И. Р. Шафаревич, Избранные главы алгебры (продолжение), *Матем. обр.*, 1998, выпуск 1, 2–21

Избранные главы алгебры (продолжение)

И. Р. Шафаревич

В российском (и ранее советском) математическом образовании существует замечательная традиция: крупные ученые, внесшие существенный вклад в развитие математики, создают произведения, рассчитанные на школьников, заинтересованных этой наукой. Мы продолжаем публикацию журнального варианта "Избранных глав алгебры", написанных выдающимся русским математиком академиком РАН И. Р. Шафаревичем. Надеемся, что материал заинтересует старших школьников и учителей, работающих по углубленной программе. Главы I, II, III были опубликованы соответственно в первом, втором и третьем номерах журнала.

Глава IV. Простые числа

§1. Бесконечность числа простых чисел

В этой главе мы вернемся к вопросу, разбиравшемуся в главе I. Там было доказано, что натуральное число единственным образом разлагается на простые сомножители. Поэтому с точки зрения операции умножения, простые числа — это простейшие элементы, из которых операцией умножения получаются все натуральные числа, подобно тому, как при помощи операции сложения они все получаются из числа 1. С этой точки зрения понятен интерес к совокупности простых чисел. В первом десятке натуральных чисел находится четыре простых: 2, 3, 5, 7. Дальше можно находить простые числа, по очереди деля каждое число на все уже найденные меньшие простые числа, чтобы выяснить, будет ли оно простым. Таким образом, мы найдем в первой сотне 25 простых чисел:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

Как далеко продолжается этот ряд? Вопрос возник еще в античности. У Евклида мы находим ответ:

Теорема 1. Число простых чисел бесконечно.

Мы приведем несколько доказательств этой теоремы.

Первое доказательство — то, которое содержится в "Началах" Евклида. Пусть мы нашли n простых чисел: $p_1, p_2, \ldots, p_n$. Рассмотрим число $N = p_1 p_2 \ldots p_n + 1$. Как мы видели в §2 главы I, каждое число имеет по крайней мере один простой делитель. В частности, N имеет простой делитель. Но им не может быть ни одно из чисел $p_1, \ldots, p_n$. Действительно, пусть это будет p_i. Тогда и $N - p_1 \ldots p_n$ должно делиться на p_i, а так как $N - p_1 \ldots p_n = 1$, то это невозможно. Таким образом, этот простой делитель отличен от всех p_i, $i = 1, \ldots, n$, и, значит, за каждыми n простыми числами следует еще одно простое число. Это доказывает теорему.

Второе доказательство. Согласно теореме параграфа "Алгебра множеств" главы III число чисел, меньших заданного числа N и взаимно простых с ним, задается формулой

$$N\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_n}\right), \tag{1}$$

где $p_1,\dots,p_n$ — все простые делители числа N. Докажем теорему от противного. Предположим, что число простых чисел конечно и $p_1,\dots,p_n$ — это все простые числа. Положим $N=p_1\dots p_n$. Подставляя это выражение в формулу (1), мы получим для каждого множителя p_i $\left(1-\frac{1}{p_i}\right)$ выражение p_i-1, а для всего произведения (1) выражение $(p_1-1)(p_2-1)\dots(p_n-1)$. Так как мы знаем, что существуют простые числа, большие 2 (например, 3), то это число *больше* 1. Таким образом, существует число a, меньшее N, взаимно простое с N и отличное от 1. Но a имеет хотя бы один простой делитель, который должен содержаться среди чисел $p_1,\dots,p_n$, поэтому a не может быть взаимно простым с N. Мы получили противоречие, которое доказывает теорему.

Бесконечная последовательность простых чисел, с другой стороны, довольно редко располагается среди натуральных чисел. Например, в ней существуют сколь угодно большие "пустоты", то есть можно найти (достаточно далеко) любое заданное число последовательных чисел, не являющихся простыми. Например, n чисел: $(n+1)!+2$, $(n+1)!+3,\dots,(n+1)!+n+1$ очевидно не являются простыми — первое из них делится на 2, второе — на 3, последнее — на $n+1$.

Некоторое время пытались найти формулу, выражающую простые числа. Например, Эйлер нашел удивительный многочлен x^2+x+41, который при 40 значениях x — от 0 до 39 — принимает простые значения. Однако очевидно, что при $x=40$ он принимает непростое значение 41^2. Нетрудно убедиться, что вообще не может существовать многочлен $f(x)$, который при всех целых значениях $x=0,1,2,\dots$ принимал бы простые значения (не говоря уж о том, чтобы его значения давали *все* простые числа). Покажем это на примере многочлена второй степени ax^2+bx+c с целыми коэффициентами a,b,c. Предположим, что при $x=0$ многочлен принимает простое значение c. Тогда при любом $x=kc$ его значение $ak^2c^2+bkc+c$ делится на c. При этом от силы еще при одном значении k (кроме $k=0$) он может принимать то же значение c, как вы сами легко убедитесь. Более того, не существует многочлена $f(x)=ax^2+bx+c$, все значения которого являются простыми при всех целых x, *начиная с некоторой границы.* Действительно, предположим, что значения многочлена $f(x)$ являются простыми для всех целых $x\geq m$. Положим $x=y+m$, $f(y+m)=g(y)$; тогда все значения многочлена $g(y)$ по предположению являются простыми при всех целых $y\geq 0$, а коэффициенты его по-прежнему целые, так как $g(y)=a(y+m)^2+b(y+m)+c$. То же рассуждение применимо и к многочлену произвольной степени n : $f(x)=a_0+a_1x+\dots+a_nx^n$. Если все его значения при $x\geq 0$ и целых являются простыми, то значит и $f(0)=a_0=p$ является простым. Тогда при любом целом k значения $f(kp)=p+a_1kp+\dots+a_n(kp)^n$ делятся на p. Они могут совпадать со значением p только, если $p+a_1kp+\dots+a_n(kp)^n=p$, то есть $a_1+a_2kp+\dots+a_n(kp)^{n-1}=0$, а это — уравнение степени $n-1$ относительно k и

согласно теореме 3 главы II имеет самое большее $n-1$ корень. При всех остальных значениях k число $f(kp)$ делится на p и отлично от p, то есть не является простым.

Если же предположим, что значения многочлена $f(x)$ являются простыми лишь для целых значений $x \geq m$, где m – некоторое число, то можем положить $x = y+m$ и $f(y+m) = g(y)$. Многочлен $g(y) = a_0 + a_1(y+m) + \ldots + a_n(y+m)^n$ получается раскрытием всех скобок по формуле бинома и приведения подобных членов. Поэтому его коэффициенты опять целые, но он принимает простые значения уже для всех целых $y \geq 0$, так что мы опять приходим к противоречию.

Можно доказать, что и для любого числа неизвестных k не можеть существовать многочлен с целыми коэффициентами от k неизвестных, все значения которого при всех натуральных значениях неизвестных являются простыми числами. Тем не менее оказалось, что существует многочлен степени 25 от 26 неизвестных, обладающий следующим свойством: если отобрать значения, которые он принимает при целых неотрицательных значениях неизвестных и которые сами положительны, то их множество совпадает с множеством простых чисел. Так как 26 равно числу букв латинского алфавита, то можно неизвестные обозначить этими буквами: $a, b, \ldots, x, y, z$. Тогда многочлен имеет вид:

$$
\begin{gathered}
F(a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z) = \\
= (k+2)\{1-[wz+h+j-q]^2 - [(gk+2g+k+1)(h+j)+h_z]^2 - \\
-[2n+p+q+z-e]^2 - [16(k+1)^3(k+2)(n+1)^2+1-f^2]^2 - \\
-[e^3(t+2)(a+1)^2+1-o^2]^2 - [(a^2-1)y^2+1-x^2]^2 - \\
-[16r^2y^4(a^2-1)+1-u^2]^2 - [(a+u^2(u^2-a^2)-1)(n+4dy)^2+1-(x+cu)^2]^2 - \\
-[n+l+v-y]^2 - [(a-1)l^2+1-m^2]^2 - [ai+k+1-l-i]^2 - \\
-[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m^2] - \\
-[q+y(a-p-1)+s(2ap+2a-p^2-2p-20-x]^2 - \\
-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\}.
\end{gathered}
$$

Этот многочлен выписан здесь только для того, чтобы поразить воображение читателя. Число переменных в нем очень велико. Можно показать, что он принимает также отрицательные значения $-m$, где m не просто. Поэтому и он не дает нам представления о последовательности простых чисел.

