

Алгебра, осень 2021 г.

Е. Ю. Смирнов

АННОТАЦИЯ. Записки лекций для второго курса совместного бакалавриата ВШЭ и ЦПМ, осень 2021/22 учебного года.

1. ПЕРВАЯ ЛЕКЦИЯ, 6 СЕНТЯБРЯ 2021 Г.

1.1. Целые числа и делимость. Начнём с изучения множества целых чисел $\mathbb{Z}$. Как всем хорошо известно из начальной школы, целые числа можно *складывать* и *умножать* — то есть на них определены две операции, удовлетворяющие известным аксиомам; в начальной школе их называют *переместительный, сочетательный и распределительный законы*, а в университетском курсе — *коммутативностью, ассоциативностью и дистрибутивностью*. Про аксиоматику целых чисел мы поговорим в одной из следующих лекций. А пока что обратим внимание, что и по сложению, и по умножению есть нейтральные элементы (нуль и единица соответственно); кроме того, для каждого числа n существует число $-n$, которое будет для n *обратным по сложению* (иногда ещё говорят *противоположным*): это число, которое в сумме с n даёт нуль. Это даёт возможность *вычитать* целые числа: $m - n$ определяется как число, которое получается, если к m прибавить $-n$.

А вот делить друг на друга целые числа получается не всегда. Так, чисел n , к которым существует *обратный по умножению*, т.е. такой $m = n^{-1}$, для которого $mn = 1$, всего два: это 1 и -1 . Интересно, что каждый из них обратен сам к себе (нам это пригодится в дальнейшем). Так что гарантированно делить получается только на ± 1 . Для остальных пар чисел приходится вводить понятие *делимости*.

Определение 1.1. Пусть $a, b \in \mathbb{Z}$. Говорят, что число a *делится на* b , если существует такое $c \in \mathbb{Z}$, для которого $a = bc$. Обозначение: $a : b$. Эквивалентное обозначение: $b \mid a$; в таком случае говорят, что b *делит* a . Число b в таком случае называется *делителем* числа a .

1.2. НОД и алгоритм Евклида. Если у нас есть два числа $a, b \in \mathbb{Z}$, можно рассмотреть их *общие делители*, т.е. такие числа c , для которых $c \mid a$ и $c \mid b$. Существуют два способа определить *наибольший общий делитель* (сокращённо НОД) чисел a и b .

Определение 1.2. *Наибольшим общим делителем* чисел a и b называется самый большой из общих делителей a и b .

Определение 1.3. *Наибольшим общим делителем* чисел a и b называется такой общий делитель d чисел a и b , который делится на любой другой общий делитель d' чисел a и b .

Date: 9 сентября 2021 г.

Вы используете эти записки на свой страх и риск. Никто не гарантирует, что их текст полностью соответствует содержанию лекций. Тем более не гарантируется отсутствие в этом тексте ошибок. Впрочем, о найденных ошибках лучше сообщать автору.

У обоих этих определений есть недостатки. Так, первое определение использует дополнительную структуру — *отношение порядка* на $\mathbb{Z}$. Про определение 1.3 непонятно, почему определяемый объект вообще существует. Попробуем с этим разобраться. Лучший способ доказать существование чего-либо — предъявить способ его построения. Для нахождения НОД используется *алгоритм Евклида*. Чтобы определить алгоритм Евклида, сначала напомним, что такое деление с остатком.

Определение 1.4. Разделить с остатком число a на число $b \neq 0$ — значит найти такие $q, r \in \mathbb{Z}$, для которых $a = bq + r$, причём $0 \leq r < |b|$. Число q называется *неполным частным*, а r — *остатком*.

Очевидно, что такие q и r всегда существуют; для их нахождения надо рассмотреть наименьшее положительное из чисел вида $a - qb$, это и будет остаток r .

Упражнение 1.5. Разделите с остатком -18 на 5 .

Алгоритм Евклида. Рассмотрим два числа (a, b) ; будем считать, что $|a| \geq |b|$. Поделим a на b с остатком: $a = bq + b_1$. Далее заменим пару (a, b) на пару (b, b_1) . Снова поделим первое число в паре на второе с остатком; обозначим остаток b_2 . Заменим эту пару на (b_1, b_2) , и так далее. Будем так продолжать до тех пор, пока меньшее число в паре не обратится в нуль. Пусть последняя ненулевая пара равна $(b_n, 0) = (d, 0)$; тогда d равняется наибольшему общему делителю чисел a и b .

В силу определения 1.4 имеются равенства $|b| \geq b_1 \geq b_2 \dots$; это значит, что алгоритм завершит работу за конечное число шагов.

Для доказательства того, что алгоритм Евклида действительно возвращает НОД, заметим, что множество общих делителей для пар (a, b) , (b, b_1) , $(b_1, b_2), \dots$ совпадают для всех этих пар. Действительно, пусть c — общий делитель для a, b . Тогда c будет делителем для числа $a - bq = b_1$, то есть c делит b_1 . Обратно, если c делит b и b_1 , то c делит a . Значит, множество общих делителей для всех пар одно и то же, а значит, оно совпадает со множеством делителей числа d . Но наибольший из делителей d — это само d .

Здесь для работы с НОДом мы пользовались определением 1.2. Посмотрим, почему оно равносильно определению 1.3. Для этого воспользуемся очень полезным приёмом, известным как *линейное выражение НОДа*.

