Риман не дал доказательства теоремы о простых числах, ему удалось сделать нечто во многих отношениях более удивительное — он вывел *точную* формулу для $\pi(x)$. Эта формула имеет следующий вид:

$$\pi(x) + \frac{1}{2}\pi(\sqrt{x}) + \frac{1}{3}\pi(\sqrt[3]{x}) + \ldots = \mathrm{Li}(x) - \sum_{\rho} \mathrm{Li}(x^{\rho}),$$

где сумма берется по корням функции $\zeta(s)$ (18). Эти корни (не считая так называемых «тривиальных» корней $\rho = -2, -4, -6, \ldots$, влияние которых на формулу ничтожно) являются комплексными числами, вещественные части которых лежат между 0 и 1. Первые десять из них имеют следующий вид:

$$p_1 = \frac{1}{2} + 14{,}134725i,$$

$$p_2 = \frac{1}{2} + 21{,}022040i,$$

$$p_3 = \frac{1}{2} + 25{,}010856i,$$

$$p_4 = \frac{1}{2} + 30{,}424878i,$$

$$p_5 = \frac{1}{2} + 32{,}935057i,$$

$$\bar{p}_1 = \frac{1}{2} - 14{,}134725i,$$

$$\bar{p}_2 = \frac{1}{2} - 21{,}022040i,$$

$$\bar{p}_3 = \frac{1}{2} - 25{,}010856i,$$

$$\bar{p}_4 = \frac{1}{2} - 30{,}424878i,$$

$$\bar{p}_5 = \frac{1}{2} - 32{,}935057i.$$

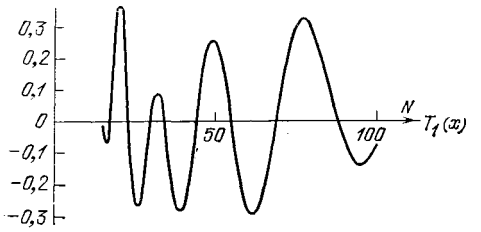

Рис. 9

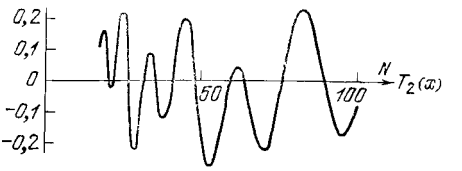

Рис. 10

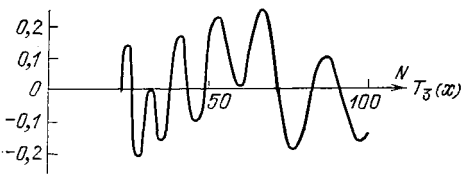

Рис. 11

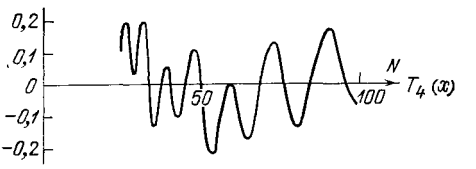

Рис. 12

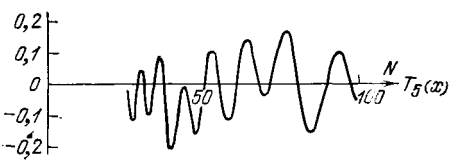

Рис. 13

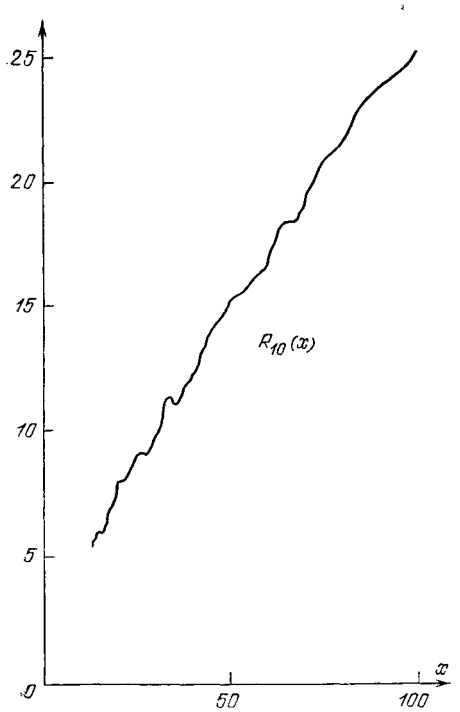

Рис. 14

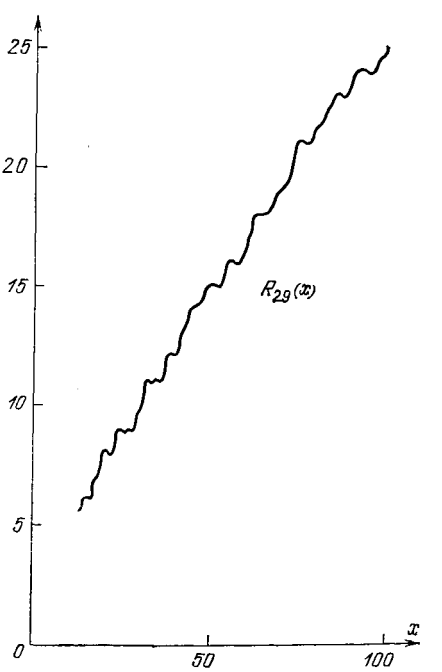

Рис. 15

