А. Шень

Простые и составные числа

Издание второе, стереотипное

Москва
Издательство МЦНМО
2008

ББК 22.1
Ш47

Шень А.

Ш47 Простые и составные числа. — 2-е изд., стереотип. — М.: МЦНМО, 2008. — 16 с.: ил.

ISBN 978-5-94057-200-8

Приведено доказательство «основной теоремы арифметики» о единственности разложения целых чисел на простые множители, а также несколько доказательств бесконечности множества простых чисел. Брошюра написана по материалам лекции для школьников 10–11 классов, прочитанной автором по приглашению А. В. Спивака.

ББК 22.1

Оригинал-макет предоставлен автором. Рисунок на обложке подготовлен В. В. Шуваловым в системе MetaPost. Электронная версия книги является свободно распространяемой и доступна по адресу

`ftp://ftp.mccme.ru/users/shen/primes.zip`

Александр Шень

Простые и составные числа

Подписано в печать 07.04.2008 г. Формат $60 \times 90\ {}^{1}/_{16}$. Бумага офсетная. Печать офсетная. Печ. л. 1. Тираж 3000 экз. Заказ №

Издательство Московского центра непрерывного математического образования
119002, Москва, Большой Власьевский пер., 11. Тел. +7(495)241-74-83.

ISBN 978-5-94057-200-8

Некоторые факты из арифметики считаются сами собой разумеющимися — настолько, что доказывать их в школе не принято (тем более что это не так просто). К их числу относится теорема об единственности разложения на простые множители (иногда её даже называют «основной теоремой арифметики»).

Другой факт, также не доказываемый в школе — бесконечность множества простых чисел.

В этой брошюре мы приведём доказательства этих двух утверждений (а для второго из них — даже несколько доказательств).

A. Единственность разложения

Простые и составные числа

Напомним, что целые положительные числа $(1, 2, 3, \ldots)$ бывают *простые* и *составные*. Составные — это те, которые разлагаются в произведение двух меньших, а простые — те, которые не разлагаются. Например, число 6 — составное, поскольку $6 = 2\times 3$. А числа $2, 3, 5, 7, 11, 13, 17, \ldots$ — простые (ни на что не делятся, кроме единицы и самого себя, в чём можно убедиться перебором).

1 Проверьте, что числа 571571 и 999991 являются составными. [Указание: $999991 = 1000000 - 9$.]

2 Докажите, что число $4^n - 1$ является составным при любом $n > 1$.

3 Докажите, что число $8^n + 1$ является составным при любом $n \geqslant 1$.

4 Докажите, что если число $k > 1$ — составное, то число $111\ldots111$ (k единиц) — тоже составное.

Разложение составного числа

По определению составное число раскладывается в произведение двух меньших чисел. Эти числа не обязаны быть простыми. Если они составные, то их можно разложить дальше — до тех пор, пока не останутся только простые множители.

Скажем, число 1001 — составное: $1001 = 7 \cdot 143$. Число 7 простое и дальше не разлагается, а вот 143 разлагается в произведение двух простых чисел: $143 = 11 \cdot 13$. В итоге получаем

$$1001 = 7 \cdot 11 \cdot 13.$$

Мы могли бы действовать иначе, заметив для начала, что $1001 = 11 \cdot 91$. Число 11 простое, а 91 — нет: $91 = 7 \cdot 13$. Получаем

$$1001 = 11 \cdot 91 = 11 \cdot 7 \cdot 13,$$

и дальше уже ничего не разлагается.

Схематически эти два разложения показаны на рис. 1.

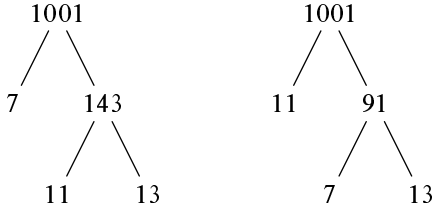

Рис. 1. Два способа получения одного разложения.