Сначала заметим, что каждое из чисел $b_1, b_2, \dots, b_n$ представляется в виде $b_k = ax_k + by_k$ для некоторых x, y . Докажем это по индукции. База: для b_1 это верно: $b_1 = a - bq$. Переход: пусть $b_{k-1} = ax_{k-1} + by_{k-1}$, $b_k = ax_k + by_k$. Поделим b_{k-1} на b_k с остатком; получим, что если $b_{k-1} = b_k q_k + b_{k+1}$, то $b_{k+1} = (ax_{k-1} + by_{k-1}) - q_k(ax_k + by_k) = a(x_{k-1} - q_k x_k) + b(y_{k-1} - q_k y_k)$, что и требовалось. Следовательно, последний элемент d тоже представим в таком же виде: $d = ax + by$.

Далее, ясно, что если d' — некоторый общий делитель a, b , то $d' \mid ax + by = d$. Поэтому число d делится на все общие делители a и b . Стало быть, d и есть НОД в смысле определения 1.3, а значит, эти определения эквивалентны.

Зафиксируем последнее рассуждение в виде следующего предложения.

Предложение 1.6. Пусть d — наибольший общий делитель чисел $a, b \in \mathbb{Z}$. Тогда существуют такие целые числа x, y , для которых $d = ax + by$.

Для нахождения этих чисел можно воспользоваться алгоритмом Евклида, как указано выше.

1.3. Взаимная простота. Будем называть два элемента a, b *взаимно простыми*, если их НОД равен 1. Это равносильно существованию таких x, y , для которых $ax + by = 1$.

- Лемма 1.7.** (1) Пусть a, b взаимно просты. Тогда, если c делится на a и на b , то c делится на ab .
- (2) Пусть a, b взаимно просты. Тогда, если b делит ac , то b делит c .
- (3) Пусть a взаимно просто с каждым из $b_1, \dots, b_k$. Тогда a взаимно просто с их произведением.

Доказательство. Для доказательства первых двух утверждений запишем линейное представление НОД чисел a, b и домножим это равенство на c :

$$asx + bcy = c.$$

- (1) В предыдущем равенстве первое слагаемое в левой части делится на ab , т.к. sx делится на b . По той же причине второе слагаемое делится на ab . Значит, и c , как их сумма делится на ab .
- (2) Пусть b делит ac ; тогда b делит и первое, и второе слагаемое в левой части предыдущего равенства, то есть $b \mid c$.
- (3) Запишем все равенства вида $ax_i + b_i y_i = 1$ и перемножим. Мы получим равенство вида $aX + (b_1 \dots b_k)(y_1 \dots y_k) = 1$, где X — некоторое целое число. Но это и значит, что 1 линейно выражается через a и $b_1 \dots b_k$, то есть они взаимно просты.

□

Замечание 1.8. В школьном курсе утверждения наподобие предыдущих обычно доказывают с помощью основной теоремы арифметики о единственности разложения числа на простые, которую сообщают без доказательства. Обратите внимание, что мы ей здесь не пользовались; напротив, в следующем разделе мы выведем основную теорему арифметики из леммы 1.7. Но для этого сперва дадим определение простого числа.

1.4. Простые числа и основная теорема арифметики.

Определение 1.9. Число $p \in \mathbb{Z}$, отличное от 0 и ± 1 , называется *простым*, если для любого представления $p = ab$ верно, что либо $a = \pm 1$, либо $b = \pm 1$.

Из определения следует, что $\{\pm 1, \pm p\}$ — это все делители простого числа p . Значит, НОД числа p и какого-нибудь другого числа может равняться либо 1, либо p ; то есть всякое число либо делится на p , либо взаимно просто с ним.

Основная теорема арифметики утверждает единственность разложения на простые множители.

Теорема 1.10. Каждое число $a \in \mathbb{Z}$ можно представить в виде произведения простых, причем это представление единственно в следующем смысле: если $a = p_1 \dots p_k = q_1 \dots q_m$, причем p_i, q_j простые, то $k = m$ и после подходящей перенумерации $p_i = q_i$.

Доказательство. Доказательство существования разложения осуществляется индукцией по $|a|$: если число не простое, то его можно представить как $a = bc$, где $|b| < |a|$ и $|c| < |a|$.

Единственность доказывается более сложно. Предположим, что $k \leq m$. Доказываем индукцией по k . База $k = 1$ отвечает случаю, когда $a = p_1$ простое, т.е. очевидна.

Пусть $p_1 \dots p_k = q_1 \dots q_m$. Докажем, что p_1 совпадает с каким-то из q_i . Действительно, если бы это было не так, то $(p_1, q_i) = 1$ для всех i , откуда по лемме 1.7 (3) p_1 взаимно просто с $q_1 \dots q_m$, что противоречит делимости $q_1 \dots q_m$ на p_1 . Значит, найдется $q_i = p_1$. Без ограничения общности положим $i = 1$. Сократив обе части равенства на p_1 , получаем, что $p_2 \dots p_k = q_2 \dots q_m$. По предположению индукции

$k - 1 = m - 1$ (а значит, $k = m$), а p_i равны q_i после подходящей перенумерации. Теорема доказана. $\square$

1.5. «Плохой» пример. Рассмотрим кольцо $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$. Умножение элементов в нем осуществляется по правилу

$$(a + b\sqrt{5})(c + d\sqrt{5}) = ac + 5bd + (bc + ad)\sqrt{5}.$$

В этом кольце нет единственности разложения элементов на множители. Так, например,

$$4 = 2 \cdot 2 = (-1 + \sqrt{5})(1 + \sqrt{5})$$

будет двумя существенно разными разложениями.

Упражнение 1.11. Проверьте это. Для этого покажите, что элементы 2 и $\sqrt{5} \pm 1$ будут простыми (т.е. не могут быть представлены в виде произведения двух необратимых элементов), и что никакие два из них не отличаются умножением на обратимый элемент $\mathbb{Z}[\sqrt{5}]$.