Длительные попытки склонили большинство математиков к убеждению, что не существует более или менее простой формулы, описывающей последовательность простых чисел. "Явные формулы", описывающие простые числа, существуют, но они используют объекты, о которых мы знаем еще меньше, чем о простых числах. Поэтому внимание математиков сконцентрировалось на характеристике последовательности простых чисел "в целом", а не "поштучно". Эту постановку вопроса мы разъясним в следующих параграфах.

Задачи

1. Докажите бесконечность числа простых чисел вида $3s+2$.

2. То же — для простых чисел вида $4s+3$.

3. Докажите, что любые два числа $2^{2^n}+1$ и $2^{2^m}+1$ взаимно просты. Выведите отсюда еще раз бесконечность числа простых чисел.

Указание: Предположив, что p — общий делитель двух таких чисел, найти остатки от деления 2^{2^m} и 2^{2^n} на p.

4. Пусть $f(x)$ — многочлен с целыми коэффициентами. Докажите, что среди простых делителей его значений $f(1)$, $f(2)$, ... существует бесконечное число различных. (Если задача не будет сразу получаться, решите ее сначала для многочлена $f(x)$ первой, потом — второй степени.)

5. Обозначим через p_n n-е по порядку простое число. Докажите, что $p_{n+1} < p_n^n + 1$.

6. В обозначениях задачи 5 докажите, что $p_n < 2^{2^n}$. Выведите близкое неравенство $p_n \leq 2^{2^n} + 1$ из результата задачи 3.

7. В обозначениях задачи 5 докажите, что $p_{n+1} < p_1 p_2 \dots p_n$.

§2. Доказательство бесконечности числа простых чисел по Эйлеру

Мы изложим еще одно доказательство бесконечности числа простых чисел, принадлежащее Эйлеру, которое проясняет некоторые общие свойства этой последовательности.

Начнем с "предыстории", то есть с некоторых простых фактов, которые были известны до того, как Эйлер стал заниматься вопросом о простых числах. Речь идет о величине сумм

$$1,\ 1+\frac{1}{2},\ 1+\frac{1}{2}+\frac{1}{3},\dots,1+\frac{1}{2}+\dots+\frac{1}{n},\dots$$

В обозначениях §3 главы II это суммы $(Sa)_n$, где a — последовательность обратных натуральных чисел $1, \frac{1}{2}, \frac{1}{3}, \dots$. Поскольку суммы m-х степеней натуральных чисел от 1 до $n-1$ мы обозначали через $S_m(n)$ (ср. формулу (28) главы II), естественно наши суммы обозначить $S_{-1}(n)$.

Мы здесь столкнулись с понятием, которое дальше будет часто встречаться, поэтому обсудим его подробнее. Оно относится вообще к свойствам *бесконечной* последовательности положительных чисел $s_1, s_2, \dots, s_n, \dots$ (у нас она возникла как последовательность сумм другой последовательности, но сейчас это не важно). Один тип последовательностей называется *ограниченными*. Это значит, что существует такое единое для всей последовательности число C, что $s_n < C$ для всех $n = 1, 2, 3, \dots$. Если последовательность этим свойством не обладает, то она называется *неограниченной*. Это значит, что *никакое* число C не может обладать указанным свойством, то есть для любого числа C найдется такой индекс n, что $s_n \geq C$. Наконец, может случиться, что для любого числа C найдется такой индекс n, что все $s_m \geq C$ для $m = n, n+1, \dots$. Иначе говоря, при достаточно большом n число s_n станет сколь угодно большим. В этом случае последовательность называется *неограниченно возрастающей*. Например, последовательность 1, 2, 1, 3, 1, 4, ..., в которой на нечетных местах стоит 1, а на четных идут подряд натуральные числа,

является неограниченной, но не неограниченно возрастающей, так как в ней сколь угодно далеко стоят числа, равные 1.

Если задана последовательность $a = a_1, a_2, \ldots, a_n, \ldots$ положительных чисел и $s = Sa$, то $s_{n+1} > s_n$ (так как $s_{n+1} = s_n + a_{n+1}$, $a_{n+1} > 0$), и вообще $s_m > s_n$ при $m > n$. Поэтому такая последовательность будет неограниченно возрастающей, если она неограниченна. Например, если все $a_i = 1$, то $s_n = n$ и последовательность $s_1, s_2, \ldots$ будет неограниченной. Но в других случаях она может быть ограниченной. Пример можно наглядно усмотреть на рис. 1, где мы делим отрезок между 0 и 1 сначала пополам и полагаем $a_1 = \frac{1}{2}$, потом отрезок между 0 и $\frac{1}{2}$ опять делим пополам и полагаем $a_2 = \frac{1}{4}$ и т. д.

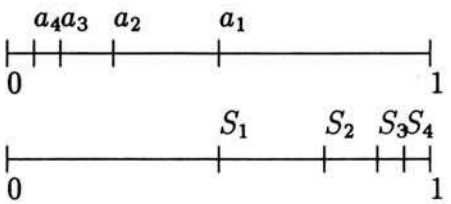

Рис. 1

Таким образом, $a_n = \frac{1}{2^n}$. Результат сложения этих чисел изображен на рис. 1 и видно, что их суммы S_n всегда остаются внутри нашего отрезка, то есть $S_n < 1$. Это легко проверить и вычислением. Если $a_n = \frac{1}{2^n}$, то

$$(Sa)_n = \frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^n} = \frac{1}{2}(1 + \frac{1}{2} + \ldots + \frac{1}{2^{n-1}}),$$

и по формуле (12) главы I

$$(Sa)_n = \frac{1}{2}\frac{\frac{1}{2^n} - 1}{\frac{1}{2} - 1} = 1 - \frac{1}{2^n},$$

так что $(Sa)_n < 1$ при любом n.

Мы покажем, что в случае последовательности $1, \frac{1}{2}, \frac{1}{3} \ldots$ имеет место *первый* случай: хотя члены последовательности убывают, но недостаточно быстро и суммы их (то есть $S_{-1}(n)$) неограниченно возрастают.

Лемма 1. Сумма $S_{-1}(n)$ при достаточно большом n больше любого наперед заданного числа.

Пусть нам задано число k. Мы утверждаем, что для некоторого n (и, значит, также для следующих за ним) $S_{-1}(n) > k$. Возьмем n таким, что $n - 1 = 2^m$ при некотором m. Сумму

$$S_{-1}(n) = 1 + \left(\frac{1}{2}\right) + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) + \ldots + \left(\frac{1}{2^{m-1}+1} + \ldots + \frac{1}{2^m}\right)$$

разобьем на части так, как указано в формуле: на группы, заключенные между двумя последовательными степенями двойки. Каждая скобка имеет вид $\frac{1}{2^{k-1}+1} + \ldots + \frac{1}{2^k}$, а число скобок равно m. В каждой скобке заменим каждое слагаемое наименьшим из входящих в скобку, то есть последним. Так как число слагаемых в такой скобке равно $2^k - 2^{k-1} = 2^{k-1}$, то мы получим, что k-я скобка больше, чем $\frac{2^{k-1}}{2^k} = \frac{1}{2}$. В результате мы получаем, что $S_{-1}(n) > 1 + \frac{m}{2}$. Это неравенство имеет место при любом n, если $n - 1 = 2^m$. Нам остается положить $1 + \frac{m}{2} = k$, то есть $m = 2k - 1$ и $n = 2^{2k-1} + 1$. Тогда $S_{-1}(n) > k$.