Замечание для педантов. Строго говоря, мы ещё не доказали, что всякое составное число раскладывается в произведение простых: вдруг процесс разложения будет продолжаться и продолжаться? Легко сообразить, однако, что такого быть не может. Ведь с каждым шагом числа уменьшаются, и потому в разложении числа n не больше n уровней. (И даже $\log_2 n$, поскольку множители по крайней мере вдвое меньше произведения.)

Единственность разложения: формулировка

В нашем примере (с числом 1001) мы двумя способами получили в итоге одно и то же разложение. Но всегда ли так будет? Чтобы убедиться, что это не так уж и очевидно, рассмотрим пример. Вот два разложения одного и того же числа (19165536773) на два множителя:

$$78227 \cdot 244999 = 19165536773 = 99599 \cdot 192427.$$

(Если хотите, проверьте эти равенства с помощью умножения в столбик — это можно сделать за несколько минут.)

На первый взгляд, в этих двух разложениях нет ничего общего. Не противоречит ли это единственности разложения на простые множители? Нет, поскольку никто не гарантирует, что выписанные множители — простые. На самом деле они составные.

5 (Для знакомых с алгоритмом Евклида.) Не читая дальше, разложите эти числа на дальнейшие множители.

Раскроем наш небольшой секрет, как сказал бы Сергей Довлатов:

$$78227 = 137 \cdot 571, \quad 99599 = 137 \cdot 727,$$
$$244999 = 337 \cdot 727, \quad 192427 = 337 \cdot 571,$$

и оба разложения получаются при различной группировке множителей в произведении

$$137 \cdot 337 \cdot 571 \cdot 727$$

(мы специально выбрали трёхзначные простые числа, чтобы делитель было труднее найти подбором).

Так что этот пример противоречит теореме о единственности разложения на простые множители лишь на первый взгляд. Сейчас мы торжественно провозгласим её формулировку, а затем приступим к доказательству.

Теорема о единственности разложения на множители («основная теорема арифметики»). Два разложения одного и того же числа на простые множители отличаются лишь порядком сомножителей.

(Другими словами, в эти два разложения входят одни и те же множители и в одном и том же количестве, хотя, возможно, и в разном порядке. Можно было бы договориться записывать множители в неубывающем порядке, и тогда разложение было бы совсем однозначно.)

В следующих разделах мы постепенно докажем эту теорему.

Основная лемма

Важную роль в доказательстве играет следующая

Лемма. Если произведение ab двух целых чисел a и b делится на простое число p, то хотя бы один из сомножителей делится на p.

Слово «делится» означает «делится без остатка»: целое число m делится на целое число $n \neq 0$, если остаток от деления m на n равен нулю (то есть m/n — целое число).

Ту же самую лемму можно сформулировать и иначе:

- если два числа не делятся на p, то и их произведение не делится на p;
- если произведение ab делится на p, а первый сомножитель a не делится на p, то второй сомножитель b делится на p.

Все эти три формулировки разными словами говорят одно и то же: не может быть, чтобы одновременно число a не делилось на p, число b не делилось на p и произведение ab делилось на p.

(Народная мудрость советской эпохи гласила, что человек не может быть одновременно порядочным, умным и членом КПСС. Равносильные формулировки: умный член КПСС не может быть порядочным, порядочный член КПСС не может быть умным и т.д.)

Замечание 1. В лемме существенно, что число p простое. Скажем, при $p = 6$ утверждение леммы неверно: произведение чисел 2 и 3 делится на 6, а ни один из сомножителей на 6 не делится.

Замечание 2. Из леммы легко следует аналогичное утверждение для произвольного числа сомножителей: если их произведение делится на простое p, то хотя бы один из сомножителей делится на p. Например, пусть произведение abc трёх сомножителей делится на p. Записав его как $(ab)\cdot c$, заключаем по лемме, что либо ab делится на p, либо c делится на p. В первом случае надо применить лемму ещё раз и заключить, что либо a делится на p, либо b делится на p. (Аналогичное рассуждение годится и для большего числа сомножителей.)

