- Тема №1 -

Основы элементарной теории чисел

Что такое теория чисел

Теория чисел — раздел математики, занимающийся изучением чисел непосредственно как таковых, их свойств и поведения в различных ситуациях**.** Упаси Боже давать здесь точное определение понятия "Теория чисел", так какдаже если Вы поместите рядом двух учёных-профессионалов, работающих, по их мнению, в теории чисел, то они могут подраться между собой, так и не придя к единому мнению из чего же состоит "Теория чисел".

В головах многих математиков, как профессионалов, так и любителей, паразитирует мнение, что теория чисел — это наиболее абстрактная и отдаленная от практических применений математическая теория, пусть красивая и стройная сама по себе, но совершенно бесполезная с точки зрения народного хозяйства.

Более того, некоторые теоретики-числовики даже гордятся такой точкой зрения, считая себя богемными представителями "чистого искусства", которое неприменимо, например, для создания атомной бомбы или чего-нибудь еще в этом роде. Они задирают нос, освобождают себя от моральных страданий Эйнштейна, они творят красоту и только красоту, выше которой идет мудрость уже божественная, океан слепящего, непостижимого света.Бедолаги. Их богемность разбивается уже фразой Пифагора "Все есть число!"и, изучая числа, они неизбежно изучают окружающий нас мир, и себя в том числе (каламбур). Но кроме этого философского замечания о практической применимости "чистой" теории чисел, она не просто красивейшая и стройнейшая область чистой науки, но и серьезная народно-хозяйственная структура.

В **элементарной теории чисел** целые числа изучаются без использования методов других разделов математики. Такие вопросы, как делимость целых чисел, алгоритм Евклида для вычисления наибольшего общего делителя и наименьшего общего кратного, разложение числа на простые множители, построение магических квадратов, совершенные числа, числа Фибоначчи, малая теорема Ферма, теорема Эйлера, задача о четырёх кубах относятся к этому разделу.

Кванторы в математике, некоторая математическая символика

Определение. Кванторы (от лат. quantum - сколько) - в логике и математике - логические эквиваленты слов "все", "каждый" и т. п. (кванторы общности), "некоторый", "существует" (кванторы существования) и др.; заменяют выражений, часто используемые в математике.

$\exists$	«существует», «для некоторого…» *квантор существования*
$\nexists$	«не существует»
$\forall$	«любой», «для любого» *квантор общности*
!	«единственный», «один» *квантор единственности*
$\exists!$	«существует единственный»
$\in$	«принадлежит»
$\notin$	«не принадлежит»

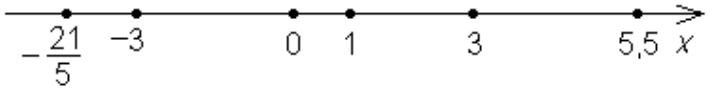
$\subset$	«содержится» (о множествах)
$\wedge$	«и»
$\vee$	«или»
=>	«следует, следовательно», *следствие*
<=>	«тогда и только тогда, когда», *равносильный переход*

Множества чисел

На протяжении курса элементарной алгебры несколько раз происходит обогащение запаса чисел. Знакомство школьника с натуральными, положительными целыми и дробными числами происходит еще в начальной школе – при изучении арифметики. Алгебра начинается по существу с введения отрицательных чисел, то есть появляется множество ***Z*** целых чисел. Затем вводится в рассмотрение множество ***Q*** рациональных чисел, состоящее из всех целых и всех дробных чисел, как положительных, так и отрицательных. Дальнейшее расширение запаса чисел происходит тогда, когда появляются иррациональные числа. Множество ***R***, состоящее из всех рациональных и всех иррациональных чисел, называется множеством действительных (или вещественных) чисел. А вот почти в конце курса элементарной алгебры, возникнет необходимость дальнейшего расширения множества ***R*** действительных чисел до множества ***C*** комплексных чисел.

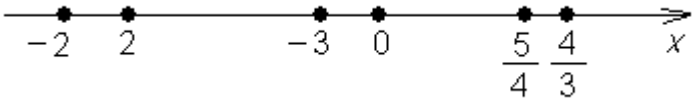
Обозначение	Определение	Примеры
N	**Натуральные числа** - числа, которые используются при счете предметов.	1, 2, 3, 4 … 10, 11, … 525, 526, … 3679, 3680, …$\in N$
Z	**Целые числа** – натуральные числа, противоположные им числа и ноль.	…, -3489, …, -500, …, -2, -1, 0, 1, 2, …, 500, … 3489, ...$\in Z$
Q	**Рациональные числа –** числа вида $\frac{p}{q}$, где p – целое число, q – натуральное число, или вида конечной или бесконечной периодической десятичной дроби. Числа, не являющиеся рациональными - **иррациональные.**	$\frac{1}{5}; \frac{2}{3}; \frac{6}{7}; \frac{-5}{9}; -4 = \frac{-4}{1};$ $0{,}5;\ 1{,}3;\ \frac{1}{3} = 0{,}(3) \in Q$
R	Все **действительные числа**: ***N, Z, Q***вместе.	Все предыдущие примеры $\in R$
C	**Комплексные числа**, с которыми вы познакомитесь в старших классах или университете.	5+4i, 2-7i, гдеi – мнимая-единица