Теперь переходим к изложению доказательства Эйлера. Его идея связана с методом вычисления сумм степеней делителей натурального числа, который был описан в §3 главы I (ср. формулу (13) главы I). Сумма k-х степеней всех делителей (включая 1 и n) натурального числа n обозначают $\sigma_k(n)$. Согласно формуле (13) главы I для числа n, имеющего каноническое разложение $n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$,

$$\sigma_k(n) = \frac{p_1^{k(\alpha_1+1)} - 1}{p_1^k - 1} \frac{p_2^{k(\alpha_2+1)} - 1}{p_2^k - 1} \cdots \frac{p_r^{k(\alpha_r+1)} - 1}{p_r^k - 1}. \tag{2}$$

Формула (2) была известна еще со времен античности, но молчаливо предполагалось, что в ней k — положительное число. Наконец она попала в круг интересов Эйлера, задавшегося вопросом — а что будет при k целом, но отрицательном? Ответ, конечно, заключается в том, что никакой разницы здесь нет, вывод формулы (2) совершенно формальный и одинаково годится как для положительных, так и для отрицательных значений k. В частности, она верна и для $k = -1$. Сумму $(-1) - x$ степеней (то есть их обратных величин) делителей заданного числа n мы, сохраняя прежние обозначения, будем записывать как $\sigma_{-1}(n)$. Формула (2) дает тогда:

$$\sigma_{-1}(n) = \frac{1 - \frac{1}{p_1^{\alpha_1+1}}}{1 - \frac{1}{p_1}} \cdot \ldots \cdot \frac{1 - \frac{1}{p_r^{\alpha_r+1}}}{1 - \frac{1}{p_r}}$$

(мы изменили порядок слагаемых в числителе и знаменателе каждой дроби). Отсюда (так как все выражения в числителе меньше 1),

$$\sigma_{-1}(n) < \frac{1}{\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_r}\right)}. \tag{3}$$

Заменим теперь в этой формуле n на $n!$ ($p_1, \ldots, p_r$ — теперь простые делители $n!$). Среди делителей $n!$ наверняка содержатся $1, 2, \ldots, n$. Поэтому в сумму $\sigma_{-1}(n)$ заведомо войдут слагаемые $1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}$, которые в сумме равны $S_{-1}(n+1)$. По лемме 1 уже сумма $S_{-1}(n+1)$ больше любого наперед заданного числа k при достаточно большом n. Так как другие слагаемые в сумме $\sigma_{-1}(n!)$ тоже положительны, то тем более это утверждение верно и для нее. Если бы число простых чисел было конечно и $p_1, \ldots, p_r$ — это был их полный список, то мы получили бы, что

$$\frac{1}{\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_r}\right)} > k,$$

где k — любое число. Это, конечно, противоречие.

В приведенном доказательстве ценно то, что оно не только приводит к противоречию предположение о конечности числа простых чисел, но когда бесконечность их числа уже доказана, дает некоторую количественную характеристику их последовательности. Именно, перефразируя полученный результат, мы можем теперь сказать, что если $p_1, p_2, \dots, p_n \dots$ — бесконечная последовательность всех простых чисел, то выражение $\frac{1}{\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_n}\right)}$ при достаточно большом n становится больше любого наперед заданного числа. Это, конечно, равносильно тому, что знаменатель выписанной выше дроби при достаточно большом n становится *меньше* любого наперед заданного числа. Нами доказана

Теорема 2. Если $p_1, p_2, \dots, p_n \dots$ — последовательность всех простых чисел, то произведение $\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_n}\right)$ при достаточно большом n становится меньше любого наперед заданного положительного числа.

Это первое приближение к нашей цели. Теперь постараемся придать полученной характеристике более привычный вид.

Теорема 3. Если $p_1, p_2, \dots, p_n \dots$ — последовательность всех простых чисел, то последовательность сумм $\frac{1}{p_1}+\frac{1}{p_2}+\dots+\frac{1}{p_n}$ неограниченно возрастает.

Вывод теоремы 3 из теоремы 2 — чисто формальный: он не зависит от того, что $p_1, p_2, \dots, p_n \dots$ — последовательность *простых чисел* — это могла бы быть любая последовательность натуральных чисел, для которой выполняется утверждение теоремы 2.

Лемма 2. Для любого натурального $n > 1$ имеет место неравенство

$$1-\frac{1}{n} \geq \frac{1}{4^{\frac{1}{n}}}. \tag{4}$$

Так как обе части неравенства (4) положительны, то возведя его в степень n, мы получим *равносильное* неравенство

$$\left(1-\frac{1}{n}\right)^n \geq \frac{1}{4}, \tag{5}$$

которое мы и докажем. Развернем левую часть неравенства (5) по формуле бинома. Мы получим

$$\left(1-\frac{1}{n}\right)^n = 1 - n\frac{1}{n} + \frac{n(n-1)}{2!}\frac{1}{n^2} - \frac{n(n-1)(n-2)}{3!}\frac{1}{n^3} + \dots + (-1)^n\frac{1}{n^n}. \tag{6}$$

Абсолютные величины слагаемых в правой части равенства (6) образуют последовательность $C_n^k\frac{1}{n^k}$. Такую последовательность чисел мы рассматривали в связи со схемой Бернулли в параграфе "Язык вероятностей" главы III (формула (34)).

Точнее говоря, если в тех формулах мы положим $p = \frac{1}{n+1}$, $q = 1 - \frac{1}{n+1} = \frac{n}{n+1}$, то получим, что $p+q = 1$, $p^k q^{n-k} = (n+1)^{-n} n^{n-k}$, и полученные нами числа отличаются от рассматривавшихся в формуле (7) лишь общим для всех множителем $\left(\frac{n}{n+1}\right)^n$. Выражение $(n+1)p - 1$ в нашем случае равно 0. Мы доказали в параграфе "Язык вероятностей" главы III, что если $k > (n+1)p - 1$ (в нашем случае $k > 0$), то $k+1$-й член меньше k-го. Значит, все числа последовательности $C_n^k \frac{1}{n^k}$, $k = 1, 2, \ldots, n$ монотонно убывают. (Мы сослались здесь на главу III, чтобы обратить внимание на то, как связаны между собой вопросы, которыми мы занимаемся. (Легко было бы и непосредственно выписать отношение $k+1$-го к k-му члену этой последовательности и убедиться, что оно меньше 1.) Мы видим, что в формуле (6) слева первые два члена сокращаются. Следующие два члена (после сокращений, которые вы легко выполните), дадут $\frac{1}{3} - \frac{1}{3n^2}$. Это число не меньше $\frac{1}{4}$ при $n \geq 2$ (проверьте и это сами!). Остальные же члены группируются в пары, причем в каждой паре первое слагаемое положительное, а следующее отрицательное, но, как мы видели, по абсолютной величине меньше первого. Поэтому каждая пара дает положительный вклад в сумму (6). Если n нечетно, то число слагаемых в правой части формулы (6) четно (оно равно $n+1$) и сумма точно разбивается на $\frac{n+1}{2}$ пар. Если же n четно, то после объединения слагаемых в пары остается еще одно положительное слагаемое $\frac{1}{n^n}$. Таким образом, в любом случае правая часть состоит из слагаемого, которое не меньше $\frac{1}{4}$, и еще некоторых положительных слагаемых. Это доказывает неравенство (6), а, значит, и лемму.