Вывод теоремы из леммы

Мы до сих пор не доказали ни основной теоремы (об единственности разложения), ни сформулированной леммы. Начнём с того, что выведем теорему из леммы. Это делается так.

Пусть имеются два разложения одного и того же числа на простые множители:

$$p_1 \cdot p_2 \cdot \ldots = q_1 \cdot q_2 \cdot \ldots$$

Если в них есть общий множитель (одно из p_i равно одному из q_j), сократим обе части на этот общий множитель. Будем повторять это до тех пор, пока общих множителей не останется. Если при этом сократится всё (в обеих частях останется единица), то это означает, что исходные разложения отличались лишь порядком множителей, как и требует теорема.

Если сократится не всё, то в обеих частях останутся какие-то несократившиеся множители. (Если с одной стороны сократится всё, то получится единица, и потому с другой стороны тоже должно всё сократиться.) Это противоречит лемме: если

$$N = p_1 \cdot p_2 \cdot \ldots = q_1 \cdot q_2 \cdot \ldots$$

и общих множителей нет, то произведение $N = q_1 \cdot q_2 \cdot \ldots$ делится на p_1 (поскольку $N = p_1 \cdot \ldots$), а ни один из сомножителей q_i не делится на p_1 (простое число q_i может делиться лишь на единицу и на себя, а $q_i \neq p_1$, так как общих множителей нет).

Итак, теорема об единственности разложения на простые множители следует из сформулированной нами леммы. Но как доказать лемму?

Лемма для конкретных p

Рассмотрим для начала случай $p = 2$. Числа, делящиеся на 2, называют чётными, а не делящиеся — нечётными. Лемма утверждает, что произведение двух нечётных чисел нечётно.

Доказать это совсем просто: при делении целого числа на 2 получается остаток 0 для чётных чисел и 1 для нечётных чисел. Поэтому нечётные числа имеют вид $2k + 1$ для целых k. Произведение двух нечётных чисел имеет вид

$$(2k + 1)(2l + 1) = 4kl + 2k + 2l + 1;$$

три первых слагаемых делятся на 2, поэтому при делении на 2 в остатке получится единица — то есть произведение нечётно.

Немного сложнее случай $p = 3$. При делении на 3 возможны остатки 0, 1 и 2, поэтому не делящиеся на 3 числа бывают двух видов: $3k + 1$ и $3k + 2$. Для произведения двух не делящихся на 3 чисел есть, таким образом, четыре варианта:

$$\begin{aligned}
(3k + 1)(3l + 1) &= 9kl + 3k + 3l + 1,\\
(3k + 1)(3l + 2) &= 9kl + 6k + 3l + 2,\\
(3k + 2)(3l + 1) &= 9kl + 3k + 6l + 2,\\
(3k + 2)(3l + 2) &= 9kl + 6k + 6l + 4.
\end{aligned}$$

Первые три слагаемых во всех случах делятся на 3 нацело, и остаток определяется последним слагаемым. Он равен соответственно $1, 2, 2, 1$ (в последнем случае $4 = 3 + 1$, так что в остатке получается 1).

Удобно изобразить сказанное в виде таблицы умножения остатков при делении на 3 («по модулю 3»):

	1	2
1	1	2
2	2	1

В правой нижней клетке (произведение двух остатков 2) стоит 1, так как $2 \cdot 2 = 4$ даёт остаток 1 при делении на 3. Видно, что во всех случах остаток не нуль, поэтому произведение не делится на 3 и лемма (для случая $p = 3$) доказана.