Задание 1. На координатной прямой изображены несколько чисел. Какие из этих чисел являются натуральными, целыми, рациональными, положительными, отрицательными, противоположными.



натуральные	целые	рациональные	положительные	отрицательные	противоположные

Задание 2. Проверьте, правильно ли расположены числа на координатной прямой? Сравните эти числа между собой. Расположите данные числа правильно.



Свойства действительных чисел и арифметических операций

Действительные числа обладают **свойствами:**

1) Для любых действительных чисел a и b имеет место и притом только одно из соотношений:
$$a = b,\ a<b,\ a>b.$$
2) Для любых действительных чисел a и b таких, что $a<b$, найдется такое действительное число c, что $a<c$ и $c<b$, то есть $a<c<b$.
3) Если $a<b$ и $b<c$, то $a<c$ (свойство транзитивности неравенств).
4) Если $a<b$, то $a+c<b+c$ для любого действительного числа c.
5) Если $a<b$ и c – положительное число, то $a\cdot c<b\cdot c$.

Для любых действительных чисел справедливы **равенства:**

1) $a+b=b+a$, $a\cdot b=b\cdot a$ - переместительный закон;
2) $a+(b+c)=(b+a)+c$, $a(bc)=(ab)c$ - сочетательный закон;
3) $a(b+c)=ab+ac$ - распределительный закон;
4) $a+0=a$; $a-0=a$; $a-a=0$;
5) $a\cdot 0=0$; $a\cdot 1=a$;
6) $-a=(-1)\cdot a$;
7) $\frac{0}{a}=0$; $\frac{a}{a}=1$, $(a\neq 0)$; $\frac{a}{1}=a$;
8) $\frac{a}{0}$ - решений нет, на нуль делить нельзя!
9) $a\cdot\frac{1}{a}=1\ (a\neq 0)$;
10) $a\cdot\frac{1}{b}=\frac{a}{b}\ (b\neq 0)$.

Вычитание отрицательного числа состоит в том, что данное вычитание заменяется сложением с противоположным числом.

Примеры: $16-(-3)=16+3=19$; $-14{,}5-(-2{,}7)=-14{,}5+2{,}7=-11{,}8$.

Умножение и деление чисел с одинаковыми знаками состоит в том, что значение данного выражения имеет знак плюс, а его модуль получают соответственно умножением или делением

модулей.Умножение и деление чисел с разными знаками состоит в том, что значение данного выражения имеет знак минус, а его модуль получают соответственно умножением или делением.

Задание 3. Вычислите, не пользуясь калькулятором

1) $724:4-4\cdot 41+1=?$ 2) $53\cdot(42+24:6)-2315=?$ 3) $57\cdot 79-57\cdot 69+10\cdot 43=?$

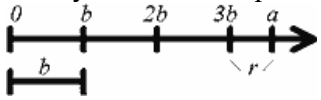
Деление с остатком

Определение. Пусть $a, b \in \mathbf{Z}$. Число a **делится на число** b, если найдется такое число $q \in \mathbf{Z}$, что $a = qb$. Синонимы: a кратно b; b — делитель a. Запись: $a \vdots b$ или $b \mid a$.

Легко проверяется также следующее **свойство**:пусть $a_1+a_2+...+a_n = c_1+c_2+...+c_k$ – равенство сумм целых чисел. Если все слагаемые в этом равенстве, кроме одного, кратны b, то и оставшееся слагаемое обязано быть кратным b.

Теорема. Для данного целого числа b, всякое целое число a единственным образом представимо в виде $a = bq + r$, где $0 \le r < |b|$.

♦**Доказательство.** Ясно, что одно представление числа a равенством $a = bq + r$ мы получим, если возьмем bq равным наибольшему кратному числа b, не превосходящему a (см. рис.)



