

Элементы теории чисел

Лектор профессор Ю.В. Нестеренко
механико-математический факультет МГУ

1 поток 1 курса, осень 2026г.

Лекция 1: Аксиомы Пеано. Делимость целых чисел.
Наименьшее общее кратное и наибольший общий делитель.

Аксиомы — это исходные положения, которые принимаются без доказательств и служат фундаментом дальнейших рассуждений.

Аксиомы Пеано, 1889: Натуральными числами называются элементы всякого непустого множества, удовлетворяющего пяти аксиомам:

1. 1 является натуральным числом;
2. Для каждого натурального числа a существует единственное **следующее** за a натуральное число, оно будет обозначаться a' ;
3. 1 не следует ни за каким натуральным числом;
4. Если натуральное число a следует как за числом b , так и за числом c , то b и c тождественны.
5. (Аксиома индукции) Если какое-либо предложение доказано для 1 и если из допущения, что оно верно для натурального числа n вытекает, что оно верно для следующего за n натурального числа, то это предложение верно для всех натуральных чисел.

Десятичная запись чисел

Цифры: $0, 1, 2, 3, 4, \dots, 8, 9$.

Символы $1, 2, 3, 4, \dots, 9, 10, 11, \dots, 19, 20, 21, \dots$ называются натуральными числами. Они образуют бесконечную последовательность — натуральный ряд чисел. Это множество принято обозначать буквой $\mathbb{N}$. Позиционная запись чисел.

Двоичная запись чисел

Цифры: $0, 1$.

Числа: $1, 10, 11, 100, 101, 111, 1000, \dots$

Шестнадцатеричная запись чисел

Цифры: $0, 1, 2, 3, 4, \dots, 8, 9, A, B, C, D, E, F$.

Числа: $1, 2, 3, \dots, F, 10, 11, \dots, FF, 100, \dots$

Из аксиом Пеано можно вывести некоторые важные свойства натуральных чисел.

1. Если для элементов каждого из двух множеств имеет место отношение следования, удовлетворяющее аксиомам 1-5, то между элементами этих множеств можно установить взаимно однозначное соответствие, сохраняющее отношение следования. Например $(FF)_{16} = (255)_{10}$.
2. Если некоторое утверждение, формулировка которого зависит от натурального числа n , доказано для числа 1 и в предположении, что оно верно для n , доказано для следующего за n числа, то это утверждение выполняется для любого натурального n .

Сложение натуральных чисел есть операция, сопоставляющая каждой паре натуральных чисел a и b натуральное число, обозначаемое $a + b$ и удовлетворяющее равенствам

$$a + 1 = a', \quad a + b' = (a + b)'.$$

Говорят, что натуральное число a **больше** натурального числа b (или b **меньше** a), если существует натуральное число c удовлетворяющее равенству $a = b + c$. Это отношение обозначается $a > b$ или $b < a$.

3. Каждое непустое подмножество натурального ряда содержит наименьший элемент.
4. Каждое непустое и ограниченное сверху подмножество натурального ряда содержит наибольший элемент.

Умножение есть операция, сопоставляющая каждой паре натуральных чисел a и b натуральное число, обозначаемое $a \cdot b$ и удовлетворяющее равенствам

$$a \cdot 1 = a, \quad a \cdot b' = a \cdot b + a.$$

Если к натуральным числам добавить отрицательные числа и ноль, получится множество целых чисел

$$0, \pm 1, \pm 2, \pm 3, \pm 4, \dots$$

Это множество принято обозначать буквой $\mathbb{Z}$.

Доказательства указанных здесь свойств, а также многих других можно найти в книге Э.Ландау "Основания анализа русский перевод опубликован в 1947 году. Там же строятся рациональные, действительные и комплексные числа, описываются и доказываются их свойства.

Глава 1. О делимости чисел

§1.1. Делимость целых чисел

Определим важное понятие делимости чисел.

Определение 1

Говорят, что целое число a делится на целое число $b \neq 0$, если найдется целое число c , удовлетворяющее равенству

$$a = b \cdot c.$$

Например,

- число 111 делится на 37, т.к. $111 = 37 \cdot 3$;
- число 28 делится на -4 , т.к. $28 = (-4) \cdot (-7)$;
- число 5 не делится на 3. В противном случае $5 - 3 = 2$ должно делиться на 3. Но это невозможно, так как $0 < 2 < 3$,

Глава 1. О делимости чисел. Свойства делимости целых чисел

Если целое число a делится на целое число b , то b — делитель, a — делимое, c — частное.

Обозначения: $b|a$ или $a:b$, а если целое число a не делится на b , то $b \nmid a$.

Ноль делится на любое целое число $a \neq 0$.

Лемма 1 (Свойства делимости)

Пусть a, b, c — целые числа.

1. Имеем $1|a$.
2. Если $a \neq 0$, то $a|a$.
3. Если $a|b$, то $a|bc$.
4. Если $a|b$ и $b|c$, то $a|c$.
5. Если $a|b$ и $a|c$, то $a|(b+c)$ и $a|(b-c)$.
6. Если $a|b$ и $b \neq 0$, то $|a| \leq |b|$.

