Шнирельман Л.Г.

Простые числа

Москва
«Книга по Требованию»

УДК 51
ББК 22.1
Ш77

Шнирельман Л.Г.
Ш77 Простые числа / Шнирельман Л.Г. – М.: Книга по Требованию, 2012. – 60 с.

ISBN 978-5-458-26220-0

ISBN 978-5-458-26220-0

§ 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 $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$, 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 $m_1 m_2 \ldots m_i$, то говорят, что a разлагается на множители $m_1, m_2, \ldots, m_i$.

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

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

Таким образом, в силу следствия 2 теоремы о разложении,

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

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

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

и

$$aa_1 \equiv bb_1 \pmod{m}. \qquad (2)$$

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.