(Здесь $a = 3b+r$)

Тогда, очевидно, $0 \le r < |b|$. Докажем единственность такого представления. Ну пусть $a = bq + r$ и $a = bq_1 + r_1$ — два таких представления. Значит $0 = a - a = b(q - q_1) + (r - r_1)$. Здесь 0 делится на b; $b(q - q_1)$ делится на b, следовательно $(r - r_1)$ обязано делиться на b. Так как $0 \le r < |b|$ и $0 \le r_1 < |b|$, то $r - r_1 < b$ и $r - r_1$ делится на b, значит $r - r_1$ равно нулю, а, значит и $q - q_1$ равно нулю, т. е. два таких представления совпадают. ♦

Определение. Число q называется **неполным частным**, а число r — **остатком от деления** a на b.

Идея рисунка, поясняющего доказательство теоремы, принадлежит древним грекам, которые, впрочем, не знали, что они древние. Именно древние греки, почему-то, очень любили многократно укладывать один отрезок в другой, а оставшуюся часть большего отрезка, естественно, называли "остатком".

Заметим, что остаток — всегда есть число неотрицательное, а вот неполное частное может быть каким угодно целым числом. Поэтому на вопрос: "Сколько будет минус пять поделить на три с остатком?", каждый должен бойко отвечать: "Минус два, в остатке — один!". Разберемся на примерах.

Примеры.

1) Разделим 5 на 2: →5= 2·2+1, где 1 – остаток;

2) Другое дело с отрицательными числами. Разделим -10 на 3: →

Сначала разделим 10 на 3. То есть, 10 = 3·3 + 1. Разделим на (-1).

-10 =3·(-3) - 1, но остаток должен быть нулевым или положительным. Тогда преобразуем:

-10 = 3·(-3) - 3 +2 = 3·(- 3 - 1) + 2 = 3·(-4) + 2. Здесь (-4) - неполное частное, а 2 - остаток.

3) Разделим (-23) на 5. Сначала: 23 = 5·4 + 3 → -23 = 5·(-4) - 3.

-23 = 5·(-4) - 5 +2 = 5·(-5) +2. Т.е., неполное частное - (-5), остаток - 2.

4) Разделим 41 на (-7). Сначала: 41 = 7·5 + 6 →41 = (-7)·(-5) +6. Здесь с остатком все в порядке!

5) Разделим с остатком (-189) на (-3). Так как 189 = 3·63, то -189 = (-3)·63. Здесь остаток - нулевой.

Здесь обозначение $|b|$ называется **модулем числа** b ***(см. далее).*** Запомните пока, что это - всегда положительное число. То есть, если $b < 0$, то минус «убирается».

Признаки делимости нацело чисел

- Число делится **на 2** тогда и только тогда, когда последняя цифра делится на2 (то есть чётная);
- Число делится **на 3** тогда и только тогда, когда сумма цифр делится на 3;
- Число делится **на 4** тогда и только тогда, когда его две последние цифрынули или образуют число, делящееся на 4;
- Число делится **на 5** тогда и только тогда, когда последняя цифра делится на5 (то есть равна 0 или 5);
- Число делится **на 6** тогда и только тогда, когда оно делится на 2 и на 3;
- Число делится **на 7** тогда и только тогда, когда результат вычитанияудвоенной последней цифры из этого числа без последней цифры делитсяна 7 (например, 364 делится на 7, так как $36 - 2 \cdot 4 = 28$ делится на 7);
- Число делится **на 8** тогда и только тогда, когда его три последние цифрынули или образуют число, делящееся на 8;
- Число делится **на 9** тогда и только тогда, когда сумма цифр делится на 9;
- Число делится **на 10** тогда и только тогда, когда последняя цифра — ноль;
- Число делится **на 11**, если у него сумма цифр, занимающих четные места,либо равна сумме цифр, занимающих нечетные места, либо отличается отнее на число, делящееся на 11;
- Число делится **на 12** тогда и только тогда, когда оно делится на 3 и на 4;
- Число делится **на 13** тогда и только тогда, когда результат вычитанияпоследней цифры умноженной на 9 из этого числа без последней цифрыделится на 13 (например, 858 делится на 13, так как $85 - 9 \cdot 8 = 13$ делится на13);
- Число делится **на 14** тогда и только тогда, когда оно делится на 2 и на 7;
- Число делится **на 15** тогда и только тогда, когда оно делится на 3 и на 5;
- Число делится **на 19** тогда и только тогда, когда число его десятков,сложенное с удвоенным числом единиц, кратно 19 (например, 646 делитсяна 19, так как $64 + 6 \cdot 2 = 76$ делится на 19);
- Число делится **на 25** тогда и только тогда, когда две последние цифрыделятся на 25.

