Гимназия 1543, математический спецкурс, 8 В

Занятие 6: отношение делимости (дополнение)

Предпорядки Целые числа можно сравнивать между собой. Говорят, что множество целых чисел являются упорядоченным, а отношение $\leqslant$ задаёт порядок на нём. Перечислим важнейшие свойства этого отношения.

1) Для любого a выполнено $a \leqslant a$; (рефлексивность)

2) Если $a \leqslant b$ и $b \leqslant c$, то $a \leqslant c$; (транзитивность)

3) Если $a \leqslant b$ и $b \leqslant a$, то $a = b$; (симметричность)

4) Для любых a и b истинно хотя бы одно из высказываний $a \leqslant b$ и $b \leqslant a$. (цепная или линейная упорядоченность)

Самые важные из этих свойств — 1 и 2. Отношения, удовлетворяющие только этим двум свойствам, называются *предпорядками*. Для полноты изложения приведём примеры предпорядков, обладающих одним из свойств 3 и 4.

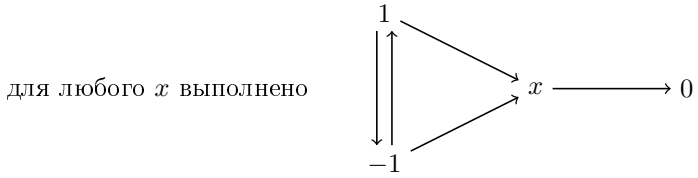
1) Отношение «быть подмножеством» на множестве подмножеств некоторого множества — симметричный, но не цепной предпорядок. (Симметричные предпорядки ещё называются *частичными порядками*.)

2) Отношение «не превышать по абсолютной величине» $a \prec b$ на множестве целых чисел, заданное как $|a| \leqslant |b|$ — цепной, но не симметричный предпорядок.

Часто хочется симметричности. Если её нет, то можно немного облегчить ситуацию, введя понятие *эквивалентных* объектов. Объекты a и b *эквивалентны* относительно предпорядка $\leqslant$, если $a \leqslant b$ и $b \leqslant a$. Мы будем записывать это так: $a \approx b$. Если $a \approx x$, а $b \approx y$, то $a \leqslant b$ тогда и только тогда (в силу транзитивности), когда $x \leqslant y$. Поэтому в неравенствах можно левую или правую часть заменить на эквивалентную, получив при этом неравенство равносильное исходному.

Предпорядок делимости Вспомним важнейшие свойства отношения делимости целых чисел: $a \mid a$ и $a \mid b$, $b \mid c \Rightarrow a \mid c$. Эти свойства — в точности рефлексивность и транзитивность. Поэтому делимость — это предпорядок на множестве целых чисел. Нам будет удобно изображать отношение делимости на диаграммах. Договоримся в случае, если $a \mid b$, проводить стрелку $a \to b$.

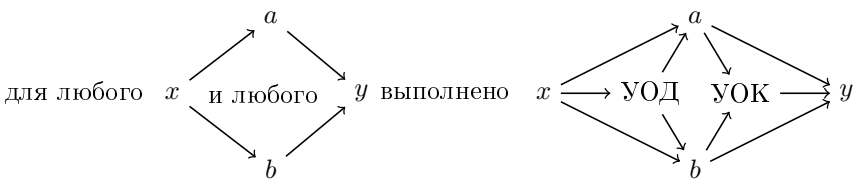
Как устроен предпорядок делимости целых чисел? Сперва заметим, что 0 является наибольшим элементом, а ± 1 — наименьшими:



Чтобы не было путаницы с отношением $\leqslant$, будем называть наименьшие объекты *начальными*, а наибольшие — *конечными* (а и то, и другое вместе — *универсальными*).

Теперь пусть a и b — два целых числа. Рассмотрим всевозможные их общие делители. Начальные среди них — всегда ± 1. Возникает вопрос: а есть ли конечные? Такой же вопрос может возникнуть и про начальное общее кратное (конечное общее кратное всегда равно 0). Как мы выясним несколько позже, для любой пары a и b существуют и конечный общий делитель и начальное общее кратное. Но для начала поймём, зачем нам это может пригодиться. Одна из причин — очень полезная лемма Евклида. Но перед тем, как её сформулировать, дадим два определения.

Определение. *Универсальными* общим делителем и общим кратным (УОД и УОК) будем называть, соответственно, конечный общий делитель и начальное общее кратное.