Теорема 1 (Теорема о делении с остатком)

Для любых $a \in \mathbb{Z}$ и $b \in \mathbb{N}$ существуют единственным образом определённые целые числа q, r , с условиями

$$a = bq + r, \quad 0 \leq r < b. \quad (1)$$

Доказательство.

При $a = 1$ условия (1) выполняются с $q = 1$ и $r = 0$, если $b = 1$, и с $q = 0$, $r = 1$ при $b > 1$.

- Предположим, что первое утверждение теоремы выполняется для натурального числа $a = n$ с некоторыми целыми числами q, r , удовлетворяющими условиям (1). Тогда $n + 1 = bq + r + 1$.
- Если $r = b - 1$, то $n + 1 = b(q + 1)$ и (1) имеет место с $q_1 = q + 1$ вместо q и $r_1 = 0$ вместо r .
- Если же $r < b - 1$, то (1) для $n + 1$ имеет место с $q_1 = q$ и $r_1 = r + 1$ вместо r .
- С помощью аксиомы индукции утверждаем, что для любого $a \in \mathbb{N}$ с некоторыми $q, r \in \mathbb{Z}$ выполняется (1). □

Продолжение доказательства теоремы 1

При $a = 0$ утверждение теоремы будет выполняться для $q = 0$ и $r = 0$.

Осталось рассмотреть случай $a < 0$. Из этого неравенства следует условие $-a + b - 1 > 0$, так что по доказанному с некоторыми целыми числами u, v имеем

$$-a + b - 1 = ub + v, \quad 0 \leq v < b.$$

Из последнего равенства находим $a = (-u)b + b - 1 - v$ и значит с числами $q = -u$ и $r = b - 1 - v$, поскольку $0 \leq v \leq b - 1$, получаем утверждение теоремы. Итак, существование чисел q и r доказано во всех возможных случаях.

Продолжение доказательства теоремы 1

Допустим теперь, что вместе с парой чисел (q, r) , удовлетворяющих условиям (1), существует ещё одна, отличная от неё пара чисел (u, v) , для которой

$$a = bu + v, \quad 0 \leq v < b. \quad (2)$$

Из равенств (1) и (2) следует $bq + r = bu + v$. Поэтому $r - v = b(u - q)$, так что $b|(r - v)$. Из неравенств (1) и (2) находим также $|r - v| < b$. Согласно последнему свойству леммы 1 можно утверждать теперь, что $r - v = 0$, т.е. $v = r$.

Но тогда $b(u - q) = 0$ и, значит, $u = q$. Получаем, что пары (q, r) и (u, v) должны совпадать, вопреки нашему предположению. Это противоречие завершает доказательство теоремы 1.

Числа r и q , определенные в теореме 1, называются *остатком от деления* числа a на b и *неполным частным* при делении a на b . В случае $r = 0$ слово "неполное" в названии q опускают.

Например, справедливо равенство

$$-1234 = 23 \cdot (-54) + 8.$$

Можно сказать, что остаток от деления числа -1234 на 23 равен 8 , а неполное частное равно -54 .

Из доказательства теоремы 1 следует, что целое число a делится на натуральное b в том и только том случае, когда соответствующий остаток равен нулю.

Числа, делящиеся на 2 , называются *четными*, числа, не делящиеся на 2 , т.е. имеющие при делении на 2 остаток 1 , называются *нечетными*.

Для нахождения остатка и неполного частного можно использовать так называемый алгоритм *деления столбиком*.

§1.2. Наименьшее общее кратное и наибольший общий делитель

Пусть $a_1, \dots, a_n$ – ненулевые целые числа. Целое число K называется *общим кратным* чисел $a_1, \dots, a_n$, если оно кратно каждому из этих чисел, т.е. $a_1|K, \dots, a_n|K$.

Например, $|a_1 \cdots a_n|$ есть одно из их общих кратных.

Определение 2

Самое маленькое из положительных чисел, делящихся на каждое из чисел $a_1, \dots, a_n$ называется их наименьшим общим кратным.

Наименьшее общее кратное чисел $a_1, \dots, a_n$ будет обозначаться символом **НОК**($a_1, \dots, a_n$) или $[a_1, \dots, a_n]$.

Теорема 2

Любое общее кратное нескольких чисел делится на их наименьшее общее кратное.

Доказательство.

Пусть $m = [a_1, \dots, a_n]$ и K - какое-нибудь общее кратное чисел $a_1, \dots, a_n$. Разделив с остатком число K на m , получим целые q, r , удовлетворяющие условиям

$$K = mq + r, \quad 0 \leq r < m.$$

Из свойств делимости находим, что $r = K - mq$ делится на каждое из целых чисел a_j и потому есть общее кратное чисел $a_1, \dots, a_n$. Учитывая, что m есть наименьшее из положительных общих кратных, приходим к заключению, что неравенство $r > 0$ невозможно. Поэтому $r = 0$ и $m|K$. Теорема доказана. □

Множество всех делителей целого отличного от нуля числа a конечно. Действительно, если $d|a$, то, согласно последнему свойству из леммы 1, выполняется неравенство $|d| \leq |a|$.