Наибольший общий делитель

Определение. Число $d \in \boldsymbol{Z}$, делящее одновременно числа $a, b, c, \ldots, k \in \boldsymbol{Z}$, называется **общим делителем** этих чисел. Наибольшее d с таким свойством называется **наибольшим общим делителем (НОД)**. Обозначение: $d = (a, b, c, \ldots, k)$ или *НОД (a,b,c…).*

Пример: НОД (20, 40) = 20.

Свойства:

1) Если $НОД\ (a, b) = d$, то найдутся такие целые числа u и v, что $d = au + bv$.
2) Для любых целых чисел a и k, очевидно, справедливо: $НОД\ (a, ka) = a$; $НОД\ (1, a) = 1$.
3) Если $a = bq + c$, то совокупность общих делителей a и b совпадает с совокупностью общих делителей b и c, в частности, $НОД\ (a, b) = НОД\ (b, c)$.
4) Пусть a, b и m - произвольные целые числа. Тогда$НОД(am, bm) = m\ НОД(a, b)$.
5) Пусть s - делитель a иb. Тогда $НОД\ (a / s, b / s) = НОД\ (a, b)/s$.
6) Очевидно теперь, что $\text{НОД}\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$.
7) Если $НОД\ (a, b) = 1$, то $НОД\ (ac, b) = (c, b)$.

Наименьшее общее кратное

Определение.Наименьшее общее кратное (НОК) двух целых чисел m и n есть наименьшее натуральное число, **которое** делится на m и n. Обозначение: $c=[a,b]$ *или НОК (a,b).*

Пример: НОК(16, 20) = 80.

$$НОД\ (a, b) \cdot НОК\ (a, b) = a \cdot b$$
$$НОД\ (a, b) = a \cdot b : НОК\ (a, b)$$
$$НОК\ (a, b) = a \cdot b : НОД\ (a, b)$$

Пример. Вычислим НОК (83, 90). Очевидно, что НОД (83, 90) = 1, тогда НОК (83, 90) = 83 · 90 : 1 = 7470.

Степень числа с натуральным показателем

Определение. Степень числа *a* с натуральным показателем – это произведение *n* множителей, каждый из которых равен *a* , т.е.

$$a^n = \underbrace{a \cdot a \cdot a \cdot \ldots \cdot a}_{n \text{ раз}}$$

a^n- степень, *a* - основание степени, *n*- показатель степени.

Свойства (a≠0, b≠0, m и n – произвольные целые числа):

1) $a^1 = a$.
2) $a^m a^n a^k = a^{m+n+k}$
3) $a^m : a^n = a^{m-n}$
4) $(a^m)^n = a^{mn}$
5) $(a \cdot b)^m = a^m \cdot b^m$
6) $(\frac{a}{b})^m = \frac{a^m}{b^m}$

Простые и составные числа

Определение. Простым числом называют натуральное число, которое больше 1 и делится только на 1 и на себя. Непростые натуральные числа, большие 1, называют **составными**.

Пример. 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47 … - простые.

Все простые числа невозможно выписать, так как их бесконечно много. Любой список простых чисел можно пополнить еще одним простым числом, отличным от этих чисел. Этот факт доказал древнегреческий ученый Эвклид (IIIв. до н.э.).

Таким образом, ***N*** **=** *(простые числа)+(составные числа)+1.*

Великий математик Леонард Эйлер нашел формулу простого числа $P = n^2 – n + 41$, при подстановке в которую вместо n любого числа от 1 до 40 получается простое число.

Определение. Целые числа a и b называются **взаимно простыми**, если НОД (a , b) = 1.

Основная теорема арифметики

Определение. Если делитель – простое число, то его называют **простым делителем.**

Примеры.

$28 = 2^2 \cdot 7$
$22 = 2 \cdot 11$ **- разложения на простые множите-**
$81 = 3^4$ ***ли***
$100 = 2^2 \cdot 5^2$

Разложить данное натуральное число на простые множители – это значит представить его как произведение различных его простых делителей, взятых в соответствующих степенях. Этот процесс называется **факторизацией**.

Теорема. Каждое натуральное число можно разложить на простые множители. Такое разложение единственно для каждого натурального числа, то есть, нет других простых делителей и его простые делители нельзя записать в других степенях.

Факториал числа

Факториал числа — это произведение всех натуральных чисел до этого числа включительно.

Обозначается с восклицательным знаком в конце.

$$n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot \ldots \cdot (n-2) \cdot (n-1) \cdot n$$

Случай 0! определен и имеет значение 0!=1, соответствующее комбинаторной интерпретации комбинации нуля объектов, другими словами, есть единственная комбинация нуля элементов, а именно: пустое множество.

Ниже приведены значения факториалов от 0 до 10.