Теперь теорема 3 почти очевидна. Для любого p_i мы имеем согласно лемме:

$$1 - \frac{1}{p_i} \geq \frac{1}{4^{\frac{1}{p_i}}}.$$

Перемножая эти неравенства для $i = 1, \ldots, n$, мы получим:

$$\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_n}\right) \geq \frac{1}{4^{\left(\frac{1}{p_1} + \frac{1}{p_2} + \ldots + \frac{1}{p_n}\right)}}.$$

Если бы суммы $\frac{1}{p_1} + + \ldots + \frac{1}{p_n}$ для всех n не превосходили некоторой величины k, то отсюда следовало бы, что

$$\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_n}\right) \geq \frac{1}{4^k}.$$

Это противоречит теореме 2.

Мы сталкиваемся здесь с вопросом нового типа. Если N — подмножество конечного множества M, то мы можем сказать, насколько N "меньше", чем M, сравнивая их число элементов, например, вычисляя отношение $\frac{n(N)}{n(M)}$. Но сейчас мы имеем два бесконечных подмножества: множество натуральных чисел и содержащееся в нем множество простых чисел. Как сравнить их? Теорема 3 предлагает один способ сравнения, на первый взгляд не очень простой. Его можно применить к любой последовательности натуральных чисел a : $a_1, a_2, \ldots, a_n, \ldots$. Согласно лемме 1, для последовательности всех натуральных чисел суммы обратных величин (то

есть суммы $S_{-1}(n)$) неограниченно возрастают. Мы можем считать последовательность a "густо" расположенной среди натуральных чисел, если для нее сохраняется то же свойство, то есть суммы $\frac{1}{a_1}, \frac{1}{a_1}+\frac{1}{a_2}, \ldots, \frac{1}{a_1}+\frac{1}{a_2}+\ldots+\frac{1}{a_n}, \ldots$ неограниченно возрастают. Это значит, что в последовательности a сохранилось еще достаточно много натуральных чисел, так что суммы обратных величин ее членов не намного меньше сумм $S_{-1}(n)$ обратных всех натуральных чисел. Если же суммы обратных величин последовательности a остаются ограниченными, то мы можем считать ее "редко" расположенной в натуральном ряду. Теорема 3 утверждает, что последовательность простых чисел "густа". Самый крайний "редкий" случай — когда последовательность a состоит только из конечного числа членов.

Но бывают и промежуточные случаи. Например, последовательность квадратов: $1, 4, 9, \ldots, n^2 \ldots$. Для нее соответствующие суммы $1+\frac{1}{4}+\frac{1}{9}+\ldots+\frac{1}{n^2}$ естественно обозначить $S_{-2}(n)$. Докажем, что они ограничены величиной, не зависящей от n. Для этого применим тот же прием, что и при доказательстве леммы 1. Пусть m таково, что $2^m \geq n$. Тогда $S_{-2}(n) \leq S_{-2}(2^m)$. Сумму $S_{-2}(2^m) = 1+\frac{1}{2^2}+\frac{1}{3^2}+\ldots+\frac{1}{2^{2m}}$ разобьем на части:

$$(1)+\left(\frac{1}{2^2}\right)+\left(\frac{1}{3^2}+\frac{1}{4^2}\right)+\ldots+\left(\frac{1}{(2^{m-1}+1)^2}+\ldots+\frac{1}{2^{2m}}\right).$$

В каждой части $\frac{1}{(2^{k-1}+1)^2}+\ldots+\frac{1}{2^{2k}}$ опять содержится 2^{k-1} членов и первый член является наибольшим. Поэтому эта часть не превосходит $2^{k-1}\frac{1}{(2^{k-1}+1)^2} < 2^{k-1}\frac{1}{(2^{k-1})^2} = \frac{1}{2^{k-1}}$. Таким образом, $S_{-2}(2^m) \leq 1+1+\frac{1}{2}+\frac{1}{2^2}+\ldots+\frac{1}{2^{m-1}} = 1+\frac{1-\frac{1}{2^m}}{1-\frac{1}{2}} \leq 1+\frac{1}{1-\frac{1}{2}} = 3$. То есть, все суммы $S_{-2}(n)$ не превосходят 3.

Таким образом теорема 3 показывает, например, что простые числа в натуральном ряде расположены "гуще", чем квадраты.

Задачи

1. Докажите, что при любом заданном целом $k \geq 2$ и всех натуральных n суммы $S_{-k}(n) = \frac{1}{1^k}+\frac{1}{2^k}+\ldots+\frac{1}{n^k}$ ограничены.

2. Пусть последовательность a является арифметической прогрессией: $a_0 = p$, $a_1 = p+q$, $a_2 = p+2q, \ldots, a_n = p+nq$ при некоторых натуральных p и q. Доказать, что суммы $\frac{1}{a_0}, \frac{1}{a_0}+\frac{1}{a_1}, \ldots, \frac{1}{a_0}+\frac{1}{a_1}+\ldots+\frac{1}{a_n}, \ldots$ становятся неограниченно большими при достаточно больших n.

3. Пусть последовательность a является геометрической прогрессией: $a_0 = c$, $a_1 = cq$, $a_2 = cq^2, \ldots, a_n = cq^n \ldots$, где c и q — некоторые натуральные числа. Является она "густой" или "редкой" в ряду натуральных чисел?

4. Пусть $p_1, \ldots, p_n, \ldots$ — последовательность всех простых чисел. Доказать, что выражения $\frac{1}{\left(1-\frac{1}{p_1^2}\right)\left(1-\frac{1}{p_2^2}\right)\ldots\left(1-\frac{1}{p_n^2}\right)}$ ограничены для всех n.

§3. Функция $\pi(n)$

В этом параграфе мы еще раз попытаемся оценить, насколько отличается последовательность простых чисел от всей последовательности натуральных чисел. При этом более вычурный метод сравнения "густых" и "редких" последовательностей, обсуждающийся в предыдущем переграфе, заменим более наивным, сразу приходящим в голову. А именно, наивный вопрос — "какую долю составляют простые числа среди всех натуральных?" — попытаемся решить, определяя, сколько есть простых чисел, меньших 10, сколько — меньше 100, сколько — меньше 1000 и т.д. Для любого натурального числа n через $\pi(n)$ обозначают число простых чисел, не превосходящих n, так что $\pi(1) = 0, \pi(2) = 1, \pi(4) = 2, \ldots$. Что можно сказать об отношении $\frac{\pi(n)}{n}$, когда n неограниченно возрастает?

Прежде всего, познакомимся с тем, что говорят таблицы. Любое утверждение или вопрос о натуральных числах можно проверить для всех натуральных чисел, не превосходящих некоторой границы N. Это обстоятельство играет для теории чисел, изучающей свойства натуральных чисел, такую же роль, как возможность эксперимента для теоретической физики. В частности, можно вычислить значение $\pi(n)$ для $n = 10^k$, $k = 1, 2, \ldots, 10$. Получается следующая таблица.

n	$\pi(n)$	$\frac{n}{\pi(n)}$
10	4	2,5
100	25	4,0
1000	168	6,0
10000	1229	8,1
100000	9592	10,4
1000000	78498	12,7
10000000	664579	15,0
100000000	5761455	17,4
1000000000	50847534	19,7
10000000000	455059512	22,0

Таблица 1

Мы видим, что отношение $\frac{n}{\pi(n)}$ постоянно растет, а, значит, $\frac{\pi(n)}{n}$ все время уменьшается. То есть доля простых чисел среди первых n чисел становится с ростом n все ближе к нулю. Можно сказать, что согласно таблицам "простые числа составляют нулевую долю среди всех натуральных чисел". Так это формулировал Эйлер, хотя его рассуждения не содержат полного доказательства. Это утверждение мы и сформулируем точно, а потом докажем.

