149. Разложение на множители

Целое число $p > 1$ называется *простым*, если оно не представляется в виде произведения двух меньших положительных целых чисел, и *составным* в противном случае.

1. Всякое целое положительное число разлагается в произведение простых множителей. В самом деле, если число простое, то оно и будет единственным множителем, если нет — разложим его в произведение двух. Если они простые, хорошо, если нет — разложим их дальше. На каждом шаге числа уменьшаются, и процесс этот рано или поздно кончится. (Формально можно доказать существование разложения числа n индукцией по n.)

2. Разложение на множители однозначно (с точностью до порядка множителей). Доказательство этого факта использует такую лемму: если произведение ab делится на простое p, то хотя бы одно из чисел a и b делится на p. Пусть лемма уже доказана. Тогда легко доказать аналогичный факт для произведения трёх и более сомножителей: если $abc = (ab)c$ делится на простое p, то хотя бы одно из чисел ab и c делится на p, и, следовательно, хотя бы одно из чисел a, b и c делится на p. (Формально: индукция по числу сомножителей.) Теперь представим себе, что есть два разложения

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

одного и того же числа на множители. Покажем, что любое простое p входит в них одинаковое число раз. В самом деле, если оно входит в одну из частей, то по доказанному должно входить и во вторую. Сокращаем и повторяем до тех пор, пока множителей p не останется ни слева, ни справа — значит, их было одинаковое количество.

Итак, осталось доказать лемму.

3. Важное замечание. В предыдущем пункте мы доказали такой факт: если для некоторого p верно утверждение леммы, то в любые два разложения одного и того же числа на простые множители это p входит одинаковое число раз.

4. Доказательство леммы. Пусть она верна не для всех p и пусть P — наименьшее простое число, для которого она не верна. (Другими словами, мы применяем индукцию по p.) Пусть a и b таковы, что ab делится на P, но ни a, ни b не делятся на P. Не ограничивая общности, можно считать, что a и b меньше P (в противном случае заменим их на остатки по модулю P — это ничего не изменит с точки зрения делимости на P). По предположению

$$ab = Pz$$

для некоторого целого z. Разложим a, b и z на простые множители (P и так простое). Получим два разложения одного числа, причём слева стоят только простые числа, меньшие P. Для них лемма верна и потому в любых двух разложениях они должны встречаться одинаковое число раз. Значит, все множители левой части входят и в правую — но вдобавок к ним там есть ещё и P (по крайней мере). Противоречие.

Лемма (а значит, и теорема об однозначности разложения на множители) доказана.

150. Другой вариант доказательства

Будем доказывать, что если произведение двух чисел a и b делится на простое число p, то зотя бы одно из них делится на p.

Пусть n — положительное целое число (пока не требуется, чтобы оно было просты). Рассмотрим всевозможные остатки при делении на n (т.е. $0, 1, 2, \ldots, n-1$) и изобразим их точками — вершинами правильного n-угольника. Пусть a — произвольное число. Соединим вершины стрелками, проведя из каждой точки x стрелку в $x + a$ (сложение по модулю n) (Например, при $n = 3$ мы соединяем вершины многоугольника через две на третью.)

1. Из каждый вершины выходит ровно одна стрелка (что очевидно по построению); в каждую вершину x входит только одна стрелка (из вершины $x - a$).

2. Отсюда следует, что стрелки группируются в циклы. В самом деле, идя по стрелкам, мы должны когда-то попасть в уже пройденную вершину, но это может быть только начальная вершина, так как во все остальные стрелки уже ведут.

3. В нашем конкретном случае все циклы будут одинаковой длины. (Следовательно, эта длина — делитель n.) Геометрически это ясно — циклы, начинающиеся из разных точек, отличаются поворотом. А можно сказать иначе: последовательность

$$x \mapsto x + a \mapsto x + 2a \mapsto \ldots \mapsto x + ka$$

свернётся в цикл, когда x сравнимо с $x + ka$ по модулю n, то есть когда ka делится на n, и это не зависит от x.

4. Из сказанного видно, что длина циклов — это минимальное k, при котором ka делится на n.

5. Пусть теперь n просто (и равно числу p, для которого ab делится на p). Тогда размер цикла должен быть делителем простого p и потому есть два варианта: либо цикл имеет длину 1 (тогда стрелки ведут из вершины в неё же, то есть $x + a$ сравнимо с a, то есть a делится на p), либо цикл имеет длину p.

6. Нам осталось доказать, что в последнем случае b делится на b. В самом деле, после b шагов по стрелкам мы прибавляем число ab, которое кратно p, то есть возвращаемся в исходную точчку. Значит, мы сделали целое число оборотов по циклу длиной p, то есть b делится на p. Что и требовалось доказать.

151. Третий вариант доказательства

1. Лемма: если числа m и n взаимно просты (не имеют общих делителей, кроме 1), то можно найти такие целые x и y, что $mx + ny = 1$.

Доказательство. Для данных m и n рассмотрим все числа, которые представимы в виде $mx + ny$ при некоторых x и y. (Для краткости будем просто называть их «представимым».) Сумма и разность представимых чисел представима (сложим представления). Любое кратное представимого числа само представимо (умножим представление на число). Как говорят, «представимые числа образуют идеал».

Рассмотрим наименьшее положительное представимое число d и докажем, что все представимые числа ему кратны. В самом деле, если какое-то представимое число s делится на d с остатком, то $s = qd + r$, тогда s, d, qd и $r = s - qd$ представимы. Получилось, что меньшее ($r < d$) число представимо, что возможно лишь если $r = 0$. Итак, все представимые числа кратны d. В частности, m и n (которые представимы) кратны d, и потому $d = 1$ (так как

m и n не имеют общих делителей). Следовательно, число 1 представимо, что и требовалось доказать.

2. Докажем теперь, что если ab делится на простое число p, то одно из чисел a и b делится на p. В самом деле, пусть a не делится на p. Тогда a и p взаимно просты. По лемме найдём x и y, для которых $ax + py = 1$. Умножим это равенство на b, получим $abx + pby = b$. Оба сомножителя в левой части делятся на p (первый содержит ab, второй – p), так что и их сумма b делится на p, что и требовалось доказать.

152. Четвёртый вариант доказательства

1. Будем называть *преобразованием Евклида* такое действие: в паре целых положительных чисел a, b заменяем большее (пусть это a) на его остаток при делении на меньшее.

Лемма: при таком преобразовании наибольший общий делитель не меняется (в частности, взаимно простые числа остаются взаимно простыми).

(В самом деле, у пар (a, b) и $(a \bmod b, b)$ одни и те же общие делители.)

2. Начав с пары a, b, мы многократно применяем преобразование Евклида. При этом все числа во всех парах могут быть представлены как комбинация a и b с целыми коэффициентами, то есть как $ax + by$ для некоторых целых x и y. В самом деле, два числа p и q представимы в таком виде, то и $p \bmod q$ представимо.

3. Алгоритм Евклида: применять преобразование, пока не останется пара $x, 0$. Поскольку преобразование не меняет наибольший общий делитель и $НОД(x, 0) = x$, то $x = (a, b)$.

Следовательно, $НОД(a, b)$ представимо как $ax + by$ при некоторых x и y.

Далее рассуждаем как в предыдущем варианте доказательства.