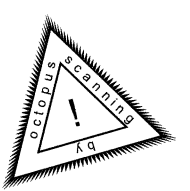
Я. И. ПЕРЕЛЬМАН

ПРОСТЫЕ ЧИСЛА

ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
ТЕХНИКО-ТЕОРЕТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1948 ЛЕНИНГРАД

Л. Г. ШНИРЕЛЬМАН

ПРОСТЫЕ ЧИСЛА



ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
ТЕХНИКО-ТЕОРЕТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1940 ЛЕНИНГРАД

Л. Г. Ш н и р е л ь м а н. Простые числа. Государственное издательство технико-теоретической литературы, 1940 г. Индекс 24-4-4. Изд.ат. № 13.

Редактор *Д. А. Райков.* Технический редактор *О. Залышкина.*
Корректоры: *А. С. Бакулова, З Л. Соколина.* и *В. Зазульская.*

Сдано в набор 31/X 1939 г. Подписано к печати 7/II 1940 г. Формат 84×108/32.
Объем: 15/16 бум. л., 5 3/4 печ. л., 3,4 авт. л., 3,5 уч. авт. л. Тип. зн. в печ. л. 44160.
Тираж 5000. Бумага Камской ф-ки Заказ № 2725.
Уполн. Главлита № А-23152 Цена книги 1 р. 25 к.

4-я тип. ОГИЗ'а им. Евг. Соколовой, Ленинград, пр. Красных Командиров, 29.

Предисловие.

Настоящая брошюра может служить введением в ту часть математики, которая занимается изучением свойств целых чисел и носит название теории чисел. В этой брошюре затрагиваются, однако, только те свойства целых чисел, которые связаны с разложением их на простые множители.

От читателя не требуется никаких предварительных познаний кроме школьного курса математики. Эта брошюра будет понятной также и интересующимся математикой учащимся последних классов средней школы.

Только для чтения последнего параграфа нужно иметь некоторые сведения из интегрального исчисления. Не знающие интегрального исчисления могут просто не читать этот параграф, нисколько не потеряв при этом главного содержания брошюры.

Можно также при чтении пропустить четвертый параграф, если он покажется трудным, потому что для понимания дальнейшего содержания брошюры этого параграфа знать не нужно.

Л. Шнирельман.

ОГЛАВЛЕНИЕ

§ 1. Разложение целых чисел на простые множители.

Мы будем считать известным понятие о целом числе, положительном и отрицательном, и о действиях сложения, вычитания, умножения и деления целых чисел.

Целые числа, положительные и отрицательные, могут быть расположены по величине в последовательность ..., —3, —2, —1, 0, 1, 2, 3, ..., бесконечную в обе стороны.

Сумма, разность и произведение двух целых положительных или отрицательных чисел есть снова целое положительное или отрицательное число. Частное от деления одного целого числа на другое может уже не быть целым числом.

Если целое число a при делении на целое число b дает целое частное c, то говорят, что a делится на b. Число b называется множителем или делителем числа a, число a называется кратным b.

Если число a равно произведению целых чисел $m_1 m_2 \dots m_i$, то говорят, что a разлагается на множители $m_1, m_2, \dots, m_i$.

Настоящая брошюра посвящена изучению закономерностей, касающихся делимости чисел и разложения чисел на множители.

Для всей теории делимости основным является понятие простого числа. Простым числом называется целое число, не имеющее никаких делителей, меньших его по абсолютной величине, кроме чисел ± 1 [1]). В дальнейшем под простыми числами мы будем всегда разуметь положительные простые числа.

В теории делимости чисел играет основную роль разложение всякого целого числа на простые множители.

Принцип математической индукции.

Мы будем в дальнейшем пользоваться важным вспомогательным средством при математических исследованиях, заключающимся в следующем общем положении, называемом принципом математической индукции:

---

[1]) ± 1 не причисляются к простым числам.

Если какое-нибудь свойство принадлежит числу 1 и если можно доказать, что справедливость этого свойства для чисел, не превосходящих n, влечет за собой справедливость его для числа $n+1$, то это свойство имеет место для всех целых положительных чисел.

В качестве приложения принципа математической индукции докажем следующее предложение:

Теорема. *Всякое целое положительное число либо равно единице, либо простое, либо может быть представлено в виде произведения простых чисел.*

Доказательство. Для единицы наша теорема, очевидно, справедлива. Пусть она имеет место для всех чисел, не превосходящих n. Докажем, что она верна и для $n+1$.

Если $n+1$ есть простое число, то теорема верна для $n+1$. Если $n+1$ не есть простое число, то $n+1=n_1n_2$, где n_1 и n_2 — числа, меньшие $n+1$. Числа n_1 и n_2, согласно предположению индукции, можно разложить на простые множители. Тогда из равенства $n+1=n_1n_2$ следует, что и $n+1$ можно разложить на простые множители.

Согласно принципу математической индукции, заключаем о справедливости высказанной теоремы для любых целых положительных чисел.

Доказательство Эвклида бесконечности ряда простых чисел.

Теорема. *Простых чисел существует бесконечное множество.*

Доказательство. Допустим, что простых чисел существует лишь конечное число, и пусть $p_1, p_2, \ldots, p_r$ будут все простые числа. Образуем произведение

$$p_1p_2\ldots p_r+1.$$

Согласно доказанному выше, это число должно разлагаться на простые множители. Пусть разложение его на простые множители напишется в виде

$$p_1p_2\ldots p_r+1=q_1q_2\ldots q_s.$$

Очевидно, что ни одно из простых чисел $q_1, q_2, \ldots, q_s$ не может совпадать ни с одним из $p_1, p_2, \ldots, p_r$, потому что совпадение p_i с q_j влекло бы за собой, на основании равенства $p_1p_2\ldots p_r-q_1q_2\ldots q_s=1$, делимость 1 на p_i, что, очевидно, абсурдно.

Мы доказали, таким образом, что из предположения, что кроме $p_1, p_2, \ldots, p_r$ других простых чисел нет, вытекало бы,

что кроме них существуют еще простые числа $q_1, q_2, \ldots, q_s$. Полученное противоречие доказывает теорему.

Примечание. Аналогично можно доказать, что существует бесконечное множество простых чисел вида $4n-1$. Именно, предполагая, что простых чисел вида $4n-1$ существует лишь ограниченное число: $q_1, q_2, \ldots, q_r$, образуем произведение $m = 4q_1q_2 \ldots q_r - 1$. Это число не может иметь лишь простых множителей вида $4n+1$, так как произведение чисел подобного вида также имело бы вид $4n+1$. Так как всякое нечетное простое число имеет или вид $4n+1$, или вид $4n-1$, то среди простых множителей числа m должно быть по крайней мере одно простое число вида $4n-1$, которое, очевидно, не совпадает ни с одним из q_i, и значит $q_1, q_2, \ldots, q_r$ не исчерпывают все простые числа вида $4n-1$.

Совершенно так же докажем, что существует бесконечное множество простых чисел вида $6n-1$.

Некоторые общие замечания о целых числах.

Приведем следующие, хотя и простые, но важные и часто применяемые свойства целых чисел.

а) Существует лишь конечное число целых положительных чисел, меньших данного целого числа. Поэтому

б) Если имеем последовательность убывающих целых положительных чисел $n_1 > n_2 > n_3 > \ldots$, то такая последовательность всегда конечна.

в) Если имеется какое-нибудь множество целых положительных чисел, меньших данного, то среди них всегда найдутся наибольшее и наименьшее.

Общий наибольший делитель.

Общим наибольшим делителем целых чисел m и n называется наибольшее из целых чисел, являющихся одновременно делителями m и n. Такое число должно существовать на основании замечания в).

Предварительные замечания. а) Если два числа m и n делятся на число d, то все числа вида $km \pm ln$, где k и l — целые числа, тоже делятся на d.

Доказательство. Обозначим частные от деления m на d и n на d соответственно через m_1 и n_1. Тогда, очевидно, $km \pm ln = d(km_1 \pm ln_1)$, т. е. $km \pm ln$ делится на d.

Этим свойством мы уже пользовались при изложении доказательства Эвклида бесконечности ряда простых чисел.

б) Вычитая из целого положительного числа a наибольшее не превосходящее его кратное cb целого положительного числа b, получим остаток r от деления a на b, так что $a = cb + r$; c называют частным от деления a на b. Остаток r меньше b. Он равен нулю тогда и только тогда, когда a делится на b.

Алгорифм Эвклида.

Пусть даны два числа m и n, и $m > n$. Разделим m на n и образуем частное m_1 и остаток r_1. Имеем $m = m_1 n + r_1$. Докажем, что общий наибольший делитель чисел m и n равен общему наибольшему делителю чисел n и r_1. Для этого достаточно показать, что всякий общий делитель чисел m и n является общим делителем чисел n и r_1 и обратно. Но на основании замечания а) видим из равенства $m = m_1 n + r_1$, что всякий общий делитель чисел n и r_1 делит m (и n), а из равенства $r_1 = m - m_1 n$ видим, что всякий общий делитель чисел m и n делит r_1 (и n).

Если формулировать словами полученный результат, то можно сказать, что общий наибольший делитель чисел m и n равен общему наибольшему делителю числа n и остатка от деления m на n. Этот остаток меньше n.

Таким образом задача о нахождении общего наибольшего делителя чисел m и n свелась к задаче о нахождении общего наибольшего делителя меньших чисел n и r_1.

Алгорифм Эвклида заключается в повторном применении этого приема. Применяя его к числам n и r_1, получим новые числа r_1 и r_2, где r_2 есть остаток от деления n на r_1. Общий наибольший делитель чисел r_1 и r_2 тот же, что у n и r_1, т. е. у m и n. r_1 и r_2, в свою очередь, заменяем через r_2 и r_3, где r_3 есть остаток от деления r_1 на r_2, и т. д.

Так как каждое следующее r_{i+1} меньше предшествующего r_i, то их последовательность не может быть бесконечной. Поэтому при повторении последовательного деления r_i на r_{i+1} мы должны притти, в конце концов, к такому r_j, которое делится нацело на r_{j+1}, давая в качестве следующего остатка r_{j+2} нуль. Общий наибольший делитель всякой пары последовательных r_i и r_{i+1}, в частности r_j и r_{j+1}, равен общему наибольшему делителю m и n. Но r_j делится на r_{j+1}. Их общим наибольшим делителем является, очевидно, r_{j+1}. Следовательно, общий наибольший делитель m и n равен r_{j+1}.

Иными словами, общий наибольший делитель двух целых чисел m и n равен последнему не равному нулю остатку, получающемуся при применении алгорифма Эвклида к числам m и n.

Следствие 1. Обозначим последовательные частные, получающиеся при применении алгорифма Эвклида, через m_1, $m_2, \ldots, m_j$. На основании связи между делимым, делителем и остатком, очевидно, имеем

$$\begin{aligned} r_1 &= m - m_1 n, \\ r_2 &= n - m_2 r_1, \\ r_3 &= r_1 - m_3 r_2, \\ &\cdots\cdots \\ r_{j+1} &= r_{j-1} - m_{j+1} r_j. \end{aligned}$$

$r_{j+1} = d =$ общему наибольшему делителю m и n. Вставляя последовательно выражения $r_1, r_2, \ldots, r_j$ в последующие, получим соотношение вида

$$r_{j+1} = d = mX - nY,$$

где X и Y — целые числа.

Следствие 2. Если m и n — взаимно простые числа, т. е. их общий наибольший делитель равен 1, то можно подобрать целые числа X и Y, удовлетворяющие уравнению

$$mX - nY = 1.$$

Следствие 3. Если произведение целых чисел m и n делится на число k, взаимно простое с m, то n должно делиться на k.

Доказательство. Так как m взаимно простое с k, то по следствию 2 можно подобрать числа X и Y, удовлетворяющие уравнению

$$mX - kY = 1.$$

Умножая обе части этого уравнения на n, получаем уравнение

$$mnX - knY = n.$$

Левая его часть делится на k, потому что mn делится на k по условию. Следовательно, n делится на k.

Следствие 4. Если произведение чисел m и n делится на простое число p, то или m, или n делится на p.

Доказательство. Если m не делится на p, то, ввиду простоты числа p, m взаимно простое с p, и тогда, на основании следствия 3, n должно делиться на p.

Теорема. *Всякое целое положительное число разлагается единственным образом на простые множители, если отвлечься от порядка сомножителей в разложении.*

Доказательство. Пусть мы имеем два разложения одного и того же числа на простые множители, т. е. равенство

$$p_1 p_2 \dots p_r = q_1 q_2 \dots q_s, \qquad (*)$$

где все p и q — простые числа.

На основании следствия 4, из того, что произведение $q_1 q_2 \dots q_s$ делится на p_r, следует, что один из сомножителей q_i должен делиться на p_r. В самом деле, $q_1 q_2 \dots q_s$ есть произведение двух множителей q_1 и $q_2 \dots q_s$, и по следствию 4, если q_1 не делится на p_r, то $q_2 \dots q_s = q_2 (q_3 \dots q_s)$ делится на p_r. Тогда, если q_2 не делится на p_r, то $q_3 \dots q_s$ делится на p_r, и т. д. Таким образом, в конце концов, мы придем к числу q_i, делящемуся на p_r. Это число, как простое, должно совпадать с p_r[1]). Деля обе части равенства (*) на p_r, получим равенство

$$p_1 p_2 \dots p_{r-1} = q_1 q_2 \dots q_{i-1} q_{i+1} \dots q_s.$$

Повторяя то же рассуждение применительно к p_{r-1}, получим

$$p_{r-1} = q_{i_1}.$$

Продолжая это рассуждение, убедимся в том, что каждое p_i совпадает с каким-нибудь из q_j и обратно, т. е. $r = s$ и $p_1, p_2, \dots, p_r$ и $q_1, q_2, \dots, q_r$ представляют одну и ту же совокупность чисел, если отвлечься от порядка, в котором они расположены.

Следствие 1. В силу доказанной теоремы всякое целое положительное число может быть, и притом единственным образом, представлено в виде произведения

$$p_1^{\alpha_1} \dots p_r^{\alpha_r},$$

где $p_1, \dots, p_r$ — различные простые числа, а показатели степеней — целые неотрицательные.

Следствие 2. Каждый делитель числа $p_1^{\alpha_1} \dots p_r^{\alpha_r}$ имеет вид

$$p_1^{\beta_1} \dots p_r^{\beta_r},$$

где $0 \leqslant \beta_1 \leqslant \alpha_1, \dots, 0 \leqslant \beta_r \leqslant \alpha_r$.

Доказательство. В силу единственности представления числа в виде $p_1^{\alpha_1} \dots p_r^{\alpha_r}$ ни один из его делителей не может делиться на простое число, не содержащееся среди чисел $p_1, \dots, p_r$. По той же причине ни один из делителей числа $p_1^{\alpha_1} \dots p_r^{\alpha_r}$ не может содержать, например, p_1 в сте-

[1]) Подчеркнем еще раз, что мы всюду предполагаем простые числа положительными.

пени, высшей чем α_1. В обоих случаях, умножая делитель на частное от деления на него числа $p_1^{\alpha_1} \dots p_r^{\alpha_r}$, мы получили бы существенно отличное разложение этого последнего числа на простые множители.

Применения теоремы о разложении чисел на простые множители.

I. Решение неопределенного уравнения,

$$x^2 + y^2 = z^2$$

в целых числах.

Можно предположить x, y, z не имеющими общего множителя, бóльшего единицы, ибо иначе можно было бы заранее сократить обе части уравнения $x^2 + y^2 = z^2$ на квадрат этого множителя. Из этого предположения будет следовать, очевидно, что x, y, z попарно взаимно просты, ибо если бы, например, x и y делилось на $d > 1$, то и z делилось бы на d. Таким образом, в частности, одно из чисел x, y должно быть нечетным. Легко видеть, что другое должно быть четным. В противном случае, если бы $x = 2k + 1$, $y = 2l + 1$, то $x^2 + y^2 = 4(k^2 + k + l^2 + l) + 2$ делилось бы на 2, но не делилось бы на 4 и не могло бы быть поэтому квадратом [1]).

Пусть x четное, y нечетное; тогда z нечетное. Полагая $z - y = 2t$, $z + y = 2u$, имеем

$$x^2 = z^2 - y^2 = (z + y)(z - y) = 4tu.$$

t и u взаимно просты. В самом деле, если бы t и u имели общего множителя $d > 1$, то d входил бы также в $z = t + u$ и $y = u - t$, а мы видели, что z и y взаимно просты.

Поэтому t и u должны быть порознь точными квадратами.