Легко показать, что каждому корню отвечает комплексно сопряженный, но то, что вещественная часть каждого корня равна точно 1/2, пока еще не доказано. Это известная гипотеза Римана, значение которой для теории чисел огромно (20). Правильность этой гипотезы подтвердилась для 7 миллионов корней.

С помощью упомянутой нами выше функции Римана $R(x)$ формулу Римана можно записать в следующем виде:

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

В виде k-го приближения к функции $\pi(x)$ имеем функцию

$$R_k(x) = R(x) + T_1(x) + T_2(x) + \ldots + T_k(x),$$

где $T_n(x) = -R(x^{p_n}) - R(x^{\bar{p}_n})$ — доля n-й пары корней дзета-функции. Для каждого n функция $T_n(x)$ — это гладкая знакопеременная функция от x. На рис. 9—13 приведены графики для первых пяти функций $T_n(x)$.

Отсюда следует, что $R_k(x)$ — также гладкая функция для каждого k. С ростом k эти функции приближаются к $\pi(x)$. Рассмотрим для примера графики 10-го (рис. 14) и 29-го (рис. 15) приближений. Сравнивая эти кривые с графиком $\pi(x)$ для первых 100 чисел (см. рис. 1), мы получим картину, показанную на рис. 16.

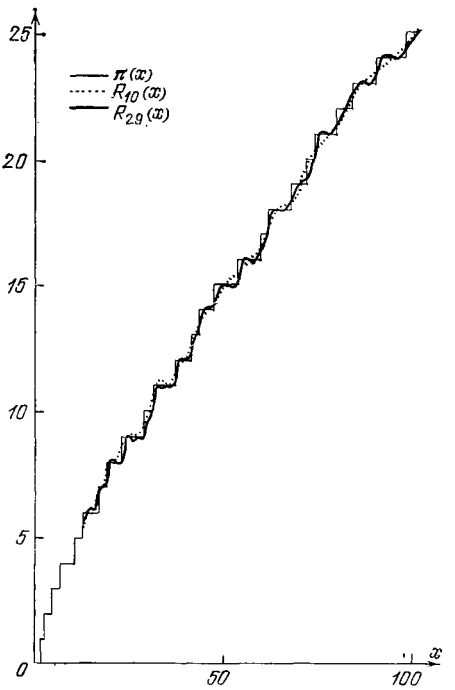

Рис. 16

Я надеюсь, что с помощью этого и всех остальных приведенных мной графиков мне удалось не только раскрыть для вас безграничное очарование простых чисел, но и познакомить с некоторыми сюрпризами, которые они нам преподносят и запас которых неиссякаем.

ЗАМЕЧАНИЯ

(1) J. M. G a n d h i. Formulae for the n-th prime.— Proc. Washington State Univ. Conf. on Number Theory, Washington State Univ., Pullman, Wash., 1971, p. 96—106.