Теорема 4. Отношение $\frac{\pi(n)}{n}$ становится меньше любого наперед заданного положительного числа при достаточно большом n.

Для доказательства теоремы нам надо как-то оценить функцию $\pi(n)$. Для фактического вычисления ее значения начинают с простого числа 2, затем вычеркивают все числа, кратные 2 и не превосходящие n. Затем берут первое оставшееся число — это будет 3 — и повторяют тот же процесс с ним. Так поступают, пока

не исчерпают все числа, не превосходящие n. Не вычеркнутые (2, 3 и т.д.) и будут всеми простыми числами, не превосходящими n. Такой прием применялся еще в античности; он называется "решетом Эратосфена".

Этот же процесс мы применим в нашем рассуждении. Пусть мы уже нашли первые r простых чисел: $p_1, p_2, \dots p_r$. Тогда следующие простые числа, не превосходящие n, содержатся среди "невычеркнутых" чисел, не превосходящих n, то есть среди тех чисел $m \leq n$, которые не делятся ни на одно из чисел $p_1, p_2, \dots p_r$. Но число чисел, не превосходящих n и не делящихся ни на одно из простых чисел $p_1, p_2, \dots p_r$, мы исследовали в главе III — оно задается формулой в §Алгебра множеств главы III. Выражение, входящее в эту формулу, можно, как мы там показали, заменить на более простое: $n\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_r}\right)$, причем ошибка не будет превосходить 2^r (формула (28) главы III). Таким образом, число s чисел $m \leq n$ и не делящихся ни на одно из простых чисел $p_1, p_2, \dots p_r$, удовлетворяет неравенству

$$s \leq n\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_r}\right)+2^r. \tag{7}$$

Все $\pi(n)$ простых чисел, не превосходящих n, содержатся либо среди r простых чисел $p_1, p_2, \dots p_r$, либо среди s чисел, учтенных неравенством (7). Таким образом, $\pi(n) \leq s + r$ и, значит,

$$\pi(n) \leq n\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_r}\right)+2^r+r. \tag{8}$$

Неравенство (8) замечательно тем, что в него входит произведение $\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_r}\right)$, сведения о величине которого дает нам теорема 2.

Теперь мы можем перейти непосредственно к доказательству теоремы 4. Пусть нам дано сколь угодно малое положительное число ε. По нему мы должны найти такое число N, что $\frac{\pi(n)}{n} < \varepsilon$ для всех $n > N$. В неравенстве (8) мы заменим r большей величиной 2^r (ср. задачу 6 к §2 главы I), чтобы получить более простое неравенство

$$\pi(n) \leq n\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_r}\right)+2^{r+1}. \tag{9}$$

В неравенстве (9) присутствуют два слагаемых, и мы выберем N так, чтобы при $n \geq N$ каждое слагаемое не превосходило $\frac{\varepsilon n}{2}$. Тогда из неравенства (9) получится, что $\pi(n) < \varepsilon n$ и, значит, $\frac{\pi(n)}{n} < \varepsilon$. Но вспомним, что пока число r в нашем рассуждении было произвольным. Мы выберем сначала его так, чтобы первое слагаемое не превосходило $\frac{\varepsilon n}{2}$, а потом выберем N так, чтобы второе слагаемое не превосходило $\frac{\varepsilon n}{2}$. Первый выбор возможен в силу теоремы 2. Она утверждает, что при достаточно большом r произведение $\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_r}\right)$ меньше любого наперед заданного положительного числа. За такое положительное число мы можем взять $\frac{\varepsilon}{2}$. Тогда первое слагаемое в неравенстве (9) не превосходит $\frac{\varepsilon n}{2}$. Со вторым слагаемым дело обстоит еще проще. Теперь r нами уже выбрано. Выберем N так, что $2^{r+1} < \frac{\varepsilon N}{2}$. Для этого надо выбрать $N > \frac{2^{r+2}}{\varepsilon}$. Тогда $2^{r+1} < \frac{\varepsilon N}{2} \leq \frac{\varepsilon n}{2}$ для любого $n \geq N$. Теорема 4 доказана.

Заметим, что если мы выберем арифметическую прогрессию $am + b$ даже с очень большой разностью a, то есть идущую очень редко, то число членов этой прогрессии, не превосходящих n, совпадает с числом целых m, для которых $am \le n-b$, то есть $[\frac{n-b}{a}]$. Мы видели в §3 главы III, что $[\frac{n-b}{a}]$ отличается от $\frac{n-b}{a}$ не больше, чем на 1. Поэтому число членов прогрессии, не превосходящих n, не меньше, чем $\frac{n-b}{a}-1$. Его отношение к n не меньше, чем $\frac{1}{n}(\frac{n-b}{a}-1) = \frac{1}{a} - \frac{1}{n}\frac{b}{a} - \frac{1}{n}$. С ростом n это число приближается к $\frac{1}{a}$ и не становится неограниченно малым. Поэтому теорема 4 была бы неверна, если бы за последовательность мы взяли любую арифметическую прогрессию. Она показывает, что простые числа расположены реже любой арифметической прогрессии.

Задачи

1. Пусть p_n обозначает n-е простое число. Докажите, что для любого сколь угодно большого положительного числа C выполняется неравенство $p_n > Cn$ для всех достаточно больших n.

(**Указание**. Воспользоваться тем, что $\pi(p_n) = n$).

2. Рассмотрим натуральные числа, обладающие тем свойством, что их запись в десятичной системе счисления не содержит определенной цифры (например, 0). Пусть $q_1, q_2, q_3, \ldots, q_n, \ldots$ — эти числа, записанные в порядке возрастания и $\pi_1(n)$ обозначает число таких чисел, не превосходящих n. Докажите, что отношение $\frac{\pi_1(n)}{n}$ становится меньше любого наперед заданного положительного числа при достаточно большом n. Докажите, что суммы $\frac{1}{q}, \frac{1}{q_1}+\frac{1}{q_2}, \ldots, \frac{1}{q_1}+\frac{1}{q_2}+\ldots+\frac{1}{q_n}, \ldots$ ограничены.

(**Указание.** Не пытайтесь копировать доказательство теоремы 4. Разбейте сумму на участки, где знаменатели расположены между 10^k и 10^{k+1}. Найдите число чисел q_i в таком интервале. Ответ зависит от той цифры r, которую мы исключаем: $r = 0$ или $r \ne 0$.)

Приложение. Чебышевские неравенства для $\pi(n)$

Мы вынесем этот текст в приложение, во-первых, по формальной причине, так как здесь мы будем вынуждены пользоваться логарифмами, знакомство с которыми в остальном тексте не предполагается. Напомним, что *логарифмом при основании a числа x* называется такое число y, что

$$a^y = x.$$

Это записывается так: $y = \log_a x$. Дальше всегда будет предполагаться, что $a > 1$ и будут рассматриваться положительные числа x. Основные свойства логарифмов, сразу вытекающие из определения:

$$\log_a(xy) = \log_a(x) + \log_a(y), \quad \log_a c^n = n \log_a c, \quad \log_a a = 1.$$

$\log_a(x) > 0$ тогда и только тогда, когда $x > 1$. Логарифм является монотонной функцией, то есть $\log_a x \le \log_a y$ тогда и только тогда, когда $x \le y$.

Если основание логарифмов не указано, то предполагается, что оно равно 2: $\log x$ — это $\log_2 x$.