Докажем это. Именно здесь мы будем опираться на теорему о разложении чисел на простые множители. Имеем

$$tu = \left(\frac{x}{2}\right)^2 = \left(p_1^{\alpha_1} \dots p_r^{\alpha_r}\right)^2 = p_1^{2\alpha_1} \dots p_r^{2\gamma_r}.$$

Таким образом, в силу следствия 2 теоремы о разложении,

$t = p_1^{\beta_1} \dots p_r^{\beta_r}$, $u = p_1^{\gamma_1} \dots p_r^{\gamma_r}$, где $\beta_i + \gamma_i = 2\alpha_i$ $(i = 1, \dots, r)$.

Но так как t и u взаимно просты, то для каждого i одно из чисел β_i, γ_i равно нулю и потому другое равно $2\alpha_i$. Значит,

---

[1]) Если a^2 четно, то и a четно, $a = 2b$, $a^2 = 4b^2$, т. е. a^2 делится на 4. Таким образом квадрат не может делиться на 2, не делясь на 4.

все показатели в разложениях чисел t и u четны, откуда и следует, что каждое из этих чисел есть точный квадрат:

$$t = t_1^2, \quad u = u_1^2.$$

Отсюда

$$x = 2u_1t_1, \quad y = u_1^2 - t_1^2, \quad z = u_1^2 + t_1^2. \qquad (**)$$

Таким образом каждое решение уравнения (*) во взаимно простых целых числах должно быть представимо в виде (**), где t_1 и u_1 — взаимно простые целые числа, из которых одно четно, а другое нечетно (иначе y и z были бы оба четными). Но и обратно, каковы бы ни были взаимно простые целые числа t_1 и u_1 разной четности, числа x, y, z, составленные из них по формулам (**), дают решение уравнения (*) во взаимно простых числах. В самом деле, прежде всего

$$x^2 + y^2 = 4u_1^2t_1^2 + (u_1^2 - t_1^2)^2 = (u_1^2 + t_1^2)^2 = z^2;$$

кроме того, если бы y и z делились на простое число d, то также $z - y = 2t_1^2$ и $z + y = 2u_1^2$ делились бы на d, и так как d не может быть равно 2 (ибо, в силу разной четности чисел t_1 и u_1, y и z нечетны), то в силу следствия 4 (стр. 9) u_1 и t_1 должны были бы делиться на d, в противоречие с предположением о их взаимной простоте. Следовательно, y и z, а значит, также все три числа x, y и z взаимно просты.

Таким образом формулы (**) при t_1 и u_1 взаимно простых разной четности дают все решения уравнения (*) во взаимно простых целых числах.

II. Доказательство теоремы Ферма для четвертых степеней.

Докажем следующую теорему:

Уравнение $x^4 + y^4 = z^4$ не имеет решений в целых числах, отличных от нуля, и даже более: уравнение $x^4 + y^4 = z^2$ не имеет отличных от нуля целых решений.

Доказательство. Допустим, что существует система отличных от нуля решений последнего уравнения. Тогда среди этих систем решений должна существовать такая, для которой z принимает наименьшее возможное значение. Покажем, что x и y при этом будут взаимно простыми. В самом деле, если бы x и y имели общий делитель d, то z делилось бы на d и целые числа $\frac{x}{d}$, $\frac{y}{d}$ и $\frac{z}{d}$ давали бы систему решений с меньшим z.

Как и в предшествующем исследовании уравнения $x^2 + y^2 = z^2$, убеждаемся в том, что из пары чисел x и y одно должно быть четным, другое нечетным.

Пусть x четное. На основании выведенных выше формул (**) имеем

$$x^2 = 2uv, \quad y^2 = u^2 - v^2, \quad z = u^2 + v^2,$$

причем u и v — взаимно простые числа, одно из которых нечетное, а другое — четное. Если бы u было четным, v — нечетным, то y^2 имело бы вид $4t^2 - (4k^2 + 4k + 1) = 4l - 1$, что невозможно, ибо квадрат нечетного числа всегда имеет вид $4m + 1$. Поэтому $v = 2q$, $\left(\frac{1}{2}x\right)^2 = uq$, и так как u и q взаимно просты, то так же, как выше, убеждаемся в том, что

$$u = r^2, \quad q = s^2,$$

где r и s взаимно просты, причем r нечетное.

Равенство $y^2 = u^2 - v^2$ перепишется теперь в виде

$$(2s^2)^2 + y^2 = r^4,$$

где $2s^2$ и y взаимно просты. Отсюда снова находим

$$2s^2 = 2mn, \quad r^2 = m^2 + n^2,$$

где m и n взаимно просты. Первое из этих равенств, как и выше, показывает, что

$$m = a^2, \quad n = b^2,$$

а это в соединении со вторым дает

$$a^4 + b^4 = r^2.$$

Но, очевидно, $r \leqslant r^2 = u \leqslant u^2 < z$, и, таким образом, мы пришли к уравнению того же вида $x^4 + y^4 = z^4$, но с меньшим z, в противоречие с предположением о минимальности z.

§ 2. Сравнения.

Если разность чисел a и b делится на число m, то a и b называют сравнимыми по модулю m.

Записывают эту зависимость следующим образом:

$$a \equiv b \pmod{m}.$$

Подобного рода зависимости обладают рядом свойств обыкновенных равенств. Например, если

$$a \equiv b \pmod{m}, \quad a_1 \equiv b_1 \pmod{m_1},$$

то

$$a + a_1 \equiv b + b_1 \pmod{m}, \quad a - a_1 \equiv b - b_1 \pmod{m} \tag{1}$$

и

$$aa_1 \equiv bb_1 \pmod{m}. \tag{2}$$

В справедливости этих соотношений легко убедиться, если заметить, что $a \equiv b \pmod m$ означает, что $a = b + um$, где u — некоторое целое число, и аналогично $a_1 \equiv b_1 \pmod m$ означает, что $a_1 = b_1 + u_1 m$; отсюда $a \pm a_1 = b \pm b_1 + (u \pm u_1) m$, $aa_1 = bb_1 + (u + u_1 + muu_1) m$, а эти равенства означают, что имеют место сравнения (1) и (2).

Применяя последовательно сложение, вычитание и умножение сравнений, получим следующее общее правило:
Если

$$a \equiv b \pmod m, \quad a_1 \equiv b_1 \pmod m, \ldots, \quad a_i \equiv b_i \pmod m,$$

то

$$F(a_1, a_2, \ldots, a_i) \equiv F(b_1, b_2, \ldots, b_i) \pmod m$$

для любого выражения F, составленного из своих аргументов путем конечного числа сложений, вычитаний и умножений.

Так как каждое число, очевидно, сравнимо с собой по любому модулю:

$$c \equiv c \pmod m,$$

то из (2), в частности, вытекает, что обе части сравнения можно умножить на любое целое число:

$$\text{если } a \equiv b \pmod m, \text{ то и } ca \equiv cb \pmod m.$$

Не так обстоит дело с делением: если $a \equiv b \pmod m$ и a и b делятся на $c > 1$, то отсюда еще не следует, что обе части сравнения можно сократить на c, т. е. что также

$$\frac{a}{c} \equiv \frac{b}{c} \pmod m.$$

В этом убеждаемся уже на простом примере: $6 \equiv 4 \pmod 2$, но $\frac{6}{2} \not\equiv \frac{4}{2} \pmod 2$.

Однако если a и b имеют общий делитель, взаимно простой с модулем m, то на него сравнение можно сократить. В самом деле, пусть $a = a'd$, $b = b'd$ и d взаимно просто с m. Сравнение $a \equiv b \pmod m$ означает, что $a - b = (a' - b')d$ делится на m; но так как d взаимно просто с m, то $a' - b'$ должно делиться на m, т. е. должно выполняться сравнение $\frac{a}{d} \equiv \frac{b}{d} \pmod m$, что мы и утверждали.

Деля любое целое число на m, убеждаемся в том, что всякое целое число сравнимо по модулю m с одним из чисел $0, 1, \ldots, m-1$, остатком от деления его на m.

Малая теорема Ферма.

Если какая-нибудь величина может принимать значения $a_1, a_2, \ldots, a_k$, сравнимые по модулю m соответственно с $b_1, b_2, \ldots, b_k$, то мы будем говорить, что эта величина принимает значения $b_1, b_2, \ldots, b_k$ по модулю m.

Пусть p — простое число. Рассмотрим величину $y = ax$, где x пробегает значения $1, 2, \ldots, p-1$ и a не делится на p. Покажем, что y тоже принимает те же значения $1, 2, \ldots, p-1$ по модулю p, но, быть может, в другом порядке.

В самом деле, для двух разных по модулю p значений x_1 и x_2 y принимает разные по модулю p значения, ибо, если бы было $ax_1 \equiv ax_2 \pmod{p}$, то $a(x_1 - x_2)$ делилось бы на p, т. е. $x_1 - x_2$ делилось бы на p против предположения. Поэтому y должно принимать по модулю p ровно $p-1$ различных значений, среди которых нет нуля. Но это значит, что y принимает все значения по модулю p кроме 0, т. е. $1, 2, \ldots, p-1$, проходимые в каком-то порядке.

В силу доказанного выше правила произведение всех значений x сравнимо с произведением всех значений y по модулю p, т. е.

$$a \cdot 1 \cdot a \cdot 2 \cdot a \cdot 3 \ldots a \cdot (p-1) \equiv 1 \cdot 2 \ldots (p-1) \pmod{p},$$

или

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

Ввиду того что p простое, произведение $1 \cdot 2 \ldots (p-1)$ взаимно просто с p, и, как доказано выше, можно обе части сравнения разделить на него. Получим сравнение

$$a^{p-1} \equiv 1 \pmod{p},$$

где a — любое не делящееся на p число. Это сравнение было указано впервые Ферма. Его можно, очевидно, писать также в форме

$$a^p \equiv a \pmod{p}.$$

В этой форме оно справедливо для любого a (в том числе и делящегося на p).

Функция Эйлера.

Пусть n — целое положительное число. Обозначим через $\varphi(n)$ число целых чисел, не превосходящих n и взаимно простых с n. Имеем $\varphi(1) = \varphi(2) = 1$, $\varphi(3) = \varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$. Докажем следующее свойство функции $\varphi(n)$: если a и b — взаимно простые положительные целые числа, то $\varphi(ab) = \varphi(a)\varphi(b)$.

Все положительные целые числа, меньшие ab, могут быть, как убеждаемся делением их на a, единственным образом представлены в форме $aq+r$, где r принимает значения $0, 1, \ldots, a-1$, а q — значения $0, 1, \ldots, b-1$. Число вида $aq+r$ будет взаимно простым с a тогда и только тогда, когда r взаимно просто с a. Таких чисел r имеется $\varphi(a)$. Пусть r_1 — одно из этих чисел.

Образуем числа $r_1, a+r_1, 2a+r_1, \ldots, (b-1)a+r_1$. Остатки этих чисел по модулю b все различны и поэтому суть числа $0, 1, \ldots, b-1$, расположенные, быть может, в другом порядке. В самом деле, если бы $ca+r_1$ и $da+r_1$, где $0 \leqslant c < b$, $0 \leqslant d < b$ и $c \neq d$, давали одинаковые остатки при делении на b, то их разность $(ca+r_1)-(da+r_1) = (c-d)a$ делилась бы на b, а значит (ввиду взаимной простоты a и b), также разность $c-d$ делилась бы на b, что невозможно, ибо c и d меньше b и по предположению различны. Поэтому среди выписанных чисел имеется ровно $\varphi(b)$ взаимно простых с b, — столько, сколько имеется взаимно простых с b среди их остатков $0, 1, \ldots, b-1$. Мы видим, что каждому r_1, взаимно простому с a, соответствует ровно $\varphi(b)$ чисел вида r_1+aq, взаимно простых с b, а значит, и с ab. Поэтому общее число чисел, взаимно простых с ab и меньших ab, равно $\varphi(a)\varphi(b)$. Но, с другой стороны, это число есть $\varphi(ab)$. Поэтому $\varphi(ab) = \varphi(a)\varphi(b)$.

Пусть теперь p — простое число, e — положительное целое число. Докажем, что $\varphi(p^e) = p^{e-1}(p-1) = p^e\left(1-\frac{1}{p}\right)$.

В самом деле, из совокупности чисел, меньших p^e, те и только те будут взаимно просты с p^e, которые не делятся на p. Число делящихся на p чисел, меньших p^e, равно p^{e-1}. Поэтому не делящихся на p и меньших чем p^e целых чисел остается $p^e - p^{e-1} = p^e\left(1-\frac{1}{p}\right)$. Отсюда $\varphi(p^e) = p^e\left(1-\frac{1}{p}\right)$.

Сопоставляя только что доказанные свойства функции $\varphi(n)$, получаем следующий результат:

Если разложение числа n на степени различных простых множителей есть $p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$, то

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\ldots\varphi(p_k^{\alpha_k}) =$$

$$= p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right)p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right)\ldots p_k^{\alpha_k}\left(1-\frac{1}{p_k}\right),$$

т. е.

$$(\varphi n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right).$$

Эйлерово обобщение

Пусть a — число, взаимно простое с n (a и n — положительные). Тогда

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

В самом деле, обозначим через $a_1, a_2, \ldots, a_k$ все числа, меньшие n и взаимно простые с n. Их количество k равно $\varphi(n)$. Два числа aa_i и aa_j при $i \neq j$ не могут давать при делении на n одинаковых остатков, ибо в противном случае разность $a(a_i - a_j)$, а значит (ввиду взаимной простоты a и n), также $a_i - a_j$ делилась бы на n, что невозможно, ибо a_i и a_j меньше n и по предположению различны. Следовательно, число различных среди остатков от деления чисел aa_i на n равно k, т. е. $\varphi(n)$. Но все эти остатки, очевидно, взаимно просты с n. Поэтому остатки чисел aa_i по модулю n суть, расположенные, быть может, в другом порядке, те же числа $a_1, a_2, \ldots, a_k$.

Произведение $(aa_1)(aa_2)\ldots(aa_k)$ должно поэтому сравнимо с $a_1a_2\ldots a_k$ по модулю n, т. е.

$$a^k a_1 a_2 \ldots a_k \equiv a_1 a_2 \ldots a_k \pmod{n}.$$

Ввиду того что $a_1, a_2, \ldots, a_k$ взаимно просты с n, можем сократить обе части сравнения на произведение этих чисел. Вспоминая, что $k = \varphi(n)$, окончательно получаем

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Сравнение первой степени.

Пусть требуется найти число x, удовлетворяющее сравнению

$$ax \equiv b \pmod{n}.$$

Это сравнение равносильно неопределенному уравнению $ax - ny = b$. Если a и n не имеют общих делителей, то, как мы убедились при ознакомлении с алгорифмом Эвклида, это неопределенное уравнение имеет решение. Нетрудно видеть, что по модулю n такое решение единственно. В самом деле, если $ax_1 \equiv b \pmod{n}$ и $ax_2 \equiv b \pmod{n}$, то $ax_1 \equiv ax_2 \pmod{n}$, т. е. $x_1 \equiv x_2 \pmod{n}$ (ввиду взаимной простоты чисел a и n).

Сравнения высших степеней по простому модулю.

Если имеем сравнение n-й степени ($n < p$)

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv 0 \pmod{p}, \qquad (A)$$

где p — простое число и не все a_i делятся на p, то такое сравнение имеет не более n решений, различных по модулю p.

Для сравнения первой степени теорема верна. Пусть она верна для всех степеней до $n-1$. Покажем, что она верна тогда и для степени n.

В самом деле, пусть α есть решение сравнения (А). Мы можем предположить a_0 не делящимся на p, ибо в противном случае степень сравнения можно было бы понизить. Делим $f(x)$ на $x-\alpha$. Получим в частном многочлен $Q(x)$ с целыми коэфициентами и в остатке целое число R, не зависящее от x:

$$f(x) = (x-\alpha)\,Q(x) + R.$$

Подставляя $x = \alpha$, получим $f(\alpha) = R$. Но $f(\alpha) \equiv 0 \pmod p$. Поэтому $R \equiv 0 \pmod p$, и наше сравнение можно записать так:

$$f(x) \equiv (x-\alpha)\,Q(x) \equiv 0 \pmod p.$$

Но мы знаем, что если произведение делится на простое число p, то хоть один из сомножителей должен делиться на p. Поэтому наше сравнение дает:

$$\text{или} \quad x-\alpha \equiv 0 \pmod p,$$

$$\text{или} \quad Q(x) \equiv 0 \pmod p.$$

Первое сравнение имеет одно решение, второе есть сравнение $(n-1)$-й степени, которое по предположению имеет не более $n-1$ решения, потому что старший коэфициент многочлена $Q(x)$ равен a_0 и не делится на p. Таким образом наше сравнение n-й степени имеет не более n решений.

На основании принципа математической индукции заключаем, что теорема верна для любой степени n.

Говоря о числе решений сравнения, мы будем в дальнейшем подразумевать под ним число решений, различных по модулю сравнения.