(2) J. P. J o n e s. Diophantine representation of the set of prime numbers.— Notices of the AMS, 1975, 22, p. A-326.

(3) Имеются веские основания тому факту, что многие числа этого списка имеют вид $M_k = 2^k - 1$. Согласно теореме Лукаса число M_k, $k > 2$, будет простым тогда и только тогда, когда M_k будет делителем числа L_{k-1}, где числа L_n определяются по индукции, исходя из того факта, что $L_1 = 4$, а $L_{n+1} = L_n^2 - 2$ (отсюда $L_2 = 14$, $L_3 = 194$, $L_4 = 37\,634$, ...), следовательно, гораздо легче проверить, будет ли M_k простым числом, нежели подвергать проверке еще одно число той же величины.

Простые числа вида $2^k - 1$ (для которых само k обязательно должно быть простым числом) называются простыми числами Мерсенна (по имени французского математика Мерсенна, предложившего в 1644 г. список таких простых чисел вплоть до 10^{79}, но корректный только до 10^{18}), и имеют большое значение в связи с совершенно иной проблемой теории чисел. Евклид обнаружил, что когда $2^p - 1$ — простое число, то число $2^{p-1}(2^p - 1)$ является «совершенным», т. е. оно равно сумме своих собственных делителей (например, $6 = 1 + 2 + 3$, $28 = 1 + 2 + 4 + 7 + 14$, $496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$). Эйлер же показал, что каждое четное совершенное число имеет такой вид.

Пока неизвестно, существует ли вообще хоть одно нечетное совершенное число; если оно и существует, его значение должно быть не меньше чем 10^{100}. Существует точно 24 значения $p < 20\,000$, для которых $2^p - 1$ — простое число [1]).

(4) C. F. Gauss. Werke II.— 1892, S. 444—447. См. также L. J. Goldsgtein. A history of the prime number theorem.— Amer. Math. Monthly, 1973, 80, p. 599—615.

(5) A. M. Legendre. Essai sur la theorie de Nombres, 2nd edition.— Paris, 1808, p. 394.

(6) Точнее

$$\mathrm{Ls}\,(x) - 1{,}5 < \mathrm{Li}(x) < \mathrm{Ls}(x),$$

т. е. разность между $\mathrm{Li}(x)$ и $\mathrm{Ls}(x)$ ограничена. Следует также отметить, что логарифмический интеграл часто определяют как главное значение по Коши интеграла

$$\mathrm{Li}\,(x) = \int_0^x \frac{dt}{\log t} \underset{\text{DEF}}{=\!=} \lim_{\varepsilon \to 0} \left(\int_0^{1-\varepsilon} \frac{dt}{\log t} + \int_{1-\varepsilon}^{x} \frac{dt}{\log t} \right).$$

Этот интеграл отличается от интеграла, приведенного в тексте, только константой.

(7) Коэффициенты получаются следующим образом: коэффициент числа $\mathrm{Li}(\sqrt[n]{x})$ равен $+1/n$, если n — произведение четного числа различных простых чисел; коэффициент равен $-1/n$, если n — произведение нечетного числа различных простых чисел, и коэффициент равен 0, если n содержит кратные простые сомножители.

(8) Раманужан предложил следующие формулы для этой функции:

$$R\,(x) = \sum_0^\infty \frac{(\log x)^t\, dt}{t\Gamma\,(t+1)\,\zeta\,(t+1)}$$

($\zeta(s)$ — дзета-функция Римана, а $\Gamma(s)$ — гамма-функция) и

$$R\,(e^{2\pi x}) \doteq \frac{2}{\pi}\left(\frac{2}{B_2}\,x + \frac{4}{3B_4}\,x^3 + \frac{6}{5B_6}\,x^5 + \ldots\right) = \frac{2}{\pi}\left(12x + 40x^3 + \frac{252}{5}\,x^5 + \ldots\right)$$

(B_k — k-число Бернулли, символ $\doteq$ означает, что при $x \to \infty$ разность между правой и левой частями стремится к 0). См. G. H. Hardy. Ramanujan, Twelve Lectures on Subjects Suggested by His Life and Work.— Cambridge University Press, 1940, Chapter 2.