Пусть $a_1, a_2, \dots, a_n$ – целые числа и $d \in \mathbb{Z}$ – их *общий делитель*, т.е. $d|a_1, d|a_2, \dots, d|a_n$. Из сказанного выше следует, что если среди чисел $a_1, a_2, \dots, a_n$ есть не равное нулю, то множество общих делителей этих чисел конечно.

Оно всегда содержит ± 1 и потому не пусто. Говоря в дальнейшем об общих делителях мы, даже если это не оговаривается особо, всегда будем подразумевать, что в соответствующем наборе $a_1, a_2, \dots, a_n$ содержится хотя бы одно не равное нулю число.

Определение 3

Самое большое положительное число, делящее каждое из чисел $a_1, \dots, a_n$ называется их наибольшим общим делителем.

Целые числа называются взаимно простыми, если их наибольший общий делитель равен 1.

Найдем, например, все общие делители чисел 6, 10, 15. Они содержатся среди делителей 6, т.е. среди чисел $\pm 1, \pm 2, \pm 3, \pm 6$. Учитывая, что $15 = 2 \cdot 7 + 1$ не делится на 2, а, значит, не делится и на 6, из списка возможных общих делителей следует исключить $\pm 2, \pm 6$. Равенство $10 = 3 \cdot 3 + 1$ означает, что 10 не делится на 3. Поэтому в списке общих делителей остаются лишь числа ± 1 , и потому числа 6, 10, 15 взаимно просты.

Наибольший общий делитель чисел $a_1, a_2, \dots, a_n$ обозначается символом **НОД**($a_1, \dots, a_n$) или просто $(a_1, \dots, a_n)$.

Выведем из теоремы 2 соотношение между наибольшим общим делителем двух чисел и их наименьшим общим кратным.

Следствие 1

Для любых двух натуральных чисел a, b справедливо равенство

$$[a, b] \cdot (a, b) = a \cdot b.$$

Доказательство.

Произведение ab есть общее кратное чисел a и b . Согласно теореме 2 оно делится на их наименьшее общее кратное, т.е. $\frac{ab}{[a, b]}$ есть целое число. Из равенств

$$a = \frac{ab}{[a, b]} \cdot \frac{[a, b]}{b}, \quad b = \frac{ab}{[a, b]} \cdot \frac{[a, b]}{a}$$

следует, что $\frac{ab}{[a, b]}$ есть общий делитель чисел a и b . □

Продолжение доказательства следствия 1

Пусть теперь d – произвольный общий делитель a и b . В силу равенств

$$\frac{ab}{d} = a \cdot \frac{b}{d} = b \cdot \frac{a}{d}$$

закключаем, что $\frac{ab}{d}$ есть общее кратное чисел a и b . По теореме 2 оно делится на $[a, b]$, т.е. отношение $\frac{ab}{d \cdot [a, b]}$ есть положительное целое число. Поэтому $\frac{ab}{d \cdot [a, b]} \geq 1$ и $\frac{ab}{[a, b]} \geq d$. Следовательно, $\frac{ab}{[a, b]}$ – наибольший из всех общих делителей чисел a и b . Это завершает доказательство следствия.

Следствие 2

Если $a|bc$ и $(a, b) = 1$, то c делится на a .

Доказательство.

Произведение bc есть общее кратное чисел b и a . По теореме 2 оно делится на $[a, b]$. Согласно условию и следствию 1 заключаем $[a, b] = ab$, так что $ab|bc$ и, значит, $a|c$. □

Теорема 3

1. Если $a_1, \dots, a_n$ – натуральные числа и $d_1, \dots, d_m$ – все их положительные общие делители, то $(a_1, \dots, a_n) = [d_1, \dots, d_m]$.
2. Наибольший общий делитель нескольких чисел делится на любой их общий делитель.

Доказательство.

- Каждое из чисел a_k есть общее кратное всех делителей $d_1, \dots, d_m$. По теореме 2 можно утверждать, что $d = [d_1, \dots, d_m] | a_k$. Так как это верно при любом индексе k , заключаем, что **d есть общий делитель чисел $a_1, \dots, a_n$.**
- Согласно определению число d есть общее кратное всех d_k , т.е. при любом k имеем $d_k | d$. Поэтому $d_k \leq d$ и **d есть наибольший общий делитель чисел $a_1, \dots, a_n$.** Первое утверждение доказано.
- Далее $a_1, \dots, a_n$ – числа из второго утверждения. Согласно первому утверждению и доказанной делимости $d_k | d$, $1 \leq k \leq m$, находим $d_k | d = [d_1, \dots, d_m] = (a_1, \dots, a_n)$. Теорема доказана. □

Литература Годаются любые издания указанных ниже книг.

1. Виноградов И.М., Основы теории чисел.
2. Бухштаб А.А., Теория чисел.
3. Нестеренко Ю.В., Теория чисел.
4. Ландау Э., Основания анализа.

Конец 1-й лекции