Следствие 1. Если сравнение n-й степени $(n < p)$

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv 0 \pmod p$$

имеет более n решений, то все его коэфициенты делятся на p.

Следствие 2. Если имеем сравнение

$$f_n(x)\,f_m(x) \equiv 0 \pmod p, \qquad \text{(В)}$$

где $f_n(x)$ — многочлен n-й степени, а $f_m(x)$ — многочлен m-й степени, и знаем, что это сравнение имеет $n+m$ решений, то сравнения $f_n(x) \equiv 0 \pmod p$ и $f_m(x) \equiv 0 \pmod p$ имеют соответственно n и m решений.

Действительно, если бы одно из этих сравнений имело меньшее число решений, чем n, или соответственно m, то (В) имело бы меньше, чем $n+m$, решений.

Следствие 3. Рассмотрим сравнение

$$x^{p-1} - 1 \equiv 0 \pmod{p}. \qquad (C)$$

Это сравнение на основании теоремы Ферма имеет $p-1$ решение $1, 2, \ldots, p-1$. Пусть p не есть 2, тогда $p-1$ есть четное число и сравнение (C) можно представить в виде

$$\left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}.$$

На основании следствия 2 заключаем, что оба сравнения

$$x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p} \quad \text{и} \quad x^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$$

имеют по $\frac{p-1}{2}$ решений каждое.

Следствие 4. *Теорема Вильсона.*

Рассмотрим сравнение

$$x^{p-1} - 1 \equiv (x-1)(x-2)\ldots(x-p+1) \pmod{p},$$

где p — простое число. На основании теоремы Ферма видим, что это сравнение имеет $p-1$ решение $1, 2, \ldots, p-1$. Но x^{p-1} можно сократить в обеих частях. Получится сравнение степени $p-2$, имеющее $p-1$ решение, что, согласно следствию 1, возможно только в том случае, если все коэфициенты в правой и левой частях сравнимы по модулю p. Взяв, в частности, свободные члены, получаем сравнение

$$-1 \equiv (-1)^{p-1}(p-1)! \pmod{p}.$$

Если p — нечетное простое число, то $(-1)^{p-1} = +1$, и

$$(p-1)! \equiv -1 \pmod{p}.$$

Непосредственная проверка показывает, что последнее сравнение выполняется и при $p = 2$, т. е. оно имеет место для любого простого p.

Нетрудно доказать и обратное предложение: если

$$(n-1)! \equiv -1 \pmod{n},$$

то число n простое.

В самом деле, если бы $n = ab$, где a и b больше 1, то $(n-1)!$ делилось бы на a и сумма $(n-1)! + 1$ не могла бы делиться на a.

Определение. Квадратичным вычетом по модулю n называют такое число d, для которого существует решение сравнения

$$x^2 \equiv d \pmod{n}.$$

Если для числа d решения этого сравнения не существует, то d называют квадратичным невычетом по модулю n.

Пусть p — простое нечетное число. Докажем, что по модулю p существует ровно $\frac{p-1}{2}$ квадратичных вычетов и ровно $\frac{p-1}{2}$ квадратичных невычетов.

В самом деле, все числа, не делящиеся на p, суть $1, 2, \ldots, p-1$ (по модулю p). Если мы возведем их в квадрат, то получим $1^2, 2^2, \ldots, (p-1)^2$. Очевидно, $a^2 \equiv (p-a)^2 = p^2 - 2ap + a^2 \pmod{p}$. Поэтому последняя половина этих квадратов дает по модулю p те же числа, что и первая. Это означает, что может существовать не более $\frac{p-1}{2}$ квадратичных вычетов по модулю p. Рассмотрим числа $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$. Эти числа все различны по модулю p. В самом деле, если i и j пробегают значения $1, 2, \ldots, \frac{p-1}{2}$, то $i^2 - j^2 = (i+j)(i-j)$ не может делиться на p, ибо оба множителя $i+j$ и $i-j$ меньше p. Поэтому $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ все различны по модулю p и дают $\frac{p-1}{2}$ вычетов $d_1, d_2, \ldots, d_{\frac{p-1}{2}}$ по модулю p. Все остальные $\frac{p-1}{2}$ чисел, отличных от $d_1, d_2, \ldots, d_{\frac{p-1}{2}}$ и меньших p, дадут невычеты по модулю p.

Докажем следующую теорему: необходимое и достаточное условие того, чтобы число d было вычетом или невычетом по простому нечетному модулю p, является выполнение соответственно сравнений

$$d^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

или

$$d^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

В самом деле, пусть d есть вычет по модулю p. Тогда существует такое x, что $x^2 \equiv d \pmod{p}$. Возводя обе части этого сравнения в $\left(\frac{p-1}{2}\right)$-ю степень, получаем в силу теоремы Ферма $1 \equiv x^{p-1} \equiv d^{\frac{p-1}{2}} \pmod{p}$. Таким образом сравнению $y^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ удовлетворяют все $\frac{p-1}{2}$ вычетов по

модулю p. Но мы знаем, что сравнение $y^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ тоже должно иметь $\frac{p-1}{2}$ решений (очевидно, уже не могущих быть вычетами). Поэтому последнее сравнение имеет своими решениями все $\frac{p-1}{2}$ невычетов.

Следствие 1. Для того чтобы -1 была квадратичным вычетом по простому нечетному модулю p, необходимо и достаточно, чтобы p имело вид $4n+1$. Наоборот, для того чтобы -1 была невычетом по простому нечетному модулю p, необходимо и достаточно, чтобы p имело вид $4n+3$.

В самом деле, всякое нечетное простое число p должно иметь или вид $4n+1$, или вид $4n+3$. В первом случае

$$(-1)^{\frac{4n+1-1}{2}} \equiv +1 \pmod{p},$$

во втором

$$(-1)^{\frac{4n+3-1}{2}} \equiv -1 \pmod{p}.$$

На основании предыдущего критерия видим, что в первом случае -1 есть вычет, во втором — невычет.

Иными словами этот результат можно выразить так: если простое число p имеет вид $4n+1$, то существует такое x, что x^2+1 делится на p; если же p имеет вид $4n+3$, то оно не может быть делителем выражения x^2+1.

Следствие 2. Число вида a^2+b^2, где a и b — взаимно простые числа, имеет простые множители только вида $4n+1$.

В самом деле, пусть p — простой множитель числа a^2+b^2. a не может делиться на p, ибо в противном случае b тоже делилось бы на p, что противоречит взаимной простоте чисел a и b. Найдем число a', удовлетворяющее сравнению $aa' \equiv 1 \pmod{p}$. Очевидно, p есть делитель числа $(aa')^2+(ba')^2$, следовательно, p есть также делитель числа $1+(ba')^2$. Делителями же этого последнего числа, как мы видели, могут быть только простые числа вида $4n+1$.

Следствие 3. Существует бесконечное множество простых чисел вида $4n+1$.

В самом деле, пусть простых чисел вида $4n+1$ имеется лишь конечное число. Обозначим их через $q_1, q_2, \ldots, q_t$. В силу следствия 1 число $(q_1 q_2 \ldots q_t)^2+1$ может иметь простые множители только вида $4n+1$. С другой стороны, ни один из простых множителей этого числа не может совпадать ни с одним из q_i. Полученное противоречие и доказывает наше утверждение.

§ 3. Теория целых комплексных чисел.

Целыми комплексными числами называются комплексные числа вида $a+bi$, где a и b — обыкновенные целые числа (каждое из которых может быть положительным, отрицательным или нулем).

Гаусс показал, что для целых комплексных чисел можно построить теорию разложения на множители, аналогичную той, которая имеет место для обыкновенных целых чисел. Эта теория представляет значительный интерес и с точки зрения изучения свойств обычных целых чисел, потому что она связана с разложением обычных целых чисел на сумму двух квадратов.

Над комплексными числами, как известно, производят действия сложения, вычитания, умножения и деления по следующим правилам:

$$(a+bi)+(a_1+b_1i)=(a+a_1)+(b+b_1)i,$$

$$(a+bi)-(a_1+b_1i)=(a-a_1)+(b-b_1)i,$$

$$(a+bi)(a_1+b_1i)=(aa_1-bb_1)+(ab_1+a_1b)i,$$

$$\frac{a+bi}{a_1+b_1i}=\frac{(a+bi)(a_1-b_1i)}{a_1^2+b_1^2}=\frac{aa_1+bb_1}{a_1^2+b_1^2}+\frac{a_1b-ab_1}{a_1^2+b_1^2}i.$$

Как видно из этих формул, если $a+bi$ и a_1+b_1i — целые комплексные числа, то их сумма, разность и произведение — тоже целые комплексные числа. Частное же двух целых комплексных чисел может и не быть целым комплексным числом (частное обычных целых чисел ведь тоже уже не всегда целое).

Если частное от деления числа $A=a+bi$ на $B=c+di$ есть целое комплексное число, то говорят, что A делится на B.

Существуют четыре числа $+1$, -1, $+i$, $-i$, на которые делится любое целое комплексное число; действительно,

$$\frac{a+bi}{+1}=a+bi,\quad \frac{a+bi}{-1}=-a+(-b)i,$$

$$\frac{a+bi}{i}=b+(-a)i,\quad \frac{a+bi}{-i}=-b+ai.$$

Легко видеть, что кроме указанных четырех чисел других подобных чисел не существует. В самом деле, пусть $z=x+yi$ есть целое комплексное число, на которое делится любое другое. Тогда, в частности, на него делится 1. Имеем

$$\frac{1}{x+yi}=\frac{x}{x^2+y^2}-\frac{y}{x^2+y^2}i.$$

Для того чтобы $\frac{x}{x^2+y^2}$ и $\frac{y}{x^2+y^2}$ были обыкновенными целыми числами, необходимо, чтобы или $x=0$, $y=\pm 1$, или $y=0$, $x=\pm 1$ ($x=0$, $y=0$ здесь не может быть), т. е. необходимо, чтобы z совпадало с одним из чисел $+1$, -1, $+i$ или $-i$.

Числа $+1$, -1, $+i$, $-i$ будем называть единицами в области целых комплексных чисел. Если имеем два целых комплексных числа A и B, то может случиться, что имеется комплексное число C, не являющееся одной из единиц, которое является одновременно делителем A и B. Может случиться, что такого общего делителя (не считая, разумеется, единицы) не имеется. В последнем случае A и B называются взаимно простыми в области целых комплексных чисел.

Если какое-нибудь число A, не являющееся единицей, не имеет делителей кроме самого себя и четырех единиц, то оно называется простым в области целых комплексных чисел.

Примечание. Совокупность обыкновенных целых чисел входит как часть в состав совокупности целых комплексных чисел. Поэтому, если какое-нибудь обыкновенное целое число является простым даже в области комплексных чисел, то оно является также простым и в области обыкновенных целых чисел. Обратное же не верно. Например, 5 есть простое число в области обыкновенных целых чисел, но разлагается на два множителя в области целых комплексных чисел:

$$5=(1+2i)(1-2i).$$

Вопрос о том, какие из обыкновенных простых чисел остаются простыми в области комплексных чисел и какие нет, весьма интересен и будет в дальнейшем разобран.

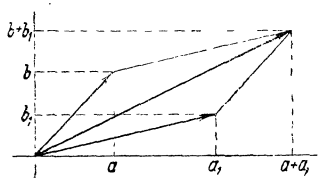
Геометрическое изображение комплексных чисел.

Комплексные числа $a+bi$ изображают геометрически, пользуясь прямоугольной системой координат, вектором, начало которого совпадает с началом координат, а конец находится в точке с координатами (a, b).

Как легко видеть, сумме двух комплексных чисел A и A_1 соответствует вектор, являющийся геометрической суммой векторов, соответствующих A и A_1, т. е. являющийся диагональю параллелограма, построенного на векторах A и A_1 (см. черт. 1).

Длина вектора, соответствующего комплексному числу $A=a+bi$, равная $\sqrt{a^2+b^2}$, носит название модуля комплекс-

ного числа A. Квадрат модуля целого комплексного числа есть вещественное положительное целое число. Модуль числа A обозначается через $|A|$.



Черт. 1.

Модуль каждой из единиц равен 1. Модуль каждого целого комплексного числа, не являющегося единицей, больше 1.

Нетрудно доказать перемножением, что модуль произведения двух чисел равен произведению модулей сомножителей. Алгебраически это выражается тождеством $(a^2+b^2)(c^2+d^2)=(ac-bd)^2+(ad+bc)^2$.

Из него следует, в частности, что модуль делителя целого комплексного числа меньше модуля этого числа, если только частное не есть единица.

Два комплексных числа $a+bi$ и $a-bi$, отличающиеся только знаком при мнимой части, называются сопряженными друг с другом. Из сопоставления равенств

$$(a+bi)\pm(c+di)=(a\pm c)+(b\pm d)i,$$
$$(a-bi)\pm(c-di)=(a\pm c)-(b\pm d)i$$

следует, что сумма и разность двух комплексных чисел, сопряженных с данными, есть комплексное число, сопряженное с суммой или разностью данных комплексных чисел.

Аналогично, равенства

$$(a+bi)(c+di)=(ac-bd)+(ad+bc)i,$$
$$(a-bi)(c-di)=(ac-bd)-(ad+bc)i$$

показывают, что произведение чисел, сопряженных с данными, есть число, сопряженное с произведением данных чисел.

Легко доказать аналогичное свойство частного: частное чисел, сопряженных с данными, сопряжено с частным данных чисел.

Следствие 1. Если в выражении $F(A, B, C, \ldots, K)$, составленном путем сложений, умножений, вычитаний и делений из комплексных чисел $A, B, C, \ldots, K$, заменим все числа $A, B, C, \ldots, K$ их сопряженными, то и $F(A, B, C, \ldots, K)$ перейдет в сопряженное.

Доказательство этого предложения, проводимое путем индукции, предоставляется провести читателю.

Следствие 2. Если вещественное целое число n делится на комплексное $a+bi$, то n делится также и на $a-bi$.

В самом деле, из равенства $n=n+0\cdot i=(a+bi)(c+di)$ следует $n=n-0\cdot i=(a-bi)(c-di)$.

Разложение целых комплексных чисел на простые множители.

Теорема. *Всякое целое комплексное число разлагается на простые множители.*

Доказательство этой теоремы аналогично доказательству соответственной теоремы для целых вещественных чисел. Если комплексное число A само не простое, то оно должно иметь множитель A_1 меньшего модуля. Если теперь предположить, что для всех чисел, модули которых не превосходят $\sqrt{n}$, теорема доказана, то отсюда получится, что для чисел модуля $\sqrt{n}+1$ она тоже окажется справедливой. Сложнее доказать, что в области целых комплексных чисел имеет место также и единственность разложения на простые множители (если отвлечься от порядка сомножителей и от возможности комбинировать эти множители с четырьмя единицами).

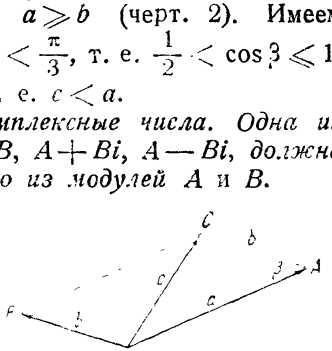
Для доказательства этого предложения нам придется ввести процесс, аналогичный алгорифму Эвклида, и показать, что для двух целых комплексных чисел A и B существует общий наибольший делитель, т. е. такой их общий делитель D, что всякий другой общий делитель чисел A и B входит множителем в D.

Лемма 1. *Если имеем два вектора в плоскости A и B, образующие угол, заключенный между $\frac{2\pi}{3}$ и π (причем π не исключается), то их сумма по модулю меньше, чем наибольший из модулей A и B.*

Доказательство. Пусть модуль A есть a, модуль B есть b, модуль $A+B$ есть c, и $a \geqslant b$ (черт. 2). Имеем $c^2 = a^2 + b^2 - 2ab\cos\beta$, где $0 \leqslant \beta < \frac{\pi}{3}$, т. е. $\frac{1}{2} < \cos\beta \leqslant 1$. Значит, $c^2 < a^2 + b^2 - ab \leqslant a^2$, т. е. $c < a$.

Лемма 2. *Пусть A и B — комплексные числа. Одна из четырех комбинаций $A+B$, $A-B$, $A+Bi$, $A-Bi$, должна быть по модулю меньше наибольшего из модулей A и B.*

Доказательство. Векторы, соответствующие числам B, $-B$, Bi, $-Bi$, образуют между собой четыре прямых угла и равны по величине. Они не могут все четыре образовывать с A углы, меньшие $\frac{2\pi}{3}$. Поэтому хотя бы один из них должен (согласно предыдущей лемме) в сумме с A давать вектор меньшей длины, чем наибольший из A и B.



Черт. 2.

Пусть имеем целые комплексные числа A и B. Докажем, что у них имеется общий наибольший делитель, т. е. такой их общий делитель, что всякий другой общий делитель чисел A и B входит в него множителем.