(9) А именно, вероятность того, что для произвольно выбранной пары чисел (m, n) как m, так и $n \not\equiv 0 \bmod p$, очевидно, равна $[(p-1)/p]^2$; для произвольного числа n вероятность того, что и n, и $n+2 \not\equiv 0 \bmod p$ равны $1/2$, если $p = 2$, и $(p-2)/p$, если $p \neq 2$. Следовательно, вероятность того, что n и $n+2$ по модулю p суть пара простых чисел двойников, отличается от соответствующей вероятности для двух произвольных чисел m и n на множитель

$$\frac{p-2}{p} \cdot \frac{p^2}{(p-1)^2},$$

если $p \neq 2$, и на множитель 2, если $p = 2$. Таким образом, мы увеличиваем нашу вероятность на множитель

$$C = 2 \cdot \prod_{p>2} \frac{p^2-2p}{p^2-2p+1} = 1{,}32032, \quad p\text{— простое число.}$$

С боле подробным изложением этого доказательства можно ознакомиться в монографии Hardy and Wright. An introduction to the theory of numbers.— Oxford: Clarendon Press, 1960, § 22.30, p. 371—373.

(10) M. F. Jones, M. Lal, W. J. Blundon. Statistics on certain large primes.— Math. Comp. 1967, **21**, p. 103—107.

(11) D. Shanks. On maximal gaps between successive primes.— Math. Comp. 1967, **18**, p. 646—651.

График функции $g(x)$ построен на основании данных, взятых из таблиц, приведенных в следующих работах: L. J. Lander, T. R. Parkin. On first appearance of prime

[1]) См. сноску на с. 117. (*Прим. перев.*)

differences.— Math. Comp. 1967, **21**, p. 483—488. R. P. B r e n t. The first occurrence of large gaps between successive primes.— Math. Comp. 1973, **27**, p. 959—963.

(12) Данные для построения этого графика взяты из таблицы простых чисел, предлагаемой Лемером: D. N. L e h m e r. List of prime numbers from 1 to 10 006 721.— New York: Hafner Publishing Co., 1956.

(13) Значения $\pi(x)$ для построения этого и следующего за ним графиков взяты из работы D. C. M a p e s. Fast method for computing the number of primes less than a given limit.— Math. Comp., 1963, **17**, p. 179—185.

В отличие от использованных нами в предыдущем графике данных, предлагаемых Лемером, значения $\pi(x)$ в данном случае находились по формуле, а не простой выборкой простых чисел, не превосходящих x.

(14) S. S k e w e s. On the difference $\pi(x) - \mathrm{li}(x)$ (I).— J. London Math. Soc., 1933, **8**, p. 277—283.

В своем доказательстве Скьюз исходил из того факта, что гипотеза Римана, речь о которой пойдет ниже, справедлива. Двадцать два года спустя (On the difference $\pi(x) - \mathrm{li}(x)$ II.— Proc. Lond. Math. Soc., (3), 1955, **5**, p. 48—70), уже не опираясь на гипотезу Римана, он доказал, что существует x, меньшее (тем не менее значительно превосходящее указанный в тексте предел), чем

$$10^{10^{10^{964}}},$$

для которого $\pi(x) > \mathrm{Li}(x)$. Коэн и Мейхью снизили этот предел до

$$10^{10^{10^{529,7}}},$$

а Леман — до $1{,}65 \times 10^{1165}$ (см. On the difference $\pi(x) - \mathrm{li}(x)$.— Acta Arithm. 1966, **11**, p. 397—410). Леман даже показал, что на интервале между $1{,}53 \times 10^{1165}$ и $1{,}65 \times 10^{1165}$ существует отрезок не менее чем из 10^{500} чисел, на котором $\pi(x) > \mathrm{Li}(x)$. На основании его исследований можно сделать заключение, что, вероятно, в окрестности числа $6{,}663 \times 10^{370}$ существует число, для которого $\pi(x) > \mathrm{Li}(x)$, и нет такого числа, которое обладало бы подобными свойствами и было бы меньше чем 10^{20}.