Аналогичная таблица умножения остатков при делении на 4 имеет вид

	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

В ней имеется нуль; этот нуль гласит, что произведение двух чисел, дающих при делении на 4 остаток 2, делится на 4 без остатка:

$$(4k+2)(4l+2) = 16kl + 8k + 8l + 4.$$

Это и не удивительно, ведь число 4 не простое и для него лемма неверна: произведение $2 \cdot 2 = 4$ делится на 4, а сомножители не делятся.

Зато для $p = 5$ всё опять хорошо:

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Скажем, четвёртый элемент второй строки соответствует произведению

$$(5k+2)(5l+4) = 25kl + 20k + 10l + 8 = \\ = 25kl + 20k + 10l + (5+3) = 5(5kl + 4k + 2l + 1) + 3,$$

и остаток при делении на 5 равен 3.

Мораль: хотя общего доказательства леммы (для произвольного p) мы пока не знаем, для любого конкретного значения p лемма (если верна!) может быть доказана перебором всех вариантов: надо перемножить все возможные пары остатков a, b от 1 до $p-1$ и убедиться, что ни одно из этих произведений не делится на p.

Вывод леммы из теоремы

Сформулированную нами лемму можно доказывать так. Пусть a и b не делятся на p. Разложим их на множители. В этих разложениях множителя p нет. Соединяя разложения для a и b, получим разложение для ab, в котором нет множителя p. С другой стороны, если ab делится на p, то начав с выделения множителя p, мы получим разложение для ab, в котором множитель p есть. Что противоречит единственности разложения: в одном разложении множитель p есть, а в другом нет.

Что даёт нам это рассуждение? Раньше мы выводили теорему об единственности разложения из леммы, а теперь наоборот: предположив единственность разложения, доказали лемму. Проку в этом, впрочем, немного: Иван кивает на Петра, а Пётр кивает на Ивана, как говорит пословица, и получается «порочный круг». Так что оба утверждения — теорема о единственности разложения на множители и наша лемма — остаются недоказанными, хотя мы и знаем, что из одного из них следует другое.

Удивительным образом оказывается, что всё-таки это не совсем круг. Если подробно проанализировать доказательства, то мы увидим, что утверждение леммы сводится к самому себе, но для меньших p, что позволяет завершить рассуждение по индукции. Сейчас мы подробно объясним, что имеется в виду.

Завершение доказательства

Пока мы не доказали лемму, будем называть простое число p *хорошим*, если для него лемма верна. (На самом деле все простые числа хорошие, только этого мы ещё не знаем.) Остальные (не хорошие) простые числа мы будем называть *плохими*.

Урезанная теорема: если два различных произведения простых чисел равны, то в обоих есть плохие сомножители.

По существу мы это уже доказали. Повторим соответствующее рассуждение. Если в двух разложениях одного и того же числа есть общие множители, сократим их. Нам надо доказать, что в оставшихся произведениях (обоих) есть плохие множители. Пусть это не так, и

$$p_1 \cdot p_2 \cdot \ldots = q_1 \cdot q_2 \cdot \ldots,$$

причём в одной из частей этого равенства (скажем, левой) плохих множителей нет. Тогда p_1 — хорошее простое число, и для него верна лемма (точнее, не лемма, а утверждение леммы, оно же определение хорошего числа). Получается, что произведение $q_1 \cdot q_2 \cdot \ldots$ делится на хорошее простое число p_1, а ни один из множителей q_i — нет, чего быть не может. (Мы должны ещё перейти от произведения двух чисел к произведению нескольких, но это делается точно так же, как и раньше.)

Докажем теперь, что плохих простых чисел нет. (И тем самым завершим доказательство теоремы о единственности разложения на множители.)

Рассуждая от противного, предположим, что это не так и что плохие простые числа есть. Возьмём наименьшее такое число. Обозначим его p.

Составим таблицу произведений остатков при делении на p. Поскольку p плохое, в этой таблице должен быть нуль: для некоторых a и b, меньших p, произведение ab делится на p без остатка.