Вторая причина, почему следующие далее рассуждения выделены в приложение, заключается в следующем. В остальной части книги была ясна логика рассуждений, почему мы идем именно этим путем (так я, по крайней мере, надеюсь). Здесь же мы столкнемся со случаем, не редким в математических исследованиях, когда некоторое новое соображение как бы упало с неба и даже автор часто не может объяснить, как он к нему пришел. О таких ситуациях Эйлер говорил: "Мне иногда кажется, что мой карандаш умнее меня". Разумеется, это есть результат многочисленных проб, размышлений и неосознанной работы психики.

Мы здесь продолжим изучение вопроса об отношении $\frac{\pi(n)}{n}$, когда n неограниченно возрастает. Всмотримся еще раз в таблицу 1, показывающую значения $\pi(n)$ для $n = 10^k, \quad k = 1, 2, \ldots, 10$. Обратим внимание на последний столбец таблицы, указывающий отношения $\frac{n}{\pi(n)}$ для некоторых значений n. Мы видим, что при переходе от $n = 10^k$ к $n = 10^{k+1}$, то есть при спуске на одну строку таблицы, значения $\frac{n}{\pi(n)}$ меняются почти на одну и ту же величину. А именно, первое число равно 2,5; второе отличается от него на 1,5 и дальше последовательные разности равны: 2; 2,1; 2,3; 2,3; 2,3; 2,4; 2,3; 2,3. Мы видим, что все эти числа очень близки к одному: 2,3. Не пытаясь пока разгадать загадку именно этого значения разностей, предположим, что и дальше, за пределами нашей таблицы, число $\frac{n}{\pi(n)}$ при переходе от $n = 10^k$ к $n = 10^{k+1}$ будет увеличиваться на число все более близкое к некоторой фиксированной постоянной α. Это значило бы, что $\frac{n}{\pi(n)}$ для $n = 10^k$ было очень близко к αk. Но если $n = 10^k$, то по определению $k = \log_{10} n$. Естественно тогда предположить, что и для других значений n величина $\frac{n}{\pi(n)}$ очень близка к $\alpha \log_{10} n$. Значит, $\pi(n)$ очень близко к $c\frac{n}{\log_{10} n}$, где $c = \alpha^{-1}$.

Многие математики были увлечены тайной расположения простых чисел и пытались ее раскрыть на основании таблиц. В частности, Гаусс заинтересовался этим вопросом почти в детском возрасте. Его интерес к математике начался, видимо, с детского интереса к числам и с составления таблиц. Вообще многие великие математики были виртуозами счета и умели производить громадные вычисления, иногда в уме (Эйлер таким способом даже боролся с бессоницей!). Когда Гауссу было еще 14 лет, он составил таблицы простых чисел (правда, менее обширные, чем наша таблица 1) и пришел к тому предположению, которое мы формулировали. Позже оно обсуждалось многими математиками. Но первый результат в этом направлении был доказан более полувека спустя, в 1850 г. Чебышевым.

Чебышев доказал следующее утверждение:

Теорема. Существуют такие постоянные c и C, что для всех $n > 1$

$$c\frac{n}{\log n} \leq \pi(n) \leq C\frac{n}{\log n}. \tag{10}$$

Прежде, чем переходить к доказательству, сделаем несколько замечаний по поводу формулировки теоремы. С каким основанием здесь рассматриваются логарифмы? Ответ: с любым. Из определения логарифма сразу следует, что $\log_b x = \log_b a \log_a x$: надо только в соотношении $a^{\log_a x} = x$ заменить a на $b^{\log_b a}$ и мы полу-

чим, что $b^{\log_b a \log_a x} = x$, что и показывает, что $\log_b x = \log_b a \log_a x$. Поэтому, если неравенство (10) доказано для $\log_a n$, то оно верно и для $\log_b n$ с заменой c и C на $\frac{c}{\log_b a}$ и $\frac{C}{\log_b a}$.

Неравенства (10) и выражают подсказанную таблицей мысль, что $\pi(n)$ "близко" к $c\frac{n}{\log n}$ при некотором c. Вопрос о том, почему в наших гипотетических рассуждениях встречалась одна постоянная c, а в теореме — две: c и C, и нельзя ли заменить в ней две постоянные одной — мы обсудим после доказательства теоремы.

Таинственным ключом к доказательству теоремы Чебышева являются свойства биномиальных коэффициентов C_n^k: прежде всего тот факт, что они являются целыми числами, и некоторые свойства их делимости на простые числа. Перечислим те свойства, которые нам понадобятся в доказательстве.

Прежде всего, это утверждение, доказанное в §3 главы II, согласно которому сумма всех биномиальных коэффициентов C_n^k при $k = 0, 1, \ldots, n$ равна 2^n. Так как сумма положительных слагаемых больше каждого из них, то отсюда получаем, что

$$C_n^k \leq 2^n \tag{11}$$

Нам будут особенно полезны большие биномиальные коэффициенты. Мы видели в главе II, что при четном $n = 2m$ коэффициент C_{2m}^m больше всех остальных, а при нечетном $n = 2m+1$ существуют два равных коэффициента: C_{2m}^m и C_{2m}^{m+1}, которые больше остальных. На них мы обратим особое внимание. В частности,

$$C_{2n}^n = \frac{2n(2n-1)\ldots(n+1)}{1 \cdot 2 \cdot \ldots \cdot n} \tag{12}$$

Если мы сгруппируем множители числителя с множителями знаменателя, идущими в обратном порядке, то получим:

$$C_{2n}^n = \frac{2n}{n} \cdot \frac{2n-1}{n-1} \cdot \ldots \cdot \frac{n+1}{1}.$$

Очевидно, что в этой формуле каждый множитель не меньше 2, поэтому

$$C_{2n}^n \geq 2^n \tag{13}$$

Теперь рассмотрим свойства делимости биномиальных коэффициентов на простые числа. В выражении (12) множители в числителе очевидно делятся на все простые числа, не превосходящие $2n$ и большие n. Такие простые числа не могут делить множители знаменателя, поэтому они не сокращаются и будут делителями C_{2n}^n. Число простых чисел, расположенных между $2n$ и n, равно $\pi(2n) - \pi(n)$, и все они больше, чем n, поэтому

$$C_{2n}^n \geq n^{\pi(2n)-\pi(n)}. \tag{14}$$

Аналогичное утверждение верно, конечно, и для "средних" коэффициентов $C_{2n+1}^n = C_{2n+1}^{n+1}$ с нечетным нижним индексом. Записав их в виде

$$C_{2n+1}^n = \frac{(2n+1)\ldots(n+2)}{1 \cdot 2 \cdot \ldots \cdot n}$$

мы увидим, что $\pi(2n+1)-\pi(n+1)$ простых чисел, не превосходящих $2n+1$ и больших $n+1$, входят в числитель и не могут сократиться со знаменателем. Так как они больше, чем $n+1$, то

$$C_{2n+1}^{n} > (n+1)^{\pi(2n+1)-\pi(n+1)}. \tag{15}$$

В неравенствах (14) и (15) уже вскрывается замечательная связь между биномиальными коэффициентами и простыми числами.

Наконец, приведем последнее из нужных для доказательства свойств биномиальных коэффициентов, хотя и совсем простое, но в отличие от предыдущих не совсем очевидное.

Лемма. Для любого биномиального коэффициента C_n^k степень простого числа, делящего его, не превосходит n.

Обратим внимание, что речь идет не о *показателе* степени, а о *самой степени*. То есть мы утверждаем, что если p^r делит C_n^k, где p — простое число, то $p^r \le n$. Например, $C_9^2 = 9\cdot 4$ делится на 9 и на 4, и оба числа не превосходят 9.