(15) А именно (как предположил Гаусс, 1796 г., и доказал Мертенс, 1874 г.),

$$\sum_{p<x} \frac{1}{p} = \log\log x + C + \varepsilon(x),$$

где $\varepsilon(x) \to 0$, если $x \to \infty$, а константа $C \approx 0{,}261497$. Это выражение меньше, чем 3,3, если $x = 10^9$, но даже при $x = 10^{18}$ это выражение все еще меньше, чем 4.

(16) П. Л. Ч е б ы ш ё в. Избранные труды — М.: Изд. АН СССР, 1955, с. 9—32; с. 33—54.

(17) Наибольшая степень простого числа p, на которое делится $p!$, равна $p^{[n/p]+[n/p^2]+\cdots}$, где $[x]$ — наибольшее целое число $\leqslant x$. Таким образом, используя принятые в настоящей лемме обозначения, мы имеем

$$\nu_p = \sum_{r \geqslant 1} \left(\left[\frac{n}{p^r} \right] - \left[\frac{k}{p^r} \right] - \left[\frac{n-k}{p^r} \right] \right).$$

Каждое слагаемое этой суммы равно либо 0, либо 1; и совершенно очевидно, равно 0, если $r > (\log n / \log p)$ (поскольку в этом случае $[n/p^r] = 0$). Поэтому $\nu_p \leqslant (\log n / \log p)$, откуда следует наше утверждение.

(18) Приведенная нами ранее формула $\zeta(s) = 1 + 1/2^s + 1/3^s + \ldots$ имеет смысл только в том случае, когда s — комплексное число, вещественная часть которого больше чем 1 (поскольку данный ряд сходится только при этих значениях s), и в этой области $\zeta(s)$ не имеет ни одного нуля. Но функцию $\zeta(s)$ можно аналитически продолжить на всю комплексную плоскость, с тем чтобы можно было говорить о нулях в этой плоскости. Наипростейший способ расширения области определения функции $\zeta(s)$, по меньшей мере до полуплоскости $\mathrm{Re}(s) > 0$, осуществляется с помощью тождества

$$(1 - 2^{1-s})\,\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \ldots - 2\left(\frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \ldots \right) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s},$$

справедливого при $\mathrm{Re}(s) > 1$, и последующего наблюдения, что ряд в правой части сходится для всех s, имеющих положительную вещественную часть. После этого «интересные» корни дзета-функции, т. е. корни $\rho = \beta + i\gamma$, $0 < \beta < 1$, можно найти из уравнений

$$\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^{\beta}} \cos(\gamma \log n) = 0,$$

$$\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^{\beta}} \sin(\gamma \log n) = 0.$$

Сумма, взятая по корням ρ в формуле Римана, не является абсолютно сходящейся, поэтому ее суммирование следует выполнять в правильной последовательности (т. е. в соответствии с возрастающим абсолютным значением $\mathrm{Im}(\rho)$).

И наконец, следует заметить, что хотя Риман и предложил точную формулу для $\pi(x)$ еще в 1859 г., доказательство ее было получено (фон Мангольдтом) лишь в 1903 г.

(19) Эти корни были найдены еще в 1903 г. Грэмом (J.-P. G r a m. Sur les zeros de la fonction $\zeta(s)$ de Riemann.— Acta Math., 1903, **27**, 289—304.

Монография H. M. E d w a r d s. Riemann's zeta function.— New York, Academic Press, 1974 предлагает очень красивое изложение теории дзета-функции Римана.

(20) Из гипотезы Римана следует, что погрешность гауссовского приближения $\mathrm{Li}(x)$ к $\pi(x)$ не превышает величины $x^{1/2} \cdot \log x$, умноженной на некоторую константу (что эквивалентно нашему утверждению). До сих пор пока еще не установлено, будет ли эта погрешность меньше x^c при некоторой константе $c < 1$.

(21) Этот и все последующие графики взяты из работы H. R i e s e l and G. G ö h l. Some calculations related to Riemann's prime number formula.— Math. Comp. 1970, **24**, p. 969—983.