Разложим a и b на простые множители. Все эти простые множители меньше p (поскольку a и b меньше p) и потому хорошие (по предположению число p было минимальным плохим числом). Перемножив разложения для a и b, получим разложение ab на хорошие простые множители. Но у ab есть и другое разложение, начинающееся с p (поскольку ab по предположению делится на p). А это противоречит урезанной теореме, которая говорит, что *в обоих* разложениях должны быть плохие множители.

Замечание для знатоков: более естественно доказывать однозначность разложения на множители с помощью алгоритма Евклида нахождения наибольшего общего делителя, но это — тема отдельного разговора, выходящего за рамки брошюры.

Б. Простых чисел бесконечно много

Этот факт доказан уже в «Началах» Евклида, и приведённое там доказательство до сих пор остаётся самым простым и естественным. Но есть и другие доказательства, и они по-своему поучительны. Мы приведём несколько таких доказательств, начав с Евклида.

Доказательство Евклида

Пусть нам дали список из n простых чисел $p_1, \ldots, p_n$. Покажем, что туда входят не все простые числа. Для этого рассмотрим число

$$N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1.$$

Это число не делится нацело ни на одно из $p_1, \ldots, p_n$ (остаток равен 1). Значит, в разложение N на простые множители должны входить простые числа, отсутствующие в нашем списке.

Например, для списка из трёх простых чисел $2, 3, 5$ получаем

$$N = 2 \cdot 3 \cdot 5 + 1 = 31.$$

В данном случае N само оказалось простым числом, не входящим в список. Но так бывает не всегда: например,

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 59 \cdot 509,$$

и мы получаем два простых числа (59 и 509), не входящие в список.

6 Покажите, что при любом целом положительном $n > 2$ существует хотя бы одно простое число, большее n и меньшее $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$.

7 Покажите, что существует бесконечно много простых чисел вида $3k + 2$ (дающих остаток 2 при делении на 3). [Указание: среди простых делителей числа вида $3k + 2$ всегда найдётся хотя бы одно число такого же вида.]

8 Покажите, что существует бесконечно много простых чисел вида $4k + 3$. Покажите, что существует бесконечно много простых чисел вида $6k + 5$.

Все эти утверждения — частные случаи общей теоремы Дирихле о том, что в целочисленной арифметической прогрессии, у которой первый член и разность не имеют общих делителей, бесконечно много простых чисел. Но доказательство этой теоремы использует методы математического анализа и далеко выходит за рамки брошюры.

Числа Ферма

Так называют числа

$$2 + 1, 2^2 + 1, 2^4 + 1, 2^8 + 1, 2^{16} + 1, 2^{32} + 1, \ldots$$

(показатель степени есть степень двойки). Пьер Ферма (тот самый, что в XVII веке записал на полях книги утверждение «теоремы Ферма» об уравнении $x^n + y^n = z^n$; эту теорему доказали всего несколько лет назад) высказал предположение, что все эти числа простые.

Первые пять чисел действительно простые. Эйлер, однако, обнаружил, что уже шестое число $2^{32} + 1$ простым не является и делится на 641. (Современный компьютер позволяет найти это разложение за доли секунды, но во времена Ферма и Эйлера это было совсем не просто. Эйлер нашёл его, предварительно доказав, что все делители числа $2^{32} + 1$ должны иметь вид $64k + 1$.)

Впоследствии среди чисел Ферма было обнаружено ещё много составных, но ни одного нового простого среди них пока не найдено. Тем не менее (как заметил знакомый Эйлера Гольдбах, который известен как автор *гипотезы Гольдбаха* о том, что каждое чётное число есть сумма двух простых), числа Ферма можно использовать для доказательства бесконечности множества простых чисел. Вот как это делается.

Два целых числа называются *взаимно простыми*, если у них нет общих делителей (не считая единицы).

Простое число p взаимно просто с любым числом, кроме делящихся на p. Однако взаимно простыми могут быть и два составных числа: скажем, $6 = 2 \cdot 3$ взаимно просто с $35 = 5 \cdot 7$.