Если $A = \varepsilon B$, где ε — одна из четырех единиц $1, -1, i, -i$, то общим наибольшим делителем чисел A и B будет любое из них.

Пусть $A \neq \varepsilon B$ ($\varepsilon = 1, -1, i, -i$). По лемме 2 одна из четырех комбинаций $A + B$, $A - B$, $A + Bi$, $A - Bi$ имеет модуль, меньший, чем наибольший из модулей $|A|$ и $|B|$. Пусть это будет $A_1 = A + \varepsilon B$.

Из соотношений $A_1 = A + \varepsilon B$ и $A = A_1 - \varepsilon B$ вытекает, что всякий общий делитель A и B есть также общий делитель A_1 и $B_1 = B$, и, обратно, всякий общий делитель A_1 и $B_1 = B$ есть также общий делитель A и B. Если $A_1 = \varepsilon_1 B_1$, где ε_1 — единица, то общим наибольшим делителем A и B будет, очевидно, любое из чисел A_1, B_1. Если же $A_1 \neq \varepsilon_1 B_1$ ($\varepsilon_1 = 1, -1, i, -i$), то тем же путем, что и раньше, образуем новую пару чисел A_2, B_2, которые попрежнему будут иметь те же общие делители, что и A, B; однако наибольший из их модулей будет уже меньше наибольшего из модулей $|A|$, $|B|$.

Продолжая этот процесс, получим последовательность пар комплексных чисел A_i, B_i, имеющих те же общие делители, что и A, B, причем не более чем через каждые два шага процесса будет происходить понижение наибольшего из модулей этих чисел.

Ввиду невозможности бесконечного уменьшения модулей целых комплексных чисел (квадраты этих модулей являются, ведь, обыкновенными целыми числами), через конечное число шагов процесс закончится, т. е. одно из A_i окажется равным соответственному B_i, умноженному на одну из четырех единиц. Общим наибольшим делителем D чисел A_i, B_i (а следовательно и A, B) будет тогда любое из чисел A_i, B_i.

Ввиду наличия зависимостей $A_1 = A - \varepsilon B$. $B_1 = B$ и аналогичных зависимостей для каждой следующей пары, A_i и B_i, а значит, и D выражаются через A и B в виде

$$D = MA + NB, \qquad (*)$$

где M и N — целые комплексные числа. Из выражения (*) для D так же, как и в случае обыкновенных целых чисел, непосредственно следуют основные теоремы делимости:

Если произведение AB целых комплексных чисел делится на целое комплексное C и B взаимно просто с C, то A делится на C, и отсюда:

Если произведение AB делится на простое комплексное число P, то по крайней мере один из сомножителей делится на P.

Из этих теорем делимости следует так же, как и для обыкновенных целых чисел, теорема о единственности разложения целого комплексного числа на простые множители.

Следствия.

а) Если вещественное целое n делится на комплексное число $a+bi$ со взаимно простыми a и b, то n делится на a^2+b^2.

Доказательство. Прежде всего заметим, что целое комплексное число $x+yi$ делится на $1+i$ [и значит также на $1-i=-i(1+i)$] тогда и только тогда, когда x и y — числа одинаковой четности, т. е. или оба четные, или оба нечетные. В самом деле,

$$x+yi=(1+i)\left(\frac{y+x}{2}+\frac{y-x}{2}i\right),$$

и второй множитель в правой части является целым тогда и только тогда, когда x и y одинаковой четности.

По условию a и b взаимно просты и, значит, во всяком случае не могут быть оба четными.

1-й случай: a и b разной четности.

Имеем $n=(a+bi)(c+di)$, где $c+di$ — целое комплексное число. Вместе с тем, как мы видели выше (следствие 2, стр. 24), n должно делиться также на $a-bi$. Но $a+bi$ и $a-bi$ взаимно просты. В самом деле, если бы они имели общего простого делителя $p+qi$, то он входил бы также в их сумму $2a$ и в их разность $2bi$. В 2 он входить не мог бы, ибо разложение числа 2 на простые множители есть $2=(1+i)(1-i)$, и в силу разной четности чисел a и b $a\pm bi$ не делится на $1\pm i$. Таким образом $p+qi$ должен был бы входить в a и b. Но a и b — взаимно простые в области обыкновенных целых чисел; значит, как мы видели при изложении алгорифма Эвклида, существуют такие два целых числа x и y, что $ax-by=1$. Но тогда $p+qi$, деля a и b, должно было бы делить и 1, что абсурдно.

Итак, $a+bi$ и $a-bi$ в рассматриваемом случае взаимно просты, а так как $n=(a+bi)(c+di)$ делится на $a-bi$, то второй множитель $c+di$ должен делиться на $a-bi$, т. е. n делится на $(a+bi)(a-bi)=a^2+b^2$.

2-й случай: a и b оба нечетны.

Имеем

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

$$a-bi=(1-i)\left(\frac{b+a}{2}-\frac{b-a}{2}i\right).$$

Числа $\frac{b+a}{2}$ и $\frac{b-a}{2}$ взаимно просты, ибо иначе их сумма b и разность a не были бы взаимно простыми. С другой стороны, $\frac{b+a}{2}$ и $\frac{b-a}{2}$ разной четности, потому что они дают в сумме нечетное число b. Так как n делится на $\frac{b+a}{2}+\frac{b-a}{2}i$, то в силу доказанного в 1-м случае заключаем, что n делится также на $\left(\frac{b+a}{2}\right)^2+\left(\frac{b-a}{2}\right)^2=\frac{a^2+b^2}{2}$. Последнее число, как легко видеть, нечетно. Число же n четно, ибо оно делится на $1+i$ и на $1-i$; значит, n^2 делится на $(1+i)(1-i)=2$. Поэтому n делится также на $2\cdot\frac{a^2+b^2}{2}=a^2+b^2$, и наше утверждение полностью доказано.

б) Если число вида a^2+b^2, где a и b — вещественные целые взаимно простые числа, делится на вещественное простое число p, то p не может быть простым в области целых комплексных чисел.

В самом деле, $a^2+b^2=(a+bi)(a-bi)$. Если бы p было простым в области целых комплексных чисел, то либо $a+bi$, либо $a-bi$ делилось бы на p, т. е. либо $\frac{a}{p}+\frac{b}{p}i$, либо $\frac{a}{p}-\frac{b}{p}i$ было бы целым. Но это невозможно ввиду взаимной простоты чисел a и b.

в) В § 2 (см. следствие 1, стр. 21) было доказано, что всякое простое (в области обыкновенных целых чисел) число вида $4n+1$ есть делитель числа вида x^2+1. Отсюда в силу предыдущего замечания следует, что подобное число разлагается в комплексной области на множители. Пусть $a+bi$ — простой множитель числа $p=4n+1$, простого в области обыкновенных целых чисел. Тогда в силу следствия а) p делится на a^2+b^2, а так как p — простое, то $p=a^2+b^2$. Мы получили, таким образом, что всякое простое число вида $4n+1$ может быть представлено в виде суммы двух квадратов целых вещественных чисел:

$$p=a^2+b^2.$$

Посмотрим, сколько может быть подобных разложений простого числа p на два квадрата. Пусть

$$p = a^2 + b^2 = a_1^2 + b_1^2.$$

Имеем:

$$p = (a + bi)(a - bi) = (a_1 + b_1 i)(a_1 - b_1 i).$$

На основании единственности разложения на простые множители заключаем, что $a + bi$ должно отличаться от $a_1 + b_1 i$ или $a_1 - b_1 i$ только множителем ± 1 или $\pm i$. Перебирая все эти возможности, получаем восемь разложений

$$p = a^2 + b^2 = (-a)^2 + (-b)^2 = b^2 + a^2 = (-b)^2 + (-a)^2 =$$
$$= (-a)^2 + b^2 = a^2 + (-b)^2 = (-b)^2 + a^2 = b^2 + (-a)^2.$$

Отсюда видно, что, если отвлечься от знаков чисел a, b и порядка слагаемых, то разложение простого числа p вида $4n+1$ на сумму двух квадратов возможно единственным способом.

Сопоставляя полученный результат с очевидным фактом, что никакие целые числа вида $4n+3$ не могут быть суммами двух квадратов целых чисел, получаем следующую теорему:

Простое число p вида $4n+1$ разлагается на сумму двух квадратов и притом единственным образом; простое число вида $4n+3$ не разлагается на сумму двух квадратов.

§ 4. Арифметика чисел вида $a + b\rho$, где ρ есть кубический корень из единицы.

Пусть

$$\rho = -\frac{1}{2} + \frac{1}{2} i\sqrt{3}, \quad \text{где} \quad i = \sqrt{-1}.$$

Тогда

$$\rho^2 = -\frac{1}{2} - \frac{1}{2}\sqrt{-3} = -\rho - 1, \quad \rho^3 = 1.$$

Числа 1, ρ, ρ^2 суть три корня уравнения $x^3 = 1$.

Мы будем в этом параграфе называть целыми числа вида $a + b\rho$, где a и b — целые рациональные числа.

Сумма и разность целых чисел есть, очевидно, целое число. Произведение целых чисел

$$(a + b\rho)(a_1 + b_1\rho) = aa_1 + (ab_1 + ba_1)\rho + bb_1\rho^2 =$$
$$= (aa_1 - bb_1) + (ab_1 + ba_1 - bb_1)\rho$$

есть также целое число. Для частного двух целых чисел имеем выражение

$$\frac{a + b\rho}{a_1 + b_1\rho} = \frac{(a + b\rho)(a_1 + b_1\rho^2)}{(a_1 + b_1\rho)(a_1 + b_1\rho^2)} = A + B\rho,$$

где

$$A = \frac{aa_1 + bb_1}{a_1^2 - a_1b_1 - b_1^2}, \quad B = \frac{ba_1 - ab_1}{a_1^2 - a_1b_1 + b_1^2}.$$

Это выражение показывает, что частное двух целых чисел может уже не быть целым числом. В случае, когда частное от деления $a + b\rho$ на $a_1 + b_1\rho$ есть целое число (т. е. A и B — целые рациональные числа), мы будем говорить, что $a + b\rho$ делится на $a_1 + b_1\rho$.

Так же, как для целых рациональных чисел, вводится понятие сравнения: два целых числа $a + b\rho$ и $c + d\rho$ называются сравнимыми по модулю $m + n\rho$, если их разность делится на $m + n\rho$. Очевидно, и здесь сравнения можно складывать, вычитать и перемножать.

Если целые числа M и N делятся на целое число D, то, очевидно, все числа вида $MM_1 + NN_1$, где M_1 и N_1 — целые, тоже делятся на D.

Модуль целого числа $a + b\rho$ равен $\frac{1}{2}\sqrt{(2a-b)^2 + 3b^2}$, т. е. есть половина квадратного корня из целого рационального числа, и притом всегда число не меньшее 1, за исключением случая, когда $a = b = 0$. Поэтому, если мы имеем последовательность целых чисел с уменьшающимися модулями, то такая последовательность не может быть бесконечной.

Нетрудно видеть, что из всех чисел $a + b\rho$ модуль 1 имеют только числа ± 1, $\pm\rho$, $\pm\rho^2$. В самом деле, из

$$\frac{1}{2}\sqrt{(2a-b)^2 + 3b^2} = 1, \text{ т. е. } (2a-b)^2 + 3b^2 = 4$$

следует:

$$\text{или } 2a - b = \pm 2, \quad b = 0,$$
$$\text{или } 2a - b = \pm 1, \quad b = +1,$$
$$\text{или } 2a - b = \pm 1, \quad b = -1.$$

В первом случае $a + b\rho = \pm 1$,
во втором $a + b\rho$ есть или ρ, или $1 + \rho = -\rho^2$,
в третьем $a + b\rho$ есть или $-\rho$, или $-1 - \rho = \rho^2$.

Всякое целое делится на каждое из шести чисел ± 1, $\pm\rho$, $\pm\rho^2$. И обратно, если на какое-нибудь целое число d делится всякое целое число, то на него, в частности, должно делиться число 1, а значит его абсолютная величина должна быть равна 1, т. е. d должно совпадать с одним из шести указанных чисел.

Будем в дальнейшем числа ± 1, $\pm\rho$, $\pm\rho^2$ называть единицами. Два числа, отличающиеся множителем, являющимся одной из единиц, будем называть ассоциированными.

Аналогично тому, как для целых рациональных и целых комплексных чисел, введем для целых чисел, рассматриваемых в этом параграфе, понятие о простом числе, как таком, которое не имеет никаких делителей кроме себя самого и шести единиц и которое само не есть единица.

Буквально так же, как в случае целых рациональных и целых комплексных чисел, докажем и для новых целых чисел, что всякое целое число может быть представлено в виде произведения простых множителей.

Для новых целых чисел имеет место также и единственность разложения на простые множители. Для доказательства последнего можно поступать совершенно аналогично тому, как это было сделано для целых комплексных чисел.

Основываясь на лемме 1 предыдущего параграфа, легко докажем:

Если мы имеем два комплексных числа A и B ($|A| \geqslant |B|$), то из шести чисел $A \pm B$, $A \pm \rho B$, $A \pm \rho^2 B$ одно по крайней мере имеет модуль, меньший чем A.

В самом деле, шесть векторов $\pm B$, $\pm \rho B$ и $\pm \rho^2 B$ образуют между собой попарно углы в $\frac{\pi}{3}$. По крайней мере один из них образует с A угол, заключенный между $\frac{2\pi}{3}$ и π (возможно, равный π).

Из леммы 1 предыдущего параграфа непосредственно следует тогда наше утверждение.

Далее, буквально повторяя рассуждения предыдущего параграфа, докажем существование общего наибольшего делителя D любых двух целых чисел A и B и возможность отыскать такие целые числа X и Y, что

$$AX + BY = D.$$

Повторяя обычные рассуждения, выведем отсюда:

Если произведение AB делится на простое число P, то или A, или B делится на это простое число.

Из этого же предложения непосредственно получим, как в предыдущем параграфе:

Если имеем два разложения $p_1 p_2 \ldots p_r$ и $q_1 q_2 \ldots q_s$ одного и того же числа на простые множители, то число множителей в обоих разложениях одинаково и каждое p_i совпадает с некоторым q_j, и обратно, с точностью до множителя, являющегося одной из шести единиц; иными словами, каждое p_i ассоциировано с одним из q_j.

Это и есть единственность разложения рассматриваемых целых чисел на простые множители.

В качестве приложения этой теоремы докажем теорему Ферма для третьих степеней, т. е. докажем, что неопределенное уравнение

$$\bar{x}^3 + \bar{y}^3 = \bar{z}^3$$

не имеет решений в целых рациональных числах. Получится даже более сильное заключение, что этому уравнению нельзя удовлетворить не только целыми рациональными числами, но и более общими целыми числами, введенными в этом параграфе.

Заменяя $\bar{x}$, $\bar{y}$, $\bar{z}$ через x, y, $-z$, получим уравнение

$$x^3 + y^3 + z^3 = 0,$$

очевидно, равносильное данному.

Приступая к доказательству, прежде всего заметим, что если бы это уравнение имело целые решения x, y, z, то их можно было бы предположить, без ограничения общности, попарно взаимно простыми. Действительно, если бы, например, x и y имели общего наибольшего делителя a, то, очевидно, и z делилось бы на a, и три целых числа $\frac{x}{a}$, $\frac{y}{a}$, $\frac{z}{a}$ были бы тоже решениями, так как

$$\left(\frac{x}{a}\right)^3 + \left(\frac{y}{a}\right)^3 + \left(\frac{z}{a}\right)^3 = 0;$$

но при этом $\frac{x}{a}$, $\frac{y}{a}$, $\frac{z}{a}$ были бы уже попарно взаимно простыми.

Предварительные замечания.

Число 3 в области чисел $a + b\rho$ уже не является простым числом:

$$3 = (1 - \rho)(1 - \rho^2).$$

Так как $\rho^3 = 1$, то

$$1 - \rho^2 = -\rho^2(1 - \rho) \quad \text{и} \quad (1 - \rho)^2 = -3\rho.$$

Ввиду того что $-\rho$ и $-\rho^2$ суть единицы, числа $1 - \rho^2$ и $1 - \rho$ ассоциированы точно так же, как числа $(1 - \rho)^2$ и 3. Число $1 - \rho$ простое, так как если бы $1 - \rho$ разлагалось на множители $d_1 d_2$, где d_1 и d_2 — не единицы, то $1 - \rho^2$, будучи комплексно сопряженным с $1 - \rho$, разлагалось бы на комплексно сопряженные множители $\bar{d}_1 d_2$ и 3 было бы равно произведению $|d_1^2||d_2^2|$, т. е. произведению двух целых рациональных чисел, не равных 1, что невозможно, так как 3 — простое в области целых рациональных чисел.