Запишем биномиальный коэффициент в виде

$$C_n^k = \frac{n(n-1)\dots(n-k+1)}{1\cdot 2\dots\cdot k}. \tag{16}$$

Рассматриваемое нами простое число p должно делить числитель этой дроби. Обозначим через m тот множитель, в котором p входит в максимальной степени (или один из них, если их несколько), а через p^r — эту максимальную степень. Очевидно, $n \ge m \ge n-k+1$. Положим $n-m=a$, $m-(n-k+1)=b$, тогда $a+b=k-1$ и C_n^k можно записать в виде

$$C_n^k = \frac{(m+a)(m+a-1)\dots(m+1)m(m-1)\dots(m-b)}{k!}. \tag{17}$$

Для нас сейчас множитель m является основным и мы записываем произведение в числителе как a множителей слева от него и b справа. Преобразуем аналогично знаменатель: $k! = (1\cdot 2\cdot\dots\cdot a)(a+1)\dots(a+b)(a+b+1)$. Так как $(a+1)(a+2)\dots(a+b)$ делится на $b!$, то это произведение (знаменатель) имеет вид $a!b!l$, где l – некоторое целое число. Теперь можно переписать C_n^k в удобном для нас виде:

$$C_n^k = \frac{m+a}{a}\cdot\frac{m+a-1}{a-1}\cdot\dots\cdot\frac{m+1}{1}\cdot\frac{m-1}{1}\cdot\dots\cdot\frac{m-b}{b}\cdot\frac{m}{l}, \tag{18}$$

где мы множитель $\frac{m}{l}$ перенесли в конец.

Заметим, что в каждом из множителей $\frac{m+i}{i}$ или $\frac{m-j}{j}$ $(i=1,\dots,a,\ j=1,\dots,b)$ степень p, входящая в числитель, полностью сокращается со знаменателем, так что после сокращения общих множителей в числителе и знаменателе на p делиться может только знаменатель (хотя и он может оказаться взаимно простым с p). Действительно, рассмотрим, например, дроби $\frac{m+i}{i}$ (множитель вида $\frac{m-j}{j}$ рассматривается точно так же). Пусть i делится точно на p^s, то есть $i=p^s u$, где u взаимно просто с p. Если $s<r$, то $m+i$ тоже делится точно на p^s: положив $m=p^r v$, (вспомним, что m делится на p^r), получим, что $m+i=p^s(u+p^{r-s}v)$. Если же $s\ge r$,

то точно так же $m+i$ делится на p^r и вспомнив выбор m (оно делится на самую большую степень p среди всех чисел между n и $n-k+1$ и эта степень есть p^r), мы заключаем, что на большую степень p, чем r-я, число $m+i$ делиться не может. Таким образом p^r сократится в числителе и знаменателе и в числителе останется число, не делящееся на p. В результате мы видим, что из всех множителей в выражении (18) p может содержаться в числителе последнего, то есть в m. Но степень p, делящая m, есть p^r, а значит произведение (18) не может делиться на большую степень p, чем p^r. Так как p^r делит m, а $m \le n$, то $p^r \le n$. Лемма доказана.

Представим себе, что она говорит нам о каноническом разложении $C_n^k = p_1^{\alpha_1} \dots p_m^{\alpha_m}$. Прежде всего, простые числа $p_1, \dots, p_m$ могут появиться только из числителя выражения (16), значит, все $p_i \le n$ и поэтому $m \le \pi(n)$. По лемме, $p_i^{\alpha_i} \le n$ для $i = 1, \dots, m$. В результате мы получаем, что

$$C_n^k \le n^{\pi(n)}. \tag{19}$$

Теперь можно приступить к самому доказательству теоремы Чебышева, то есть неравенств (1). Заметим, что нам достаточно доказать выполнение этих неравенств лишь для всех n, начиная с некоторой фиксированной границы n_0. Для всех $n < n_0$ выполнения можно добиться за счет уменьшения постоянной c и увеличения постоянной C. Если же стремиться получить значения этих постоянных в явном виде и наиболее экономно, то можно проверить, составляя таблицы простых чисел, что неравенства (1) выполняются при значениях $n \le n_0$ (в наших рассуждениях n_0 будет получаться небольшим числом).

Начнем с сопоставления неравенств (13) и (19) для биномиального коэффициента C_{2n}^n. Мы получаем, что $2^n \le C_{2n}^n \le (2n)^{\pi(2n)}$ и следовательно

$$2^n \le (2n)^{\pi(2n)}. \tag{20}$$

Беря от обеих частей логарифм с основанием 2 (напомним, что мы будем писать $\log_2 x = \log x$) и воспользовавшись монотонностью логарифма, мы получим, что $n \le \pi(2n) \log 2n$ и значит

$$\pi(2n) \ge \frac{n}{\log 2n} = \frac{1}{2} \frac{2n}{\log 2n},$$

то есть левое из двух неравенств (10) с постоянной $c = \frac{1}{2}$. Но покамест оно доказано только для четных значений n. Для нечетных значений вида $2n+1$ мы воспользуемся монотонностью логарифма и функции $\pi(n)$. Отсюда следует, что

$$\pi(2n+1) \log(2n+1) \ge \pi(2n) \log 2n.$$

Подставляя сюда полученное неравенство для $\pi(2n)$, мы видим, что

$$\pi(2n+1) \ge \frac{n \log 2n}{\log(2n) \log(2n+1)} = \frac{n}{\log(2n+1)}.$$

Так как всегда $n \ge \frac{1}{3}(2n+1)$, то отсюда

$$\pi(2n+1) \ge \frac{1}{3} \frac{2n+1}{\log(2n+1)}.$$

Таким образом левое из неравенств (10) доказано для нечетных n с постоянной $c = \frac{1}{3}$. Значит, левое неравенство (10) верно для всех n и $c = \frac{1}{3}$.

Переходим к доказательству второго правого неравенства (10). Мы докажем его индукцией по n. Пусть сначала n четно. Мы будем писать вместо него $2n$. Соединим неравенство (11) для коэффициента C_{2n}^{n} (то есть, заменим в C_n^k n на $2n$ и k на n) с неравенством (14). Как следствие мы получим:

$$n^{\pi(2n)-\pi(n)} \leq 2^{2n}$$

и, переходя к логарифмам, получаем:

$$\begin{array}{l} \pi(2n) - \pi(n) \leq \frac{2n}{\log n}, \\ \pi(2n) \leq \pi(n) + \frac{2n}{\log n}. \end{array} \tag{21}$$

Согласно индуктивному предположению мы можем считать нужное нам неравенство доказанным: $\pi(n) \leq C\frac{n}{\log n}$ с постоянной C, значение которой мы позже уточним. Подставляя в формулу (21), получим:

$$\pi(2n) \leq C\frac{n}{\log n} + \frac{2n}{\log n} = \frac{(C+2)n}{\log n}.$$

Мы же хотели бы доказать неравенство $\pi(2n) \leq \frac{C \cdot 2n}{\log 2n}$ и для этого нам остается подобрать постоянную C так, чтобы выполнялось неравенство

$$\frac{(C+2)n}{\log n} \leq \frac{2Cn}{\log 2n} \tag{22}$$

для всех n, начиная с некоторого.

Это уже — чисто школьное упражнение. Сократим в неравенстве обе части на n, заметим, что $\log 2n = \log 2 + \log n = \log n + 1$ и обозначим $\log n$ через x. Тогда неравенство (22) приобретает вид

$$\frac{C+2}{x} \leq \frac{2C}{x+1}.$$

Умножая обе части на $x(x+1)$ (так как $x > 0$) и приводя подобные члены, мы запишем его в виде

$$(C-2)x \geq C+2.$$

Очевидно, что C надо выбрать так, чтобы $C - 2 > 0$. Положив, например, $C = 3$, мы получаем, что оно выполнено для $C = 3$ и всех $x \geq 5$. Так как x обозначает у нас $\log n$, то это значит, что нужное неравенство будет выполнено для $n \geq 2^5 = 32$, $2n \geq 64$.