Для тренировки покажем, что числа n и $n+1$ взаимно просты при любом целом $n > 0$. Это почти очевидно: если бы у них был общий делитель $d > 1$, то это означало бы, что два кратных числа d стоят рядом, что невозможно, так как они идут с интервалом d. Другое объяснение: если два числа делятся на d, то и их разность должна делиться на d. А у соседних чисел разность равна 1 и на d делиться не может.

Лишь немного сложнее показать, что n и $n+2$ взаимно просты при нечётном n. В самом деле, общий делитель d должен быть делителем разности, то есть числа 2, поэтому остаётся единственный случай $d = 2$. Но по предположению n нечётно и не делится на 2, так что и этот случай отпадает.

9 Покажите, что при любых целых положительных n и k числа n и $kn+1$ взаимно просты.

Вернёмся к числам Ферма и покажем, что любые два из них взаимно просты. Для этого сделаем такое наблюдение: если в числе Ферма заменить $+1$ на -1, его легко разложить на множители с помощью формулы разности квадратов. Скажем,

$$2^8 - 1 = (2^4)^2 - 1^2 = (2^4 + 1)(2^4 - 1).$$

Продолжая раскладывать тем же способом, получаем

$$2^8 - 1 = (2^4 + 1)(2^4 - 1) = \\ = (2^4 + 1)(2^2 + 1)(2^2 - 1) = (2^4 + 1)(2^2 + 1)(2 + 1)(2 - 1)$$

(последний множитель $(2-1)$ можно и опустить, так как он равен единице). Аналогично и для бóльших степеней:

$$2^{16} - 1 = (2^8 + 1)(2^4 + 1)(2^2 + 1)(2 + 1)(2 - 1)$$

и вообще произведение первых k чисел Ферма почти равно следующему числу Ферма (меньше его на 2, поскольку содержит -1 вместо $+1$).

Теперь видно, почему числа Ферма взаимно просты: любой делитель d данного числа Ферма будет делителем любого следующего числа Ферма, уменьшенного на 2, и потому не может делить само это число Ферма. (Случай $d = 2$ также невозможен, так как все числа Ферма нечётны.)

Итак, любые два числа Ферма взаимно просты. Значит, в их разложения на простые множители входят различные простые множители — и потому простых чисел бесконечно много.

Гармонический ряд

Ещё одно доказательство бесконечности множества простых чисел использует *расходимость гармонического ряда*. Эти слова означают, что сумма

$$1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n}$$

может быть сделана сколь угодно большой, надо только взять достаточно много слагаемых.

Наглядно это утверждение можно представлять себе так. Мы идём уменьшающимися шажками — первый длины 1, второй $1/2$, далее $1/3$, $1/4$, $1/5,\ldots$ (рис. 2). Оказывается, что несмотря на уменьшение со временем

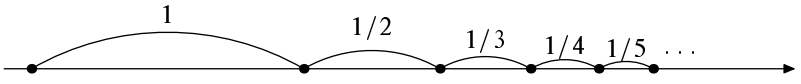

Рис. 2. Расходимость гармонического ряда.

длины шага, таким манером можно уйти сколь угодно далеко.

Чтобы убедиться в этом, разделим гармонический ряд на части:

$$1+\frac{1}{2}+\left(\frac{1}{3}+\frac{1}{4}\right)+\left(\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}\right)+\ldots$$

(в каждой скобке последнее слагаемое имеет в знаменателе степень двойки). Правило тут такое: n-я по счёту скобка начинается с дроби $1/(2^n+1)$, кончается дробью $1/2^{n+1}$ и содержит 2^n слагаемых. (Скажем, следующая скобка будет содержать числа от $\frac{1}{9}$ до $\frac{1}{16}$ включительно.) Наименьшее из чисел в каждой из скобок — последнее, и если все слагаемые заменить на него, то получится сумма

$$1+\frac{1}{2}+\left(\frac{1}{4}+\frac{1}{4}\right)+\left(\frac{1}{8}+\frac{1}{8}+\frac{1}{8}+\frac{1}{8}\right)+\ldots,$$

в которой каждая скобка равна $1/2$. Поэтому если взять достаточно много скобок, мы уйдём сколь угодно далеко, как и утверждалось.