Положим

$$d = 1 - \rho.$$

Покажем, что всякое целое число $a + b\rho$ сравнимо по модулю d с одним из трех чисел -1, 0, 1. Имеем:

$$a + b\rho = a + b - b(1 - \rho) = a + b - bd.$$

Следовательно, $a + b\rho \equiv a + b \pmod{d}$. $a + b$ — целое рациональное число и поэтому сравнимо по модулю 3 с одним из чисел -1, 0, $+1$. Пусть $a + b \equiv r \pmod 3$, где r есть -1, 0 или $+1$. Тогда, ввиду того что 3 делится на d, имеем $a + b \equiv r \pmod{d}$, а следовательно,

$$a + b\rho \equiv a + b \equiv r \pmod{d}.$$

Докажем, далее, следующее свойство числа d:

Лемма. *Если* $\xi \equiv +1 \pmod{d}$, *то* $\xi^3 \equiv +1 \pmod{d^4}$; *если* $\xi \equiv -1 \pmod{d}$, *то* $\xi^3 \equiv -1 \pmod{d^4}$.

В самом деле, если $\xi \equiv 1 \pmod{d}$, то $\xi = 1 + td$, где t — целое число, и отсюда следует, что

$$\xi^3 - 1 = (\xi - 1)(\xi - \rho)(\xi - \rho^2) = td(td + 1 - \rho)(td + 1 - \rho^2) =$$
$$= td^3(t + 1)(t - \rho^2).$$

Ввиду того, что $-\rho^2 \equiv -1 \pmod{d}$ и всякое целое число t должно быть сравнимо или с 0, или с 1, или с -1 по модулю d, один из множителей t, или $t + 1$, или $t - \rho^2$ делится на d. Поэтому все произведение делится на d^4, т. е. $\xi^3 - 1 \equiv 0 \pmod{d^4}$, и $\xi^3 \equiv 1 \pmod{d^4}$.

Аналогично докажем, что из сравнения $\xi \equiv -1 \pmod{d}$ вытекает $\xi^3 \equiv -1 \pmod{d^4}$.

Перейдем теперь непосредственно к доказательству теоремы.

Допустим, что существуют три числа x, y, z, попарно взаимно простые, удовлетворяющие уравнению

$$x^3 + y^3 + z^3 = 0.$$

Прежде всего заметим, что одно из x, y, z должно делиться на d.

Действительно, допустим, что все три числа x, y, z не делятся на d. Тогда каждое из них сравнимо или с $+1$, или с -1 по модулю d. Следовательно, согласно лемме, каждое из x^3, y^3, z^3 сравнимо или с $+1$, или с -1 по модулю d^4. Поэтому в случае справедливости нашего предположения мы имели бы $\pm 1 \pm 1 \pm 1 \equiv 0 \pmod{d^4}$. Но при всех комбинациях знаков мы получаем ± 1 или ± 3, и ни одно из этих чисел не может делиться на $d^4 = 9\rho^2$.

Мы видим, что одно из x, y, z делится на d. Пусть, например, z делится на d. Тогда z можно представить в виде $z = z_1 d^n$, где n есть наибольшая степень d, на которую делится z, так что z_1 уже не делится на d. Следовательно, имеем равенство

$$x^3 + y^3 + d^{3n} z_1^3 = 0.$$

Мы докажем, что такое равенство невозможно, и даже невозможно равенство

$$x^3 + y^3 + \varepsilon d^{3n} z_1^3 = 0, \qquad (1)$$

где ε — какая-нибудь из шести единиц.

Для доказательства невозможности этого равенства мы, с одной стороны, установим, что если бы подобное равенство имело место, то n было бы не менее 2. С другой стороны, мы покажем, что имея равенство (1) с показателем $3n$ при d, можем построить аналогичное равенство с показателем $3(n-1)$ вместо $3n$. Полученное противоречие и докажет наше утверждение.

1. Для того чтобы показать, что $n \geqslant 2$, допустим, что

$$-\varepsilon d^{3n} z_1^3 \equiv x^3 + y^3 \equiv \pm 1 \pm 1 \pmod{d^4}.$$

Так как комбинации $+1+1$ и $-1-1$ дают ± 2, т. е. число, не делящееся на $d^2 = -3\rho$, то годится только комбинация $+1-1$, дающая 0.

Итак,

$$-\varepsilon d^{3n} z_1^3 \equiv 0 \pmod{d^4}.$$

Ввиду того что $-\varepsilon z_1^3$ не делится на d, получаем

$$d^{3n} \equiv 0 \pmod{d^4},$$

т. е. $3n \geqslant 4$, откуда $n > 2$, ибо n — целое.

2. Для того чтобы показать, что можно понизить показатель $3n$ до $3(n-1)$, заметим, что

$$1 \equiv \rho \equiv \rho^2 \pmod{d},$$

следовательно,

$$x + y \equiv x + \rho y \equiv x + \rho^2 y \pmod{d}.$$

Из предположенного равенства

$$-\varepsilon d^{3n} z_1^3 = x^3 + y^3 = (x+y)(x+\rho y)(x+\rho^2 y)$$

следует, что по крайней мере один, а следовательно, и каждый из трех множителей правой части делится на d. Поэтому $\frac{x+y}{d}$, $\frac{x+\rho y}{d}$, $\frac{x+\rho^2 y}{d}$ суть целые числа.

Имеем равенство

$$-\varepsilon d^{3n-1}z_1^3 = \frac{x+y}{d}\cdot\frac{x+\rho y}{d}\cdot\frac{x+\rho^2 y}{d},$$

причем в правой части все множители целые. Ввиду того что левая часть делится на d (ибо по доказанному выше $n \geqslant 2$), по крайней мере один из сомножителей правой части должен делиться на d. Два сомножителя правой части уже не могут делиться на d ввиду того, что их попарные разности суть

$$\frac{(1-\rho)y}{d},\quad \frac{(1-\rho^2)y}{d},\quad \frac{(1-\rho)\rho y}{d},\ \text{т. е. } y,\ (1+\rho)y,\ \rho y,$$

и не делятся на d.

Предположим, что на d делится множитель $\frac{x+y}{d}$. (Если бы на d делился множитель $\frac{x+\rho y}{d}$ или $\frac{x+\rho^2 y}{d}$, то посредством подстановки $\rho y = y_1$ или $\rho^2 y = y_1$ мы пришли бы к указанному случаю.) Так как остальные два множителя не делятся на d, то d входит в $\frac{x+y}{d}$ в степени $3(n-1)$, поэтому

$$x+y = \varepsilon_1 d^{3n-3}X_1,\quad x+\rho y = dX_2,\quad x+\rho^2 y = dX_3, \qquad (а)$$

и мы получаем равенство

$$-\varepsilon z_1^3 = X_1X_2X_3. \qquad (б)$$

X_1, X_2, X_3 уже не могут иметь общих делителей (не считая единиц). В самом деле, всякий общий делитель r пары из этих чисел был бы делителем одной из разностей $(1-\rho)y$, $(1-\rho^2)y$, $\rho(1-\rho)y$, следовательно, делителем dy, так как все эти три разности ассоциированы с dy. Следовательно, r должен был бы быть делителем y, так как X_2 и X_3 не делятся на d. На основании равенств (а) x должен был бы тогда тоже делиться на r. Но x и y взаимно просты, поэтому r может быть только одной из шести единиц.

Из равенства (б) следует, ввиду взаимной простоты чисел X_1, X_2, X_3 и того, что $-\varepsilon$ есть единица, что каждое из чисел X_1, X_2, X_3 в отдельности ассоциировано кубу целого числа. Поэтому можно положить

$$x+y = \varepsilon_1 d^{3n-3}\mu^3,\quad x+\rho y = \varepsilon_2 d\nu^3,\quad x+\rho^2 y = \varepsilon_3 d\sigma^3, \qquad (в)$$

где ε_1, ε_2, ε_3 — единицы, а μ, ν, σ — целые числа. При этом μ, ν, σ попарно взаимно простые и ни одно из них не делится на d.

Из (в) следует:

$$0 = (x + y) + \rho(x + \rho y) + \rho^2(x + \rho^2 y) =$$
$$= \varepsilon_1 d^{3n-2}\mu^3 + \rho\varepsilon_2 d\nu^3 + \rho^2\varepsilon_3 d\sigma^3,$$

т. е.

$$\nu^3 + \rho\frac{\varepsilon_3}{\varepsilon_2}\sigma^3 + \rho^2\frac{\varepsilon_1}{\varepsilon_2}d^{3n-3}\mu^3 = 0,$$

причем $\frac{\varepsilon_3}{\varepsilon_2}\rho = \varepsilon_4$ и $\frac{\varepsilon_1}{\varepsilon_2}\rho^2 = \varepsilon_5$ суть единицы.

Докажем, что ε_4 есть $+1$ или -1, а не $\pm\rho$ или $\pm\rho^2$. В самом деле, как мы видели выше, каждое целое число сравнимо с $+1$, 0 или -1 по модулю d. Значит, числа ν и σ, не делясь на d, сравнимы с ± 1 по модулю d. Поэтому из соотношения

$$\nu^3 + \varepsilon_4\sigma^3 \equiv 0 \pmod{d^3}$$

следует (на основании леммы), что

$$\pm 1 + \varepsilon_4 \equiv 0 \pmod{d^3},$$

а последнее соотношение было бы невозможно, если бы ε_4 совпадало с $\pm\rho$ или $\pm\rho^2$.

Таким образом или

$$\nu^3 + \sigma^3 + \varepsilon_5 d^{3(n-1)}\mu^3 = 0, \quad \text{или} \quad \nu^3 + (-\sigma)^3 + \varepsilon_5 d^{3(n-1)}\mu^3 = 0,$$

т. е. получается соотношение вида (1) при показателе $3(n-1)$ вместо $3n$. Так как мы можем продолжать это снижение показателя до тех пор, пока n не станет равным 1, то получилось противоречие с доказанным ранее неравенством $n \geqslant 2$. Это и доказывает невозможность равенства вида (1), а вместе с тем теорему Ферма для случая третьих степеней.

Доказательство теоремы Ферма в общем случае (для n-х степеней) аналогичными методами не проходит ввиду того, что там приходится иметь дело с числами, зависящими от корней высших степеней из единицы. Теория делимости для этих чисел очень сложна.

Для того чтобы сохранить для этих чисел теорему о единственности разложения на простые множители, приходится ввести в рассмотрение так называемые идеалы, что очень усложняет теорию. Куммер, введший эти понятия, доказал таким путем теорему Ферма для всех простых показателей, не превосходящих 100; однако общего доказательства ни ему, ни дальнейшим исследователям в этой области не удалось получить.

Замечание. Мы видели, что в области целых рациональных чисел, целых комплексных чисел и целых чисел вида

$a + b\rho$, где $\rho = \frac{-1+\sqrt{-3}}{2}$, имеет место теорема о разложимости единственным образом всякого числа на простые множители. В теории чисел играет важную роль изучение других видов чисел, например, чисел $a + b\sqrt{n}$, где a и b — любые целые рациональные числа, а n — какое-нибудь фиксированное положительное или отрицательное целое рациональное число. Для этих видов чисел единственность разложения на простые множители уже не всегда имеет место.

Рассмотрим, например, числа вида $a + b\sqrt{-6}$, где a и b — обычные целые числа. Нетрудно видеть, что числа 2 и 3 — простые в области этих чисел. В самом деле, пусть 2 делится на $a_1 + b_1\sqrt{-6}$, так что имеет место равенство

$$2 = (a_1 + b_1\sqrt{-6})(a_2 + b_2\sqrt{-6}) =$$

$$= (a_1a_2 - 6b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{-6}.$$

Отсюда

$$2 = a_1a_2 - 6b_1b_2 \quad \text{и} \quad a_1b_2 + b_1a_2 = 0.$$

Поэтому

$$2 = (a_1a_2 - 6b_1b_2) - (a_1b_2 + b_1a_2)\sqrt{-6} =$$

$$= (a_1 - b_1\sqrt{-6})(a_2 - b_2\sqrt{-6}),$$

и, значит,

$$4 = (a_1^2 + 6b_1^2)(a_2^2 + 6b_2^2).$$

Отсюда прежде всего следует, что $b_1 = b_2 = 0$. Значит, одно из чисел a_1, a_2 равно ± 2, а другое равно ± 1, т. е. никаких делителей, кроме себя и ± 1, число 2 в рассматриваемой области не имеет.

Точно так же, если

$$3 = (a_1 + b_1\sqrt{-6})(a_2 + b_2\sqrt{-6}),$$

то также

$$3 = (a_1 - b_1\sqrt{-6})(a_2 - b_2\sqrt{-6}),$$

и, значит,

$$9 = (a_1^2 + 6b_1^2)(a_2^2 + 6b_2^2).$$

Поэтому или $b_1 = 0$, или $b_2 = 0$.

Пусть, например, $b_1 = 0$ (нумерация чисел в нашем распоряжении). Тогда $9 = a_1^2(a_2^2 + 6b_2^2)$, $a_1 = \pm 3$, $a_2^2 + 6b_2^2 = 1$, т. е. $b_2 = 0$, $a_2 = \pm 1$, т. е. предположенное разложение числа 3 есть $3 = (\pm 3)(\pm 1)$.

Число $\sqrt{-6}$ также неразложимо в нашей области. В самом деле, если

$$\sqrt{-6} = (a_1 + b_1\sqrt{-6})(a_2 + b_2\sqrt{-6}),$$

то, как легко видеть,

$$-\sqrt{-6} = (a_1 - b_1\sqrt{-6})(a_2 - b_2\sqrt{-6}),$$

и следовательно,

$$6 = (a_1^2 + 6b_1^2)(a_2^2 + 6b_2^2).$$

Отсюда один из множителей в правой части равен 1, а другой равен 6. Пусть, например, второй множитель равен 1, тогда $a_1 = 0$, $b_1 = \pm 1$, $a_2 = \pm 1$, $b_2 = 0$, т. е. предположенное разложение числа $\sqrt{-6}$ есть $\sqrt{-6} = (\pm 1)(\pm\sqrt{-6})$.

Из равенства $6 = 2 \cdot 3 = -\sqrt{-6}\sqrt{-6}$ мы видим, что число 6 разлагается двумя разными способами на простые (в рассматриваемой области) множители.

Для исследования законов делимости в подобных числовых областях эти области дополняются так называемыми идеалами, после чего в пополненных областях снова получается единственность разложения на множители.

Изучение подобных числовых областей является предметом так называемой алгебраической теории чисел, являющейся одной из наиболее замечательных частей теории чисел. Между прочим, решение неопределенных уравнений получает прочный фундамент именно в этих исследованиях. В частности, с изучением делимости в области некоторых классов алгебраических чисел, как уже было указано ранее, связаны работы, относящиеся к теореме Ферма.

§ 5. Разложение целых чисел на сумму четырех квадратов.

Рассмотрим числа новой природы, а именно числа вида $a + bi + cj + dk$, где a, b, c, d — вещественные числа, а i, j, k — новые символы. Два числа $a + bi + cj + dk$ и $a_1 + b_1 i + c_1 j + d_1 k$ будем считать равными между собой тогда и только тогда, когда $a = a_1$, $b = b_1$, $c = c_1$ и $d = d_1$. Будем называть суммой чисел $a + bi + cj + dk$ и $a_1 + b_1 i + c_1 j + d_1 k$ число

$$(a + a_1) + (b + b_1) i + (c + c_1) j + (d + d_1) k.$$

Введем, кроме того, действие над новыми числами, которое назовем умножением и определим следующим образом.

Прежде всего условимся считать произведения вещественного числа a на i, j, k равными, соответственно, ai, aj, ak.

Затем будем по определению считать

$$i^2 = j^2 = k^2 = -1,\ ij = k,\ jk = i,\ ki = j,$$

$$ji = -k,\ kj = -i,\ ik = -j.$$

Мы видим, что умножение новых чисел не обладает переместительным свойством.

Далее, по определению положим, что для умножения новых чисел справедлив распределительный закон: чтобы умножить сумму на какое-нибудь число, достаточно умножить на это число каждое слагаемое отдельно (но при этом не меняя порядка сомножителей). На основании этого определения и таблицы умножения для основных чисел i, j, k получим:

$$(a + bi + cj + dk)(a_1 + b_1 i + c_1 j + d_1 k) =$$
$$= (aa_1 - bb_1 - cc_1 - dd_1) + (ab_1 + ba_1 + cd_1 - dc_1) i +$$
$$+ (ac_1 + ca_1 + db_1 - bd_1) j + (ad_1 + da_1 + bc_1 - cb_1) k. \quad (A)$$

Можно было бы убедиться в том, что данные определения логически законны и что умножение новых чисел обладает следующими свойствами:

1) $A(BC) = (AB)C$ (сочетательное свойство),

2) $A(B + C) = AB + AC$, $(B + A)C = BA + CA$ (распределительное свойство),

3) если $AB = 0$, то или $A = 0$, или $B = 0$.