Определение. Числа a и b называются взаимно простыми, если 1 является их УОД.

Лемма (Евклида)**.** *Пусть a и b взаимно просты и $a \mid bc$. Тогда $a \mid c$.*

Следствие. *Из леммы Евклида следует единственность разложения натурального числа на простые множители.*

Доказательство. Если у числа n есть хотя бы два различных разложения (назовём их α и β) на простые множители, и это — минимальное такое натуральное число, то каждое простое число встречается максимум в одном из α и β (в противном случае равенство $\alpha = \beta$ можно разделить на это простое число и получить, что у меньшего натурального числа есть более одного разложения), а $n > 1$. Пусть p и q — простые, причём $\alpha = pA$, $\beta = qB$. Тогда, так как p и q взаимно просты, а $p \mid qB$, то $p \mid B$. У B же разложение единственно в силу сделанного предположения (и, очевидно, не содержит p). С другой стороны $px = B$, поэтому это разложение может быть получено как произведение p и разложения x. Но p в этом произведении присутствует. Противоречие! $\square$

Чтобы доказать лемму Евклида, нам понадобятся три вспомогательных (но очень важных) утверждения:

1) Пусть фиксирована пара чисел. Тогда все их УОДы эквивалентны между собой (и любое число, эквивалентное их УОД, является их УОД), и все их УОКи тоже эквивалентны между собой (и любое число, эквивалентное их УОК, является их УОК).

2) УОД и УОК существуют у любой пары чисел.

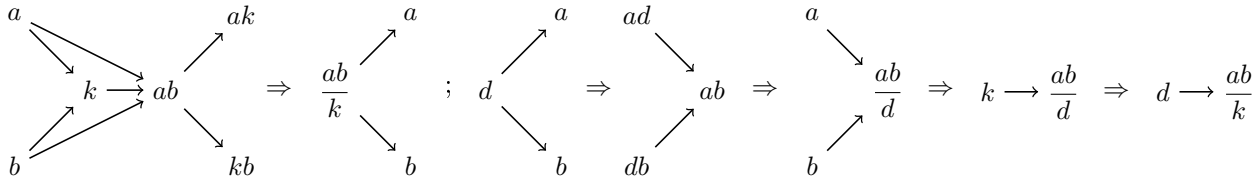
3) Пусть u — УОД чисел a и b, а m — их УОК. Тогда $ab \approx um$.

Первое из этих утверждений сразу следует из определения УОК и УОД. Докажем второе утверждение.

Доказательство. Пусть a и b — пара целых чисел. Если кто-то их них (для определённости, b) равен 0, то единственное их общее кратное — это 0, поэтому в этом случае УОК равен 0. УОД же в таком случае эквивалентны a (т.к. a делится на любой свой делитель).

Если же оба числа не равны 0, то их УОК эквивалентны их НОК. Действительно, пусть $k = \text{НОК}(a, b)$, а x — произвольное общее кратное. Тогда для некоторой пары q, r выполнено $x = kq + r$, где $0 \leqslant r < k$. Осталось заметить, что $r = x - kq$ является общим кратным a и b, меньшим наименьшего положительного. Значит, $r = 0$ и $k \mid x$. В силу произвольности x НОК является УОК.

Чтобы теперь получить УОД, достаточно ab поделить на k. Это легко увидеть из следующей цепочки диаграмм, где d — произвольный общий делитель a и b.

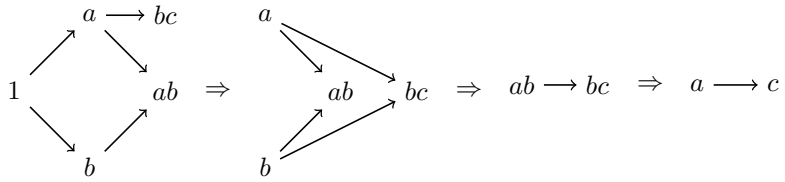


Заметим, что заодно мы доказали и третье утверждение.

□

А теперь вернёмся к лемме Евклида.

Доказательство. Если $b = 0$, то $a = \pm 1$, поэтому $a \mid c$. Если $b \neq 0$, то можно продуктивно воспользоваться тем фактом, что $ab = ab/1$ — это УОК a и b. Действительно, посмотрим на цепочку



Лемма доказана. □