10 Укажите такое количество шагов (членов ряда), чтобы сумма была больше 100.

Важно понимать, что сама по себе бесконечность числа слагаемых не гарантирует, что мы далеко уйдём. Например, сколько ни бери слагаемых в сумме

$$1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\frac{1}{16}+\frac{1}{32}+\ldots,$$

всё равно больше 2 не получится: каждый следующий член составляет половину оставшегося расстояния до точки 2 (рис. 3), и мы на каждом шаге

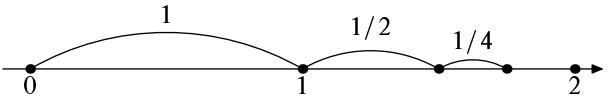

Рис. 3. Бесконечно убывающая прогрессия.

приближаемся к этой точке вдвое, так никогда её и не достигнув. Формально говоря,

$$1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\ldots+\frac{1}{2^n}=2-\frac{1}{2^n};$$

чтобы убедиться в этом, достаточно перенести $1/2^n$ из правой части в левую и затем свернуть левую часть, объединяя одинаковые слагаемые.

Разница между этими двумя примерами объясняется тем, что в бесконечно убывающей прогрессии (втором примере) слагаемые убывают гораздо быстрее.

Всё это замечательно, но при чём тут простые числа? Удивительным образом связь существует, и очень глубокая. Давайте для начала перемножим две суммы

$$\left(1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\ldots\right)\cdot\left(1+\frac{1}{3}+\frac{1}{9}+\frac{1}{27}+\ldots\right)$$

(обратные степени двойки и тройки; сколько именно слагаемых в каждой скобке, мы решим потом). После раскрытия скобок в произведении возникнут слагаемые 1 (как $1\cdot1$), $1/2$ (как $(1/2)\cdot1$), $1/3$ (как $1\cdot(1/3)$), $1/4$ (как $(1/4)\cdot1$), $1/6$ (как $(1/2)\cdot(1/3)$) и так далее. Заметьте, что при этом пропущена $1/5$, нет также $1/7$, $1/10$ и др. Формально говоря, произведение двух скобок будет суммой всех дробей вида

$$\frac{1}{2^k3^l}$$

при не слишком больших k и l (каких именно — зависит от того, сколько членов мы взяли в наших двух суммах).

Чтобы восполнить хотя бы часть пропущенного, добавим третий множитель и рассмотрим произведение

$$\left(1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\ldots\right)\cdot\left(1+\frac{1}{3}+\frac{1}{9}+\ldots\right)\cdot\left(1+\frac{1}{5}+\frac{1}{25}+\ldots\right)$$

Теперь уже есть знаменатели вида $2^k 3^l 5^m$ (так что $1/5$ и $1/10$ вошли в сумму), но, скажем, $1/7$ по-прежнему нет. Чтобы появилась $1/7$, надо домножить произведение на

$$\left(1+\frac{1}{7}+\frac{1}{49}+\dots\right)$$

и так далее.

Продолжая эти наблюдения, можно придти к такому выводу: *если бы простых чисел было конечное число n, то гармонический ряд бы не превысил 2^n* (а мы знаем, что это не так — значит, простых чисел бесконечно много).