Однако, AB и BA, вообще говоря, не равны между собой. Но если один из сомножителей есть обыкновенное число, то переместительный закон имеет место.

Сложение же новых чисел обладает свойствами, совершенно похожими на свойства сложения обыкновенных вещественных или комплексных чисел.

Числа, определенные указанным образом, носят название кватернионов. Они были введены Гамильтоном и имеют разнообразные приложения.

Назовем сопряженными кватернионы

$$a + bi + cj + dk \quad \text{и} \quad a - bi - cj - dk.$$

Произведение двух сопряженных кватернионов, как легко вычислить, равно $a^2 + b^2 + c^2 + d^2$ и есть положительное вещественное число. Корень квадратный из этого числа носит название модуля кватерниона. Модуль кватерниона A будем обозначать через $|A|$.

Пусть A и B — два кватерниона, $\overline{A}$ и $\overline{B}$ — кватернионы, им сопряженные. Нетрудно убедиться в том, что кватернионы

AB и $\overline{B}\overline{A}$ сопряжены между собой. Поэтому

$$|AB|^2 = AB\overline{B}\overline{A}.$$

Но $B\overline{B} = |B|^2$ есть вещественное число. Поэтому мы имеем право изменить порядок сомножителей: $B\overline{B}\overline{A} = \overline{A}B\overline{B}$. Имеем тогда

$$|AB|^2 = AB\overline{B}\overline{A} = A\overline{A}B\overline{B} = |A|^2|B|^2.$$

Таким образом мы доказали, что модуль произведения двух кватернионов есть произведение модулей сомножителей.

Сопоставляя это свойство кватернионов с формулой для произведения двух кватернионов (беря $A = a + bi + cj + dk$, $B = a_1 - b_1 i - c_1 j - d_1 k$), получаем замечательное алгебраическое тождество:

$$\begin{aligned}(a^2 + b^2 + c^2 + d^2)(a_1^2 + b_1^2 + c_1^2 + d_1^2) = \\ = (aa_1 + bb_1 + cc_1 + dd_1)^2 + (-ab_1 + ba_1 - cd_1 + dc_1)^2 + \\ + (-ac_1 + ca_1 - db_1 + bd_1)^2 + (-ad_1 + da_1 - bc_1 + cb_1)^2. \quad \text{(B)}\end{aligned}$$

Разумеется, это тождество легко проверить чисто алгебраически, вовсе не основываясь на теории кватернионов. Оно было получено без помощи кватернионов еще Эйлером. Но именно в теории кватернионов это тождество приобретает наиболее естественное истолкование.

Можно ввести понятие о целом кватернионе, как о таком кватернионе $a + bi + cj + dk$, у которого a, b, c, d — обыкновенные целые рациональные числа, и развить теорию разложения целых кватернионов на простые множители. Эта теория приводит к замечательному выводу, что целые рациональные числа никогда не бывают простыми в области кватернионов. Всякое целое рациональное число n, как оказывается, разлагается всегда на произведение двух сопряженных целых кватернионов, так что

$$n = (a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2.$$

Таким образом всякое целое рациональное положительное число может быть представлено в виде суммы четырех квадратов целых чисел.

Эта замечательная теорема, впервые указанная Ферма (конечно, без связи с кватернионами), получается в теории разложения кватернионов на простые множители так же естественно, как теорема о представлении простого числа вида $4n + 1$ в виде суммы двух квадратов в теории гауссовых целых комплексных чисел.

Мы, однако, не имея возможности развить здесь подробную теорию кватернионов, приведем доказательство теоремы о разложении на сумму четырех квадратов, данное Лагранжем, не пользующееся теорией кватернионов. Мы ввели понятие о кватернионах только для той цели, чтобы подчеркнуть связь теоремы о четырех квадратах с вопросом о разложении на простые множители этих обобщенных целых чисел.

Теорема о четырех квадратах.

Теорема. *Всякое целое рациональное положительное число можно представить в виде суммы четырех квадратов целых рациональных чисел.*

Доказательство этой теоремы будет основываться на тождестве (B), которое, как уже было указано, может быть легко проверено алгебраически, без помощи кватернионов.

Лемма. *Каково бы ни было простое число $p > 2$, существует такое целое число $m < p$, что*

$$mp = a^2 + b^2 + c^2 + d^2.$$

Образуем числа вида x^2 и $-1-y^2$, где x и y пробегают значения $0, 1, \ldots, \frac{p-1}{2}$. Легко видеть, что никакие два x_1^2 и x_2^2 или $-1-y_1^2$ и $-1-y_2^2$ не могут быть сравнимы по модулю p. В самом деле, если бы

$$x_1^2 \equiv x_2^2 \pmod p \quad \text{или} \quad -1-y_1^2 \equiv -1-y_2^2 \pmod p,$$

то мы имели бы

$$(x_1+x_2)(x_1-x_2) \equiv 0 \pmod p \text{ или } (y_1-y_2)(y_1+y_2) \equiv 0 \pmod p,$$

что невозможно, ибо $x_1 \pm x_2$ и $y_1 \pm y_2$ меньше p.

Так как всех x^2 и $-1-y^2$ имеется $1+p$, а всех остатков по модулю p только p, то какое-нибудь x^2 должно дать тот же остаток по модулю p, что $-1-y^2$. Поэтому существуют x и y, удовлетворяющие сравнению $x^2 \equiv -1-y^2 \pmod p$, т. е. равенству $x^2+y^2+1 = pm$. Ввиду того что $x < \frac{p}{2}$, $y < \frac{p}{2}$, имеем $x^2+y^2+1 < \frac{p^2}{2}+1 < p^2$, т. е. $m < p$. Тем самым лемма доказана (в качестве четвертого слагаемого в левой части можно взять 0).

Теперь докажем, что всякое простое число p может быть представлено в виде $a^2+b^2+c^2+d^2$, где a, b, c, d — целые числа.

Для $p = 2$ это очевидно: $2 = 1^2 + 1^2 + 0^2 + 0^2$.

Пусть $p > 2$. Обозначим через m наименьшее целое число, обладающее тем свойством, что mp разлагается на сумму четырех квадратов целых чисел. Мы знаем на основании леммы, что $m < p$.

Наша цель — доказать, что $m = 1$.

Прежде всего m должно быть нечетным.

В самом деле, если бы $m = 2m_1$, то из равенства $mp = 2m_1 p = a^2 + b^2 + c^2 + d^2$ вытекало бы, что либо все a, b, c, d — четные, либо два из них четные, а два нечетные. Во втором случае можем предположить a и b четными, c и d нечетными. В обоих случаях $\frac{a+b}{2}$, $\frac{a-b}{2}$, $\frac{c+d}{2}$ и $\frac{c-d}{2}$ — целые числа, и мы имеем

$$m_1 p = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2,$$

т. е. $m_1 p = \frac{1}{2} mp$ уже разлагается на четыре целых квадрата вопреки предположению, что mp — наименьшее подобное кратное p.

Итак, m можно считать нечетным. Допустим, что $m > 1$. Обозначим через a_1, b_1, c_1, d_1 абсолютно наименьшие остатки от деления a, b, c, d на m, т. е. разности между числами a, b, c, d и ближайшими к ним кратными числа m; a_1, b_1, c_1, d_1 суть положительные или отрицательные числа, меньшие $\frac{m}{2}$.

Имеем

$$a_1^2 + b_1^2 + c_1^2 + d_1^2 \equiv a^2 + b^2 + c^2 + d^2 = mp \equiv 0 \pmod{m}.$$

Поэтому

$$a_1^2 + b_1^2 + c_1^2 + d_1^2 = nm.$$

Здесь $n \neq 0$, ибо иначе было бы $a_1 = b_1 = c_1 = d_1 = 0$, все a, b, c, d делились бы на m, а значит $a^2 + b^2 + c^2 + d^2 = mp$ делилось бы на m^2, т. е. p делилось бы на m, что невозможно, ибо p простое и $m < p$.

Ввиду того что $|a_1|$, $|b_1|$, $|c_1|$, $|d_1|$ меньше $\frac{m}{2}$, получаем $nm < 4\frac{m^2}{4}$, т. е. $n < m$.

Перемножая $a^2 + b^2 + c^2 + d^2$ и $a_1^2 + b_1^2 + c_1^2 + d_1^2$ и применяя формулу (B), получаем

$$m^2 np = (aa_1 + bb_1 + cc_1 + dd_1)^2 + (-ab_1 + ba_1 - cd_1 + dc_1)^2 + (-ac_1 + ca_1 - db_1 + bd_1)^2 + (-ad_1 + da_1 - bc_1 + cb_1)^2.$$

Замечая, что

$$a \equiv a_1, \quad b \equiv b_1, \quad c \equiv c_1, \quad d \equiv d_1$$

по модулю m, получаем:

$$aa_1 + bb_1 + cc_1 + dd_1 \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m},$$
$$-ab_1 + ba_1 - cd_1 + dc_1 \equiv -ab + ba - cd + dc \equiv 0 \pmod{m},$$

и аналогично остальные два выражения в скобках будут сравнимы с нулем по модулю m. Поэтому, обозначая через A, B, C, D выражения в скобках, имеем

$$np = \left(\frac{A}{m}\right)^2 + \left(\frac{B}{m}\right)^2 + \left(\frac{C}{m}\right)^2 + \left(\frac{D}{m}\right)^2,$$

причем $\frac{A}{m}$, $\frac{B}{m}$, $\frac{C}{m}$, $\frac{D}{m}$ — целые числа. Значит, np разлагается на сумму четырех квадратов, что, ввиду неравенства $n < m$, противоречит определению числа m. Таким образом мы пришли к противоречию с предположением о том, что минимальное число m, обладающее тем свойством, что mp разлагается на четыре квадрата, отлично от единицы, и тем самым доказали, что всякое простое p разлагается на четыре квадрата.

Теперь уже легко доказать общую теорему: всякое целое положительное число разлагается на сумму четырех квадратов.

В самом деле, всякое целое положительное число можно разложить в произведение простых чисел. А так как каждое простое число, согласно доказанному, представимо в виде суммы четырех квадратов, а произведение сумм четырех квадратов есть, согласно тождеству (B), тоже сумма четырех квадратов, то этим самым теорема доказана.

§ 6. Различные доказательства существования бесконечного множества простых чисел.

Факт наличия бесконечного множества простых чисел был нами уже доказан с помощью рассуждения Эвклида. Несмотря на простоту этого доказательства, мы считаем полезным остановиться подробнее на доказательствах бесконечности ряда простых чисел, чтобы на этом простом примере убедиться в существовании связей между свойствами простых чисел и вопросами математического анализа. Поэтому мы приведем несколько различных доказательств бесконечности числа простых чисел.

I. Доказательство, основанное на медленности роста логарифмической функции.

Предварительное замечание. Функция $\log_a x$ при любом основании $a > 1$ растет с возрастанием x, но рост любой степени $(\log_a x)^k$ меньше чем рост x; точно говоря, $\lim\limits_{x \to \infty} \frac{(\log_a x)^k}{x} = 0$, каково бы ни было постоянное число k.

Не ограничивая общности, можно считать k целым положительным.

Ввиду того что $\log_a x = \log_a 2 \cdot \log_2 x$, достаточно доказать это соотношение для логарифмов при основании 2. Обозначая ближайшее к $\log_2 x$ большее целое число через y, видим, что достаточно доказать соотношение

$$\lim_{y \to \infty} \frac{y^k}{2^y} = 0$$

при любом постоянном целом положительном k.

Формула бинома Ньютона дает

$$2^y = 1 + C_y^1 + C_y^2 + \ldots + C_y^{k+1} + \ldots + 1.$$

Следовательно,

$$\frac{2^y}{y^k} > \frac{C_y^{k+1}}{y^k} = \frac{y(y-1)\ldots(y-k)}{y^k}.$$

Так как в числителе стоит многочлен $(k+1)$-й степени относительно y, а в знаменателе стоит y^k, то $\lim\limits_{y \to \infty} \frac{C_y^{k+1}}{y^k} = \infty$. Отсюда $\lim\limits_{y \to \infty} \frac{y^k}{2^y} = 0$.

Допустим теперь, что простых чисел — конечное число. Тогда их можно расположить в порядке возрастания: $p_1 = 2$, $p_2 = 3$, ..., p_k (p_k — наибольшее простое число).

Возьмем какое-нибудь целое число x и составим таблицу

$$\begin{array}{l} 1,\ p_1,\ p_1^2,\ \ldots,\ p_1^{r_1}, \\ 1,\ p_2,\ p_2^2,\ \ldots,\ p_2^{r_2}, \\ \cdots\cdots\cdots\cdots \\ 1,\ p_k,\ p_k^2,\ \ldots,\ p_k^{r_k}, \end{array}$$

где в каждой строке написаны степени одного и того же простого числа, не превосходящие x. Число членов в этих строчках, как легко вычислить, не более чем соответственно $\log_{p_1} x$, $\log_{p_2} x$, ..., $\log_{p_k} x$. Все целые числа, не бо́льшие x, могут быть получены перемножением членов различных строчек.

поэтому число целых чисел, не превосходящих x, не может быть больше, чем число способов, которыми можно комбинировать между собой члены различных строчек, т. е. не больше произведения чисел членов всех строчек. Но оно в свою очередь не превосходит произведения $\log_{p_1} x \log_{p_2} x \dots \log_{p_k} x$. Так как все $p_i \geqslant 2$, то последнее произведение меньше, чем $(\log_2 x)^k$. Так как k здесь постоянное, то на основании предварительного замечания, при достаточно большом x, $(\log_2 x)^k$ сделается как угодно малым по сравнению с x. Получается, что число целых чисел, не превосходящих x, должно быть при достаточно большом x меньше, чем x. Но это абсурдно, ибо число целых чисел, не превосходящих целого x, равно, очевидно, x. Таким образом предположение, что число простых чисел конечно, привело к противоречию, и, значит, это предположение неверно.

II. Доказательство Эйлера бесконечности числа простых чисел.

Пусть число простых чисел конечно и равно k. Обозначим через $p_1, p_2, \dots, p_k$ все простые числа.

Составим геометрические прогрессии

$$1+\frac{1}{p_1}+\frac{1}{p_1^2}+\dots+\frac{1}{p_1^n}+\dots=\frac{1}{1-\frac{1}{p_1}},$$

$$1+\frac{1}{p_2}+\frac{1}{p_2^2}+\dots+\frac{1}{p_2^n}+\dots=\frac{1}{1-\frac{1}{p_2}},$$

$$\dots\dots\dots\dots\dots\dots\dots\dots$$

$$1+\frac{1}{p_k}+\frac{1}{p_k^2}+\dots+\frac{1}{p_k^n}+\dots=\frac{1}{1-\frac{1}{p_k}}.$$

Так как эти прогрессии суть сходящиеся ряды положительных чисел и их число конечно, то их можно почленно перемножать и должен получиться сходящийся ряд. Получим

$$\frac{1}{1-\frac{1}{p_1}}\,\frac{1}{1-\frac{1}{p_2}}\cdots\frac{1}{1-\frac{1}{p_k}}=\sum\frac{1}{p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}},$$

где суммирование распространено на все различные возможные комбинации неотрицательных показателей $\alpha_1, \alpha_2, \dots, \alpha_k$. Но всякое целое число разлагается в произведение степеней простых чисел $p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$ и притом единственным способом.

Следовательно, сумма, стоящая справа, объединяет все дроби вида $\frac{1}{n}$ при любых целых положительных n. Так как все члены в этой сумме положительны, то мы можем располагать их в любом порядке, например, по возрастающим знаменателям. Получим гармонический ряд $1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\ldots$ Из приведенного рассуждения, основанного на предположении о конечности числа простых чисел, вытекает, что этот ряд сходится и имеет сумму, равную произведению дробей $\frac{p_1}{p_1-1}\,\frac{p_2}{p_2-1}\cdots\frac{p_k}{p_k-1}$. Между тем гармонический ряд, как известно, расходится. Получилось противоречие, доказывающее неверность предположения о конечности числа простых чисел.

§ 7. Разложение $n!$ на простые множители и тождество Чебышева.

Разложим на простые множители произведение

$$1\cdot 2\cdot 3\ldots n=n!.$$

Очевидно, что в состав $n!$ входят только простые множители, не превосходящие n. Обозначим все простые числа, не превосходящие n, в порядке их возрастания через $p_1, p_2, \ldots, p_k$. $n!$ будет произведением некоторых степеней этих простых чисел.