$0! = 1$
$1! = 1$
$2! = 1 \cdot 2 = 2$
$3! = 1 \cdot 2 \cdot 3 = 6$
$4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$
$5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$
$6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720$
$7! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 = 5040$
$8! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 = 40320$
$9! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 = 362880$
$10! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 = 3628800$

Свойство факториала:

$$(n + 1)! = (n + 1) \cdot n!$$

Например:

$(5 + 1)! = (5 + 1) \cdot 5!$

Действительно

$6! = (1 \cdot 2 \cdot 3 \cdot 4 \cdot 5) \cdot 6 = 720$

А значение $(1 \cdot 2 \cdot 3 \cdot 4 \cdot 5) = 5! = 120$

Обратите внимание, что факториал числа ***n*** - это произведение всех натуральных чисел от 1 до ***n***. То есть ***n!=1*2*3*...*(n-1)*n***.

Пример. На что оканчивается число 56! ?

В разложении числа 56! на множители есть соответственно числа 10, 20, 30, 40, 50. А это означает, что в произведении их окажутся числа, оканчивающиеся на нули (ведь так гласит признак делимости на 10). Таким образом, 56! будет оканчиваться на нули и последняя цифра - это нуль.

Такие задачки и задаются, когда факториал оканчивается на нули, потому что факториалы, которые не оканчиваются на нули - это 1!, 2!, 3!, 4! и все, так как далее 5!=120 (произведение 5 и 2 дают 10).

Алгоритм Евклида

Слово "**алгоритм**" является русской транскрипцией латинизированного имени выдающегося арабского математика ал-Хорезми Абу Абдуллы Мухаммеда ибн ал-Маджуси (787 - ок.850) и означает в современном смысле некоторые правила, список инструкций или команд, выполняя которые, некто (быть может, тупой, но усердный) достигнет требуемого результата. В этом пункте будет представлен алгоритм, позволяющий по заданным натуральным числам a и b находить их наибольший общий делитель. Считается, что этот алгоритм придумал самый влиятельный математик всех времен и народов - Евклид, он изложен в IX книге его знаменитых "Начал".

Итак, пусть даны два числа a и b ; a i 0, b i 0, считаем, что a > b . Символом := в записи алгоритма обозначаем присваивание. **Алгоритм**:

1. Ввести a и b .
2. Если b = 0 , то Ответ: a. Конец.
3. Заменить r := "остаток от деления a на b ", a := b , b := r .
4. Идти на 2.

Внимательное разглядывание и пошаговое выполнение алгоритма Евклида убеждают в его, выражаясь словами иконописца Феофана Грека, "простоте без пестроты". Я очень сожалею, что в тексте невозможно проиллюстрировать работу алгоритма на греческий лад - греки стирали отрезки, нарисованные на песке.

В современной буквенной записи, кочующей из одного учебника в другой, алгоритм Евклида выглядит так: $a > b;\ a, b \in \mathbf{Z}$.

$$
\begin{aligned}
a &= bq_1 + r_1 && 0 \le r_1 < b \\
b &= r_1 q_2 + r_2 && 0 \le r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3 && 0 \le r_3 < r_2 \\
&\cdots\cdots \\
r_{n-2} &= r_{n-1} q_n + r_n && 0 \le r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1} && r_{n+1} = 0
\end{aligned}
$$

Пример. Пусть $a = 525$, $b = 231$. Отдадим эти числа на растерзание алгоритму Евклида: (ниже приводится запись деления уголком, и каждый раз то, что было в уголке, т.е. делитель, приписывается к остатку от деления с левой стороны, а остаток, как новый делитель, берется в уголок).

```
                525 | 231
              – 462 | 2
                231 | 63
              – 189 | 3
                 63 | 42
              –  42 | 1
                 42 | 21
              –  42 | 2
                  0
```

Запись того же самого в виде цепочки равенств:

$$
\begin{aligned}
525 &= 231 \cdot 2 + 63 \\
231 &= 63 \cdot 3 + 42 \\
63 &= 42 \cdot 1 + 21 \\
42 &= 21 \cdot 2
\end{aligned}
$$

Таким образом, (525, 231) = 21. Линейное представление наибольшего общего делителя:

$$21 = 63 - 42 \cdot 1 = 63 - (231 - 63 \cdot 3) \cdot 1 =$$
$$= 525 - 231 \cdot 2 - (231 - (525 - 231 \cdot 2) \cdot 3) =$$
$$= 525 \cdot 4 - 231 \cdot 9,$$

и наши пресловутые u и v из $\mathbf{Z}$ равны, соответственно, 4 и - 9.