Остается рассмотреть случай нечетных значений имеющих вид $2n+1$. Сравним для этого неравенство (11) (заменив в нем n на $2n+1$, а k — на n) с неравенством (15). Мы получим неравенство

$$2^{2n+1} \geq (n+1)^{\pi(2n+1)-\pi(n+1)}$$

и логарифмируя его, — неравенство

$$2n+1 \geq (\pi(2n+1) - \pi(n+1))\log(n+1).$$

Отсюда, используя индуктивное предположение о $\pi(n+1)$, мы получаем, как и раньше:

$$\pi(2n+1) \leq C\frac{n+1}{\log(n+1)} + \frac{2n+1}{\log(n+1)}.$$

Нужное нам неравенство $\pi(2n+1) \leq C\frac{2n+1}{\log(2n+1)}$ будет доказано, если мы проверим, что

$$C\frac{n+1}{\log(n+1)} + \frac{2n+1}{\log(n+1)} \leq C\frac{2n+1}{\log(2n+1)} \tag{23}$$

при надлежащем подборе постоянной C и для всех n, начиная с некоторого. Это опять упражнение чисто школьного типа, хотя немного сложнее предыдущего. Чтобы сделать разные члены неравенства легче сравнимыми друг с другом, заменим в левой части $2n+1$ на большее значение: $2(n+1)$

$$C\frac{n+1}{\log(n+1)} + \frac{2n+1}{\log(n+1)} \leq \frac{(C+2)(n+1)}{\log(n+1)}. \tag{24}$$

Для преобразования правой части заметим, что $2n+1 \geq \frac{3}{2}(n+1)$ для $n \geq 1$, $\log(2n+1) \leq \log(2n+2) = \log(n+1)+1$. Поэтому

$$\frac{2n+1}{\log(2n+1)} \geq \frac{(3/2)(n+1)}{\log(n+1)+1}. \tag{25}$$

Сравнивая неравенства (24) и (25) мы видим, что неравенство (23) будет доказано, если мы докажем, что

$$\frac{(C+2)(n+1)}{\log(n+1)} \leq \frac{(3/2)C(n+1)}{\log(n+1)+1}.$$

Сократим обе части на $n+1$ и положим $\log(n+1) = x$. Мы приходим к неравенству

$$\frac{C+2}{x} \leq \frac{(3/2)C}{x+1},$$

которое решается совершенно так же, как в разобранном случае. Надо умножить обе его части на $x(x+1)$ и привести подобные члены. Мы получим неравенство $(C+2)x + C + 2 \leq \frac{3}{2}Cx$ или $(\frac{1}{2}C - 2)x \geq C + 2$. Полагая $C = 6$, мы видим, что неравенство верно при $x \geq 8$, то есть $n+1 \geq 2^8$, $2n+1 \geq 511$. Таким образом, правое неравенство (10) доказано при постоянной $C = 6$ и для всех значений n, начиная с 511. Тем самым теорема доказана.

Заметим, что теорема 4 является очень простым следствием доказанной теоремы. Действительно, раз $\pi(n) < C\frac{n}{\log n}$, то $\frac{\pi(n)}{n} \leq \frac{C}{\log n}$. А так как логарифм меняется монотонно и неограниченно растет ($\log 2^k = k$), то $\frac{\pi(n)}{n}$ становится меньше любого положительного числа. С другой стороны, доказательство теоремы Чебышева основано совсем на других соображениях, чем доказательство теоремы 4.

В заключение обратимся еще раз к предположениям, которые можно сделать из рассмотрения таблицы 1. Исходя из нее мы пришли к догадке, что $\frac{n}{\pi(n)}$ близко к $\log_{10} n$ с некоторым определенным значением постоянной C: первые два знака в десятичном представлении числа C^{-1} имеют вид 2,3. Отсюда можно заключить, что $\pi(n)$ близко к $C^{-1}\frac{n}{\log_{10} n}$. Этому выражению можно придать более простой вид $\frac{n}{\log_e n}$, если подобрать новое основание логарифмов e так, чтобы было $C\log_{10} n = \log_e n$. Но, как было сказано выше, всегда $\log_b x = \log_b a \cdot \log_a x$, поэтому наше соотношение будет выполнено, если $C = \log_e 10$. Подставляя в соотношение $\log_b x = \log_b a \cdot \log_a x$ значение $x = b$, мы получаем, что $\log_b a \cdot \log_a b = 1$ и интересующее нас соотношение $C = \log_e 10$ можно переписать в виде $C^{-1} = \log_{10} e$.

14-летний Гаусс конечно обратил внимание на эти соотношения и угадал, что это за число e, для которого $\log_{10} e$ близко к $(2,3)^{-1}$. Такое число к этому времени было хорошо известно именно благодаря тому, что логарифм с таким основанием обладает многими полезными свойствами. Для этого числа, e — это его общепринятое обозначение. Логарифм с основанием e называется *натуральным* и обозначается ln: $\log_e(x) = \ln(x)$. Здесь мы вынуждены считать (в оставшейся странице), что читатель знаком с понятием натуральных логарифмов.

Таким образом, естественное предположение, вытекающее из рассмотрения таблиц, заключается в том, что $\pi(n)$ становится все ближе к $\frac{n}{\ln n}$. Доказанная теорема Чебышева утверждает (если пользоваться натуральными логарифмами) существование двух таких постоянных c и C, что $c\frac{n}{\ln n} < \pi(n) < C\frac{n}{\ln n}$, начиная с некоторого n. То гипотетическое уточнение, к которому можно прийти исходя из таблиц, утверждает, что неравенства $c\frac{n}{\ln n} < \pi(n) < C\frac{n}{\ln n}$ выполняются начиная с некоторого n, какие бы постоянные $c < 1$ и $C > 1$ мы ни взяли. Это утверждение называется *асимптотическим законом распределения* простых чисел. Оно было высказано Гауссом и другими математиками в конце XVIII и начале XIX в. После доказательства неравенств Чебышева в 1850 г. речь шла, казалось бы, только о более точном нахождении и сближении постоянных c и C. Однако асимптотический закон распределения простых чисел был доказан лишь полвека спустя, в самом конце XIX в., на основании совершенно новых идей, предложенных Риманом.

Задачи

1. Докажите, что $p_n > an\log n$ при некоторой постоянной $a > 0$. (Указание: воспользоваться тем, что $\pi(p_n) = n$.)

2. Докажите, что $\log n < \sqrt{n}$, начиная с некоторой границы (определите ее). (Указание: сведите вопрос к доказательству неравенства $2^x > x^2$ для вещественных x, начиная с некоторой границы. Пусть $n \le x \le n+1$, где n — целое. Сведите к доказательству неравенства $2^n \ge (n+1)^2$ и используйте индукцию.)

3. Докажите, что $p_n < Cn^2$ при некоторой постоянной C. (Указание: примените неравенство предшествующей задачи и воспользуйтесь тем, что $n = \pi(p_n)$.)

4. Докажите, что $p_n < An\log n$ при некоторой постоянной A.

5. Докажите, что показатель степени a в наибольшей степени p^a, делящей $n!$,

равен

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^k}\right]$$

Здесь $\left[\frac{r}{s}\right]$ — неполное частное от деления r на s, сумма распространяется на все k, для которых $p^k \leq n$, p обозначает произвольное простое число, а n — произвольное натуральное число.

6. При помощи результата задачи 5 дайте другое доказательство леммы в Приложении.

7. Докажите, что если $p_1, \ldots, p_r$ — все простые числа, заключенные между m и $2m+1$, то их произведение не превосходит 2^{2m}.

8. Определите постоянные c и C, при которых неравенство (10) выполнено при всех n.

9. Постарайтесь найти по возможности бóльшую постоянную c и по возможности мéньшую постоянную C, при которых неравенство (10) выполнено для всех n, начиная с некоторого.