Нетрудно видеть, что степень, в которой простое число p войдет в $n!$, равна числу чисел, не превосходящих n и делящихся на p, сложенному с числом чисел, не превосходящих n и делящихся на p^2, сложенному с числом чисел, не превосходящих n и делящихся на p^3, и т. д. В самом деле, числа, не превосходящие n, делящиеся на p, но не на p^2, вносят в степень p, входящую в $n!$, по единице (т. е. должны быть засчитаны по одному разу); числа, делящиеся на p^2, но не на p^3, — по двойке (т. е. должны быть засчитаны по два раза) и т. д.

Но каждое простое число p войдет в состав следующих целых чисел, не превосходящих n:

$$p,\quad 2p,\quad 3p,\quad \ldots,\quad \left[\frac{n}{p}\right]p,$$

где $\left[\frac{n}{p}\right]$ обозначает целую часть частного $\frac{n}{p}$.

Точно так же p^2 войдет в состав чисел

$$p^2,\quad 2p^2,\quad 3p^2,\quad \ldots,\quad \left[\frac{n}{p^2}\right]p,$$

p^3 войдет в состав чисел

$$p^3,\quad 2p^3,\quad 3p^3,\quad \ldots,\quad \left[\frac{n}{p^3}\right]p^3$$

и т. д.

Отсюда вытекает, что простое число p войдет в состав произведения $n! = 1 \cdot 2 \cdot 3 \ldots n$ в степени, равной

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\ldots+\left[\frac{n}{p^t}\right], \tag{1}$$

где p^t есть наибольшая целая степень p, не превосходящая n, т. е. $t = \left[\dfrac{\log n}{\log p}\right]$.

Обозначая выражение (1) через r_p, можно написать разложение $n!$ на простые множители в следующей форме:

$$n! = p_1^{r_{p_1}} p_2^{r_{p_2}} \ldots p_k^{r_{p_k}}. \tag{2}$$

Тождество Чебышева.

Обозначим через $\Omega(n)$ наименьшее кратное всех целых чисел, не превосходящих n, и посмотрим, как $\Omega(n)$ разлагается на простые множители. Очевидно, в состав $\Omega(n)$ войдут только простые множители, не превосходящие n. При этом простое число p войдет в $\Omega(n)$ в той наибольшей степени p^v, которая не превосходит n. Из неравенства $p^v \leqslant n$ находим, что $v = \left[\dfrac{\log n}{\log p}\right]$.

Образуем произведение $\Omega(n)\,\Omega\left(\frac{n}{2}\right)\Omega\left(\frac{n}{3}\right)\ldots$ и разложим его на простые множители. Простое число p войдет в это произведение в степени

$$\left[\frac{\log n}{\log p}\right]+\left[\frac{\log \frac{n}{2}}{\log p}\right]+\left[\frac{\log \frac{n}{3}}{\log p}\right]+\ldots \tag{3}$$

Докажем, что выражение (3) равно r_p. Для этого посмотрим, сколько имеется членов в (3), не меньших 1. Очевидно столько, сколько раз $\frac{n}{i} \geqslant p$, т. е. $\left[\frac{n}{p}\right]$. Далее, членов, не меньших 2, будет столько, сколько раз выполняется неравенство $\frac{n}{i} \geqslant p^2$, т. е. $\left[\frac{n}{p^2}\right]$. Вообще легко видеть, что членов в (3), не меньших, чем целое число j, будет $\left[\frac{n}{pj}\right]$. Выражение (3) равно поэтому

$$\left(\left[\frac{n}{p}\right]-\left[\frac{n}{p^2}\right]\right)+2\left(\left[\frac{n}{p^2}\right]-\left[\frac{n}{p^3}\right]\right)+3\left(\left[\frac{n}{p^3}\right]-\left[\frac{n}{p^4}\right]\right)+\ldots,$$

т. е. (3) равно (1).

Разложение произведения $\Omega(n)\,\Omega\left(\frac{n}{2}\right)\Omega\left(\frac{n}{3}\right)\ldots$ на простые множители можно, таким образом, написать в виде

$$\Omega(n)\,\Omega\left(\frac{n}{2}\right)\Omega\left(\frac{n}{3}\right)\ldots\Omega\left(\frac{n}{n}\right)=p_1^{r_{p_1}}p_2^{r_{p_2}}\ldots p_k^{r_{p_k}}. \qquad (4)$$

Сравнивая (2) и (4), получаем тождество

$$n!=\Omega(n)\,\Omega\left(\frac{n}{2}\right)\Omega\left(\frac{n}{3}\right)\ldots\Omega\left(\frac{n}{n}\right). \qquad (5)$$

Введем в рассмотрение функцию $\psi_a(n)=\log_a\Omega(n)$, где логарифм взят при каком-нибудь основании $a>1$. Логарифмируя равенство (5), получаем

$$\psi_a(n)+\psi_a\left(\frac{n}{2}\right)+\psi_a\left(\frac{n}{3}\right)+\ldots=\log_a n!. \qquad (6)$$

Функцию $\psi_a(n)$ можно связать с другой употребительной в теории простых чисел функцией.

Обозначим через $\vartheta_a(n)$ сумму логарифмов простых чисел, не превосходящих n. Легко доказать тождество

$$\psi_a(n)=\vartheta_a(n)+\vartheta_a(\sqrt{n})+\vartheta_a(\sqrt[3]{n})+\ldots \qquad (7)$$

В самом деле,

$$\psi_a(n)=\log_a\Omega(n)=\log_a\prod_{p_i\leqslant n}p_i^{\left[\frac{\log_a n}{\log_a p_i}\right]}=\sum\left[\frac{\log_a n}{\log_a p_i}\right]\log_a p_i.$$

С другой стороны, $\log_a p$ войдет в члены правой части (7), очевидно, столько раз, сколько раз выполняется неравенство $\sqrt[j]{n}\geqslant p$ или $\frac{\log_a n}{j}\geqslant\log_a p$, т. е. $\left[\frac{\log_a n}{\log_a p}\right]$ раз. Отсюда вытекает для суммы, стоящей в правой части (7), то же выражение $\sum\left[\frac{\log_a n}{\log_a p_i}\right]\log_a p_i$, что и для левой части (7).

§ 8. Грубые оценки для числа простых чисел, не превосходящих данного числа x.

Из тождества Чебышева

$$\psi_a(x)+\psi_a\left(\frac{x}{2}\right)+\psi_a\left(\frac{x}{3}\right)+\ldots=\log_a[x]!,$$

полагая $x=2n$, где n — целое число, получаем

$$\psi_a(2n)+\psi_a\left(\frac{2n}{2}\right)+\psi_a\left(\frac{2n}{3}\right)+\ldots=\log_a(2n)!. \qquad (1)$$

Далее, полагая $x = n$, имеем

$$\psi_a(n) + \psi_a\left(\frac{n}{2}\right) + \psi_a\left(\frac{n}{3}\right) + \ldots = \log_a n!. \tag{2}$$

Вычитая из (1) удвоенное (2), получаем

$$\psi_a(2n) - \psi_a\left(\frac{2n}{2}\right) + \psi_a\left(\frac{2n}{3}\right) - \ldots = \log_a \frac{(2n)!}{(n!)^2} = \log_a C_{2n}^n. \tag{3}$$

$\psi_a(x)$ есть неубывающая функция, принимающая положительные значения. Поэтому

$$\left.\begin{aligned} \psi_a(2n) - \psi_a(n) &< \log_a C_{2n}^n, \\ \psi_a(2n) &> \log_a C_{2n}^n. \end{aligned}\right\} \tag{4}$$

Докажем следующие неравенства:

$$\frac{4^n}{2n} < C_{2n}^n < 4^n. \tag{5}$$

C_{2n}^n есть средний коэфициент при разложении бинома в степень $2n$, поэтому $C_{2n}^n < (1+1)^{2n} = 4^n$. Далее,

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

$$= \frac{2n(2n-1)}{n^2} \cdot \frac{(2n-2)(2n-3)}{(n-1)^2} \cdots \frac{2\cdot 1}{1^2} =$$

$$= 4^n\left(1-\frac{1}{2n}\right)\left(1-\frac{1}{2(n-1)}\right)\ldots\left(1-\frac{1}{2}\right) =$$

$$= 4^n \frac{1}{2}\cdot\frac{3}{4}\cdot\frac{5}{6}\ldots\frac{2n-1}{2n} > 4^n \frac{1}{2}\cdot\frac{2}{3}\cdot\frac{3}{4}\ldots\frac{2n-1}{2n} = \frac{4^n}{2n}.$$

В силу неравенств (5) выводим из (4) неравенства

$$\left.\begin{aligned} \psi_2(2n) - \psi_2(n) &< \log_2 4^n = 2n, \\ \psi_2(2n) &> \log_2 4^n - \log_2 2n = 2n - \log_2 2n. \end{aligned}\right\} \tag{4'}$$

Определяя функцию $\psi_2(x)$ для всех вещественных x равенством $\psi_2(x) = \sum_{p \leqslant x} \left[\frac{\log_2 x}{\log_2 p}\right] \log_2 p$, мы легко получим из (4') неравенства для $\psi_2(x)$ при любом вещественном x. Действительно, пусть $2n$ есть наибольшее четное число, не превосходящее x. Тогда, как это вытекает из определения функций $\psi(x)$,

$$\psi_2(x) - \psi_2(2n) \leqslant \log_2 x.$$

Отсюда в соединении с (4′) следуют неравенства

$$\psi_2(x) - \psi_2\left(\frac{x}{2}\right) < x + \log_2 x,$$

$$\psi_2(x) > x - 2 - \log_2 x \geqslant x - 2\log_2 x,$$

причем в последнем неравенстве предполагается, что $x \geqslant 4$. Из первого неравенства выводим, заменяя x последовательно через $\frac{x}{2}$, $\frac{x}{4}$, $\frac{x}{8}$, ..., ряд неравенств

$$\psi_2(x) - \psi_2\left(\frac{x}{2}\right) < x + \log_2 x,$$

$$\psi_2\left(\frac{x}{2}\right) - \psi_2\left(\frac{x}{4}\right) < \frac{x}{2} + \log_2 \frac{x}{2},$$

$$\psi_2\left(\frac{x}{4}\right) - \psi_2\left(\frac{x}{8}\right) < \frac{x}{4} + \log_2 \frac{x}{4},$$

. . . . . .

Суммируя эти неравенства и принимая во внимание, что количество их не превышает $\log_2 x$, получим

$$\psi_2(x) < 2x + \log_2{}^2 x.$$

Таким образом

$$x - 2\log_2 x < \psi_2(x) < 2x + \log_2{}^2 x. \tag{6}$$

Обозначая через $\pi(x)$ число простых чисел, не превосходящих x, имеем

$$\psi_2(x) = \sum_{p \leqslant x} \left[\frac{\log_2 x}{\log_2 p}\right] \log_2 p \leqslant \sum_{p \leqslant x} \frac{\log_2 x}{\log_2 p} \log_2 p = \pi(x) \log_2 x.$$

В соединении с первым из неравенств (6) это дает

$$\pi(x) > \frac{x}{\log_2 x} - 2. \tag{7}$$

Далее, $\left[\pi(x) - \pi\left(\frac{x}{2}\right)\right] \log_2 \frac{x}{2} < \psi_2(x)$, так как если мы просуммируем только логарифмы простых чисел между $\frac{x}{2}$ и x, то получим сумму, меньшую $\psi(x)$, но бóльшую, чем число простых чисел между $\frac{x}{2}$ и x, умноженное на логарифм наименьшего из них.

Таким образом по второму из неравенств (6) имеем

$$\left[\pi(x) - \pi\left(\frac{x}{2}\right)\right] \log_2 \frac{x}{2} < 2x + \log_2{}^2 x, \tag{8a}$$

откуда также

$$\left[\pi\left(\frac{x}{2}\right)-\pi\left(\frac{x}{4}\right)\right]\log_2\frac{x}{4}<x+\log_2{}^2\frac{x}{2}, \tag{8б}$$

$$\left[\pi\left(\frac{x}{4}\right)-\pi\left(\frac{x}{8}\right)\right]\log_2\frac{x}{8}<\frac{x}{2}+\log_2{}^2\frac{x}{4}, \tag{8в}$$

. . . . . .

Складывая левые части неравенств (8а), (8б), (8в), ..., получаем

$$\pi(x)\log_2\frac{x}{2}-\pi\left(\frac{x}{2}\right)\left(\log_2\frac{x}{2}-\log_2\frac{x}{4}\right)-$$

$$-\pi\left(\frac{x}{4}\right)\left(\log_2\frac{x}{4}-\log_2\frac{x}{8}\right)-\ldots=$$

$$=\pi(x)\log_2 x-\pi(x)-\pi\left(\frac{x}{2}\right)-\pi\left(\frac{x}{4}\right)-\ldots>$$

$$>\pi(x)\log_2 x-x-\frac{x}{2}-\frac{x}{4}-\ldots=\pi(x)\log_2 x-2x.$$

Сумма правых частей неравенств (8а), (8б), (8в), ... будет меньше $4x+\log_2{}^3 x$, так как число неравенств не превосходит $\log_2 x$. Таким образом в итоге получаем $\pi(x)\log_2 x-2x<4x+\log_2{}^3 x$, откуда

$$\pi(x)<\frac{6x}{\log_2 x}+\log_2{}^2 x. \tag{9}$$

Неравенства (7) и (9) показывают, что число простых чисел, не превосходящих x, растет вместе с x со скоростью функции $\frac{x}{\log x}$.

§ 9. Доказательство постулата Бертрана.

В связи с некоторыми вопросами алгебры Бертран высказал предположение, что при любом $x>1$ между x и $2x$ всегда заключено простое число. Доказать это удалось впервые Чебышеву. В нижеследующем мы будем придерживаться несколько упрощенного доказательства постулата Бертрана, данного Рамануджаном.

Прежде всего, очевидно, можно предполагать x целым, ибо если простое число заключено между $[x]$ и $2[x]$, то оно заключено также между x и $2x$.

Для доказательства постулата Бертрана достаточно показать, что для всех целых x выполняется неравенство $\vartheta_2(2x)-\vartheta_2(x)>0$, где $\vartheta_2(x)$ — введенная в конце § 7 функция, обозначающая сумму логарифмов (при основании 2) простых

чисел, не превосходящих x. Действительно, разность $\vartheta_2(2x) - \vartheta_2(x)$ представляет собой сумму логарифмов простых чисел p, удовлетворяющих условию $x < p < 2x$, и потому эта разность будет положительна тогда и только тогда, когда хоть одно такое простое число существует.

Из соотношения (7) § 7, связывающего функции $\vartheta(x)$ и $\psi(x)$, заключаем, что

$$\psi_2(2x) - 2\psi_2(\sqrt{2x}) =$$

$$= \vartheta_2(2x) - \vartheta_2(\sqrt{2x}) + \vartheta_2(\sqrt[3]{2x}) - \vartheta_2(\sqrt[4]{2x}) + \ldots,$$

откуда

$$\vartheta_2(2x) \geqslant \psi_2(2x) - 2\psi_2(\sqrt{2x}). \qquad (1)$$

С другой стороны, из того же соотношения (7) § 7 непосредственно вытекает, что

$$\vartheta_2(x) \leqslant \psi_2(x). \qquad (2)$$

Далее, из равенства (3) § 8 заключаем, что

$$\psi_2(2x) - \psi_2(x) + \psi_2\left(\frac{2x}{3}\right) \geqslant \log_2 C_{2x}^{x}. \qquad (3)$$

Неравенства (1), (2), (3) в совокупности показывают, что

$$\vartheta_2(2x) - \vartheta_2(x) \geqslant \psi_2(2x) - \psi_2(x) - 2\psi_2(\sqrt{2x}) \geqslant$$

$$\geqslant \log_2 C_{2x}^{x} - \psi_2\left(\frac{2x}{3}\right) - 2\psi_2(\sqrt{2x}). \qquad (4)$$

Но в силу первого из неравенств (5) § 8

$$\log_2 C_{2x}^{x} > 2x - \log_2 2x. \qquad (5)$$

Далее, в силу второго из неравенств (6) § 8

$$\psi_2\left(\frac{2x}{3}\right) + 2\psi_2(\sqrt{2x}) <$$

$$< \frac{4x}{3} + 4\sqrt{2x} + \log_2^2 \frac{2x}{3} + 2\log_2^2 \sqrt{2x}. \qquad (6)$$

Принимая во внимание полученные только что неравенства (5) и (6), выводим из (4) неравенство

$$\vartheta_2(2x) - \vartheta_2(x) >$$

$$> \frac{2x}{3} - 4\sqrt{2x} - \log_2 2x - \log_2^2 \frac{2x}{3} - \frac{1}{2}\log_2^2 2x.$$

Но, как нетрудно проверить, выражение в правой части этого неравенства становится положительным при $x > 512$.

Поэтому $\vartheta_2(2x) - \vartheta_2(x) > 0$ при $x > 512$. Другими словами, при $x > 512$ между x и $2x$ заключено по меньшей мере одно простое число. Однако, таблица простых чисел показывает, что то же положение имеет место также для всех x, заключенных между 1 и 513. Это и завершает доказательство справедливости постулата Бертрана.