В самом деле, пусть $2, 3, \dots, p$ — все простые числа и их всего n. В этом случае произведение

$$\left(1+\frac{1}{2}+\frac{1}{4}+\dots\right)\cdot\left(1+\frac{1}{3}+\frac{1}{9}+\dots\right)\cdot\dots\cdot\left(1+\frac{1}{p}+\frac{1}{p^2}+\dots\right)$$

содержит n сомножителей. Каждый из сомножителей меньше двух (про первый мы уже говорили, остальные почленно меньше первого). Значит, произведение меньше 2^n. С другой стороны, взяв достаточно членов в каждой скобке, мы можем получить после раскрытия скобок сколь угодно длинный кусок гармонического ряда без пропусков (а дальше — с пропусками). Ведь мы предположили, что других простых чисел нет, значит, любой знаменатель представим в виде произведения имеющихся.

Таким образом, расходимость гармонического ряда неизбежно влечёт за собой бесконечность множества простых чисел!

Замечание 1. Использовали ли мы в этом рассуждении однозначность разложения чисел на простые множители? На самом деле нет. Если бы разложение на множители какого-либо числа N было неоднозначным, это привело бы к тому, что при раскрытии скобок у нас появилось несколько слагаемых вида $1/N$ (столько, сколько есть различных разложений). Но если даже с несколькими такими слагаемыми сумма не больше 2^n, то уж с одним и подавно. А вот существование (хотя бы одного) разложения любого числа на простые множители мы действительно использовали, когда говорили, что в произведении можно получить любые члены гармонического ряда.

Замечание 2. Более тонкий анализ (основанный на тех же идеях) позволяет доказать, что не только гармонический ряд расходится, но и ряд

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\dots$$

(в знаменателях — простые числа) тоже расходится.

Сравнение количеств

В некотором смысле это доказательство можно считать переформулировкой предыдущего. Мы покажем, что если бы простых чисел было бы конечное число, то их произведений и произведений их степеней не хватило бы на всех.

Предположим, что имеется всего n простых чисел $p_1, \ldots, p_n$. Выберем некоторое целое положительное k и рассмотрим числа

$$1, p_1, p_1^2, \ldots, p_1^k,$$

а также числа

$$1, p_2, p_2^2, \ldots, p_2^k,$$

затем

$$1, p_3, p_3^2, \ldots, p_3^k,$$

и так далее вплоть до

$$1, p_n, p_n^2, \ldots, p_n^k.$$

Каждая строчка состоит из $k+1$ чисел (степени от 0 до k). Всего есть n строчек, соответствующих n простым числам. Выберем в каждой строчке по одному элементу и перемножим их. В каждой строчке есть $(k+1)$ вариантов выбора, поэтому всего вариантов будет $(k+1)^n$. (Наименьшее произведение получится, если выбрать все единицы, наибольшее равно $p_1^k p_2^k \ldots p_n^k$.)

Если — как мы предположили, намереваясь придти к противоречию — нет простых чисел, кроме $p_1, \ldots, p_n$, то *среди полученных произведений встретятся все числа от* 1 *до* 2^k. В самом деле, каждое из чисел от 1 до 2^k можно разложить на простые множители. При этом каждый множитель может войти в степени не больше k, поскольку даже самое малое простое число 2 в степени больше k уже выходит за пределы участка $1 \ldots 2^k$.

Что же получается? Каждое из 2^k чисел участка представимо в виде произведения, а таких произведений всего $(k+1)^n$. Это возможно, лишь если произведений хватает на всех, то есть

$$2^k \leqslant (k+1)^n.$$

Здесь n — количество простых чисел (конечное, по нашему предположению), а k можно выбрать любым. Получается, что показательная функция $k \mapsto 2^k$ растёт не быстрее степенной $k \mapsto (k+1)^n$. Что неверно, как знают любители математического анализа.

(Мы не будем проводить подробно соответствующее доказательство, но идея его проста. Если большое k увеличить ещё на единицу, то 2^k удвоится. В то же время $(k+1)^n$ возрастёт лишь в $((k+2)/(k+1))^n$ раз, что при больших k (и фиксированном n) близко к единице. Поэтому геометрическая прогрессия 2^k быстро перегонит степенную функцию, с которой она сравнивается.)