Примечание. Основываясь на неравенстве

$$\vartheta_2(x) - \vartheta_2\left(\frac{x}{2}\right) \leqslant \left[\pi(x) - \pi\left(\frac{x}{2}\right)\right] \log_2 x,$$

которым мы фактически уже пользовались в предыдущем параграфе, получим для числа простых чисел, заключенных между $\frac{x}{2}$ и x, оценку

$$\pi(x) - \pi\left(\frac{x}{2}\right) > \frac{1}{\log_2 x}\left(\frac{x}{3} - 4\sqrt{x}\right) - 1 - \frac{3}{2}\log_2 x.$$

Замечание. Вопрос о количестве $\pi(x)$ простых чисел, не превосходящих данного числа x, давно занимал математиков. Мы видели, что $\pi(x)$ возрастает со скоростью функции $\frac{x}{\log x}$. Более точный результат, полученный впервые Адамаром, заключается в том, что отношение $\pi(x)$ к $\frac{x}{\ln x}$ (где $\ln x$ означает натуральный логарифм x, т. е. логарифм при основании $e = \lim\limits_{n\to\infty}\left(1 + \frac{1}{n}\right)^n = 2{,}718281\ldots$) стремится к пределу, равному единице.

Более точным выражением для $\pi(x)$ является интеграл $\int\limits_2^x \frac{dt}{\ln t}$.

Исследование уклонений $\pi(x)$ от этого интеграла представляет большие трудности и до сих пор остается одной из интересных и трудных задач теории чисел.

§ 10. Асимптотические формулы Мертенса.

В дальнейшем мы будем пользоваться следующим обозначением: если функции $f(x)$ и $g(x)$ таковы, что отношение $\frac{f(x)}{g(x)}$ остается ограниченным по абсолютной величине, то мы будем писать $f(x) = O(g(x))$.

Например, $O(1)$ означает выражение, ограниченное по абсолютной величине.

В случае, если $\frac{f(x)}{g(x)} \to 0$ при $x \to \infty$, мы будем писать $f(x) = o(g(x))$, так что $o(1)$ означает величину, стремящуюся к нулю.

Теорема 1. *Если x стремится к бесконечности, то*

$$\sum_{p \leqslant x} \frac{\log p}{p} = \log x + O(1).$$

Доказательство. Из равенства $m! = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$, где $p_1, p_2, \dots, p_k$ суть простые числа, не превосходящие m, а

$$r_i = \left[\frac{m}{p_i}\right] + \left[\frac{m}{p_i^2}\right] + \dots + \left[\frac{m}{p_i^r}\right], \quad r = \left[\frac{\log m}{\log p_i}\right]$$

[см. формулу (2) § 7], получаем путем логарифмирования

$$\log m! = r_1 \log p_1 + r_2 \log p_2 + \dots + r_k \log p_k. \qquad (1)$$

На основании формулы Стирлинга

$$\log m! = m \log m + O(m).$$

Деля обе части равенства (1) на m, получаем

$$\log m + O(1) = \sum_{i=1}^{k} \frac{1}{m} \left\{ \left[\frac{m}{p_i}\right] + \left[\frac{m}{p_i^2}\right] + \dots \right\} \log p_i. \qquad (2)$$

Если всюду в правой части заменить выражения $\left[\frac{m}{p_i^k}\right]$ через $\frac{m}{p_i^k}$, то каждое слагаемое в фигурных скобках изменится не более чем на единицу (так как $|[a] - a| < 1$ при любом a), поэтому в каждом члене суммы ошибка будет не более чем

$$\frac{1}{m} \left[\frac{\log m}{\log p_i}\right] \log p_i \leqslant \frac{\log m}{m},$$

ошибка во всей сумме не превзойдет $k \frac{\log m}{m}$, и так как $k = O\left(\frac{m}{\log m}\right)$, то общая совершенная ошибка будет $O(1)$.

Если, далее, отбросить все члены вида $\frac{m}{p^2}$, $\frac{m}{p^3}$ и т. д., то общая сделанная ошибка не будет превосходить сумму

$$\sum_{p \leqslant x} \left(\frac{1}{p^2} + \frac{1}{p^3} + \dots\right) \log p < \sum_{n=2}^{\infty} \frac{\log n}{n(n-1)}.$$

Ряд справа, очевидно, сходящийся, так что эта часть ошибки не превзойдет постоянной величины.

Таким образом, если в равенстве (2) опустить знаки целых частей и отбросить все $\frac{m}{p^2}$, $\frac{m}{p^3}$ и т. д., то получится соотношение

$$\sum_{p \leqslant m} \frac{\log p}{p} = \log m + O(1).$$

Так как

$$\log x - \log [x] < \log ([x] + 1) - \log [x] = \log \frac{[x]+1}{[x]} \leqslant \log 2,$$

то и при любом вещественном x имеем

$$\sum_{p \leqslant x} \frac{\log p}{p} = \log x + O(1).$$

Теорема 2.

$$\sum_{p \leqslant x} \frac{1}{p} = \ln \ln x + B + O\left(\frac{1}{\ln x}\right),$$

где $\ln x$ *обозначает натуральный логарифм.*

В самом деле, положим

$$A(x) = \sum_{p_n \leqslant x} \frac{\ln p_n}{p_n} = \sum a_n \qquad \left(a_n = \frac{\ln p_n}{p_n}\right)$$

и

$$B(x) = \sum_{p_n \leqslant x} \frac{1}{p_n} = \sum b_n \qquad \left(b_n = \frac{1}{p_n}\right).$$

Пусть p_k — самое большое простое число, не превосходящее x ($x > 2$). Имеем

$$\begin{aligned}
B(x) &= \sum_{n=1}^{k} \frac{a_n}{\ln p_n} = \frac{a_1}{\ln p_1} + \sum_{n=2}^{k} \frac{A(p_n) - A(p_{n-1})}{\ln p_n} = \\
&= \sum_{n=1}^{k-1} A(p_n)\left(\frac{1}{\ln p_n} - \frac{1}{\ln p_{n+1}}\right) + \frac{A(p_k)}{\ln p_k} = \\
&= \sum_{n=1}^{k-1} A(p_n)\left(\frac{1}{\ln p_n} - \frac{1}{\ln p_{n+1}}\right) + A(p_k)\left(\frac{1}{\ln p_k} - \frac{1}{\ln x}\right) + \frac{A(x)}{\ln x} = \\
&= \sum_{n=1}^{k-1} A(p_n) \int_{p_n}^{p_{n+1}} \frac{dz}{z \ln^2 z} + A(p_k) \int_{p_k}^{x} \frac{dz}{z \ln^2 z} + \frac{A(x)}{\ln x} = \\
&= \int_{2}^{x} \frac{A(z)\,dz}{z \ln^2 z} + \frac{A(x)}{\ln x}.
\end{aligned}$$

Но в силу предыдущей теоремы $A(x) = \ln x + O(1)$, т. е. $A(x) = \ln x + r(x)$, где $|r(x)| < k$ (k — константа, не зависящая от x).

Поэтому, подставляя $\ln x + r(x)$ вместо $A(x)$, имеем

$$B(x) = \int_2^x \frac{dz}{z \ln z} + \int_2^x \frac{r(z)\,dz}{z \ln^2 z} + 1 + \frac{r(x)}{\ln x}.$$

Так как $|r(z)| < 1$, то интеграл $\int_2^\infty \frac{r(z)\,dz}{z \ln^2 z}$ сходится. Обозначая его сумму с $1 - \ln \ln 2$ через B, получаем

$$B(x) = \ln \ln x + B + R(x),$$

где

$$|R(x)| = \left| -\int_x^\infty \frac{r(z)\,dz}{z \ln^2 z} + \frac{r(x)}{\ln x} \right| < \int_x^\infty \frac{k\,dz}{z \ln^2 z} + \frac{k}{\ln x} = \frac{2k}{\ln x}.$$

Таким образом имеем

$$\sum_{p \leqslant x} \frac{1}{p} = \ln \ln x + B + O\left(\frac{1}{\ln x}\right).$$

Теорема 3.

$$\prod_{p \leqslant x} \left(1 - \frac{1}{p}\right) = \frac{e^{-C}}{\ln x}(1 + \varepsilon_x),$$

где C — константа („постоянная Эйлера"), а ε_x стремится к нулю при стремлении x к бесконечности.

Для доказательства этой теоремы мы введем в рассмотрение функцию

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \tag{3}$$

играющую фундаментальную роль в аналитической теории чисел.

Ряд в правой части формулы (3) сходится для всех $s > 1$. Докажем, что когда s, убывая, стремится к 1, то

$$(s-1)\zeta(s) \to 1. \tag{4}$$

В самом деле, так как, при фиксированном $s > 1$, $\frac{1}{x^s}$ есть убывающая функция от x, то

$$\frac{1}{s-1} = \int_1^\infty \frac{dx}{x^s} = \sum_{n=1}^{\infty} \int_n^{n+1} \frac{dx}{x^s} < \sum_{n=1}^{\infty} \frac{1}{n^s} < 1 + \sum_{n=2}^{\infty} \int_{n-1}^{n} \frac{dx}{x^s} = \frac{s}{s-1},$$

т. е.

$$\frac{1}{s-1} < \zeta(s) < \frac{s}{s-1}$$

или

$$1 < (s-1)\zeta(s) < s,$$

откуда и следует, что $(s-1)\zeta(s) \to 1$ при $s \to 1$.

Связь функции $\zeta(s)$ с простыми числами основывается на следующем представлении ее в виде „эйлерова произведения“:

$$\zeta(s) = \prod_{k=1}^{\infty} \frac{1}{1 - \frac{1}{p_k^s}} \tag{5}$$

(p_k пробегает все простые числа). Мы уже фактически встречались с этим произведением при изложении доказательства Эйлера бесконечности ряда простых чисел. Для проверки справедливости формулы (5) замечаем, что в правой ее части стоит произведение геометрических прогрессий $1 + \frac{1}{p_k^s} + \frac{1}{p_k^{2s}} + \dots$ ($k = 1, 2, \dots$). Так как эти прогрессии суть сходящиеся ряды положительных чисел, то их можно почленно перемножить (так что ряд, полученный в результате этого перемножения, будет сходящимся в случае, если произведение конечно, и расходящимся — в противном случае). Получим

$$\prod_{k=1}^{\infty} \frac{1}{1 - \frac{1}{p_k^s}} = \sum \frac{1}{(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m})^s},$$

где суммирование распространено на все различные возможные комбинации неотрицательных показателей $\alpha_1, \alpha_2, \dots, \alpha_m$, $m = 1, 2, \dots$ В силу единственности разложения целых чисел на простые множители ряд в правой части совпадает с рядом (3), чем и доказана справедливость формулы (5).

После этих предварительных замечаний мы можем перейти непосредственно к доказательству теоремы 3.

Рассмотрим бесконечный ряд

$$\frac{1}{p_1^s} + \frac{1}{p_2^s} + \frac{1}{p_3^s} + \dots,$$

где $p_1, p_2, p_3, \dots$ пробегают все простые числа. Этот ряд, очевидно, сходящийся (в силу того, что даже ряд $\frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \dots = \zeta(s)$ сходится при $s > 1$). Рассмотрим, как будет себя вести сумма этого ряда, если s, убывая, стремится к 1.

С одной стороны, при $s > 1$ (см. обозначения предыдущей теоремы)

$$g(s) = \sum_{n=1}^{\infty} p_n^{-s} = \sum_{n=1}^{\infty} b_n p_n^{1-s} = b_1 p_1^{1-s} +$$

$$+ \sum_{n=2}^{\infty} [B(p_n) - B(p_{n-1})]\, p_n^{1-s} = \sum_{n=1}^{\infty} B(p_n)\,(p_n^{1-s} - p_{n+1}^{1-s}) =$$

$$= \sum_{n=1}^{\infty} B(p_n)(s-1) \int_{p_n}^{p_{n+1}} \frac{dz}{z^s} = (s-1) \int_2^{\infty} \frac{B(z)}{z^s}\, dz.$$

По предыдущей теореме

$$B(z) = \ln \ln z + B + R(z),$$

где $R(z) = O\left(\frac{1}{\ln z}\right)$. Следовательно,

$$g(s) = (s-1) \int_2^{\infty} \frac{\ln \ln z}{z^s}\, dz + (s-1) \int_2^{\infty} \frac{B\, dz}{z^s} +$$

$$+ (s-1) \int_2^{\infty} \frac{R(z)}{z^s}\, dz = I_1 + I_2 + I_3.$$

Последний интеграл при $s \to 1$ стремится к нулю. В самом деле, $R(z) \to 0$ при $z \to \infty$. Поэтому, каково бы ни было $\varepsilon > 0$, существует такое $z_0 = z_0(\varepsilon)$, что для всех $z > z_0$ выполняется неравенство $|R(z)| < \frac{\varepsilon}{2}$. Беря

$$s - 1 < \frac{\varepsilon}{2 \int_2^{z_0} |R(z)|\, dz},$$

получаем

$$|I_3| < (s-1) \int_2^{z_0} \frac{|R(z)|}{z^s}\, dz + (s-1) \int_{z_0}^{\infty} \frac{|R(z)|}{z^s}\, dz <$$

$$< (s-1) \int_2^{z_0} |R(z)|\, dz + (s-1) \frac{\varepsilon}{2} \int_{z_0}^{\infty} \frac{dz}{z^s} < \frac{\varepsilon}{2} + \frac{\varepsilon}{2z_0^{s-1}} < \varepsilon.$$

Таким образом, при $s \to 1$, $I_3 = o(1)$.

Заменяя нижний предел в интегралах I_1 и I_2 через 1, что также дает ошибку $o(1)$, введем новое переменное y с помощью подстановки $z^{s-1} = e^y$. Получим

$$g(s) = \int_0^\infty e^{-y} \ln \frac{y}{s-1}\, dy + B + o(1) =$$

$$= \int_0^\infty e^{-y} \ln y\, dy - \ln(s-1) \cdot \int_0^\infty e^{-y}\, dy + B + o(1) =$$

$$= -C - \ln(s-1) + B + o(1), \qquad \text{(I)}$$

где

$$C = -\int_0^\infty e^{-y} \ln y\, dy$$

есть так называемая эйлерова постоянная.

С другой стороны,

$$\ln(s-1) + g(s) = \ln\{(s-1)\zeta(s)\} +$$

$$+ \sum_{k=1}^{\infty} \left\{ \ln\left(1 - \frac{1}{p_k^s}\right) + \frac{1}{p_k^s} \right\} \to \sum_{k=1}^{\infty} \left\{ \ln\left(1 - \frac{1}{p_k}\right) + \frac{1}{p_k} \right\},$$

так как $(s-1)\zeta(s)$ по доказанному выше стремится к 1 при $s \to 1$, а ряд в правой части равномерно сходится при $s \geqslant 1$. Таким образом

$$g(s) = -\ln(s-1) + \sum_{k=1}^{\infty} \left\{ \ln\left(1 - \frac{1}{p_k}\right) + \frac{1}{p_k} \right\} + o(1). \qquad \text{(II)}$$

Сравнивая выражения (I) и (II), заключаем:

$$B = C + \sum_{k=1}^{\infty} \left\{ \ln\left(1 - \frac{1}{p_k}\right) + \frac{1}{p_k} \right\}.$$

Вставляя это выражение для B в формулу предыдущей теоремы, получаем:

$$\sum_{p_k \leqslant x} \frac{1}{p_k} - \sum_{k=1}^{\infty} \left\{ \ln\left(1 - \frac{1}{p_k}\right) + \frac{1}{p_k} \right\} = \ln\ln x + C + O\left(\frac{1}{\ln x}\right).$$

В левой части можно отбросить все члены, соответствующие числам $p_k > x$, совершая ошибку

$$\sum_{p>x}\left(\frac{1}{2p^2}+\frac{1}{3p^3}+\dots\right)=O\left(\sum_{p>x}\frac{1}{p^2}\right)=O\left(\sum_{n>x}\frac{1}{n^2}\right)=$$

$$=O\left(\frac{1}{x}\right)=O\left(\frac{1}{\ln x}\right).$$

Отсюда получаем соотношение

$$\sum_{p\leqslant x}\ln\left(1-\frac{1}{p}\right)=-\ln\ln x-C+O\left(\frac{1}{\ln x}\right)$$

и, потенцируя,

$$\prod_{p\leqslant x}\left(1-\frac{1}{p}\right)=\frac{e^{-C}}{\ln x}e^{O\left(\frac{1}{\ln x}\right)}=\frac{e^{-C}}{\ln x}\left[1+O\left(\frac{1}{\ln x}\right)\right],$$

что и доказывает теорему 3.