Математика 2-й семестр, 10-й класс

Ученики 10-4 класса Оконешников Д.Д. и Паньков М.А. по лекциям Протопоповой Т.В.

Для внутреннего использования

Россия, г. Новосибирск
СУНЦ НГУ
2021

Содержание

Элементы теории чисел. Теория сравнений.

Ученик 10-4 класса Оконешников Д.Д. по лекции к.ф.-м.н. Протопоповой Т.В.

от 12 января 2021 г.

1 Лекция №12

Определение. $a \in Z$ и $b \in Z \backslash \{0\}$ определена операция деления с остатком: разделить целое a на целое b $(\neq 0)$ с остатком, означает найти такие целые $q,\ r \in Z$, что $a = b * q + r,\ 0 \leq r < |b|$.

Определение. Если при делении с остатком $r = 0$, то число a делится на b ($a \vdots b$). Число b при этом называется делителем числа a.

Пример. -7 на 5 $\qquad -7 = 5 * (-2) + 3$

1.1 Свойства делимости (нацело). ОТА

(1) Если $a \vdots c$ и $b \vdots c$, то $(a \pm b) \vdots c$

$\uparrow \begin{matrix} a = cq_1 \\ b = cq_2 \end{matrix} \Rightarrow (a \pm b) = c(q_1 \pm q_2) \Rightarrow (a \pm b) \vdots c \downarrow$

(2) $a \vdots b \Rightarrow ak \vdots b$ $(k \in Z)$

(3) $a \vdots b,\ b \vdots c \Rightarrow a \vdots c$

$\uparrow a = bq_1,\ b = cq_2 \Rightarrow a = c * (q_1 * q_2) \Rightarrow a \vdots c \downarrow$

(4) Если $a \neq 0,\ a \vdots b \Rightarrow |a| \geq |b|$

$\uparrow a \vdots b \Leftrightarrow a = b * q \Rightarrow |a| = |b| * |q| \Rightarrow$ от противного, если $|a| < |b|$, то $|q| = \frac{|a|}{|b|} < \frac{|b|}{|b|} = 1 \Rightarrow$ единственная возможность при целом $q = 0$, но тогда и $a = 0$. Противоречие. $\downarrow$

(5) $a \vdots b$ и $b \vdots a \Rightarrow |a| = |b|$

(6) $\forall\ a \in Z \backslash \{0\} \Rightarrow 0 \vdots a$

(7) $\forall\ a \in Z \Rightarrow a \vdots 1$

(8) Если $ab \vdots m$ и НОД$(a,\ m) = 1,$ то $b \vdots m$

(9) Если $a \vdots m,\ a \vdots k$ и НОД$(m,\ k) = 1,$ то $a \vdots mk$

Определение. Натуральное число $p > 1$ называется простым, если оно имеет ровно два натуральных делителя (p и 1).

Все остальные натуральные числа называются составными (кроме 1). Единица не является ни простым, ни составным.

1.1.1 Основная теорема арифметики

Th.1 (Основная теорема арифметики) Всякое натуральное число $n > 1$ может быть представлено в виде $n = p_1 * p_2 * ... * p_i$, где p_i — простые числа. Это представление единственно с точностью до порядка множителей (т.е. если $n = p_1 * p_2 * ... * p_r = q_1 * q_2 * ... * q_s$, то $r = s$ и $q_1,\ q_2, ...,\ q_s$ можно перестановкой получить из чисел $p_1,\ p_2, ...,\ p_r$)

(1) Докажем существование

Пусть $n \in \mathbb{N},\ n > 1$. Среди делителей n есть числа превосходящие 1 (например, само n). Пусть p_1 — наименьший из таких делителей.

p_1 — простое число (если оно само имело бы делитель $1 < a < p_1$, то a было бы меньше p_1 и было бы делителем n (св-ва 4,3), противоречит тому, что выбран наименьший делитель).

Итак, $n = p_1 n_1,$ где p_1 — простое, $n_1 \in \mathbb{N}$ и $n_1 < n$ (св-во 4).

Если $n_1 > 1$, то поступим с ним так же, как и числом n, представим его в виде $n_1 = p_2 n_2$, p_2 — простое, $n_2 \in \mathbb{N}, n_2 < n_1 \Rightarrow n = p_1 * p_2 * n_2$ и т.д.

В конце концов, так как $n_i \in \mathbb{N}, i = 1, 2, 3, ...$ убывают, то $\exists\ n_r = 1$ и процесс обрывается: $n = p_1 * p_2 * ... p_r$

(2) Докажем существование (единственность) От противного. Если $\exists$ хоть одно натуральное число, допускающее два существенно различных разложения, то непременно $\exists$ и наименьшее число с таким свойством:

$$m = p_1 * p_2 * ... * p_r = q_1 * q_2 * ... * q_s \qquad (1)$$

Можем допустить, что $p_1 \le p_2 \le ... \le p_r; q_1 \le q_2 \le ... \le q_s$.

А) Заметим, что $p_1 \ne q_1$.
Если равны, то разделив (1) на $p_1 = q_1$, получили бы два существенно различных разложения на простые множители для числа $< m$ (Противоречие с тем, что m — наименьшее).
На самом деле показали больше: что среди q_j нет чисел равных какому-либо p_i

Б) Из А) $p_1 < q_1$ или $p_1 > q_1$. Пусть $p_1 < q_1$ (для $p_1 > q_1$ доказательство строится аналогично).
Рассмотрим целое число:

$$m' = m - p_1 * q_2 * ... * q_s \qquad (2)$$

Подставляя вместо m два его разложения, получим:

$$m' = p_1 * p_2 * ... * p_r - p_1 * q_2 * ... * q_s = p_1(p_2 * ... * p_r - q_2 * ... * q_s) \qquad (3)$$

$$m' = q_1 * q_2 * ... * q_s - p_1 * q_2 * ... * q_s = (q_1 - p_1)q_2 * ... * q_s \qquad (4)$$

Из равенства (4) очевидно $m' > 0$. Из равенства (2) $m' < m$, а значит, для m' разложение на простые множители — единственно (с точностью до порядка сомножителей).

Из (3) $\Rightarrow p_1$ входит множителем в m', значит, из (4) p_1 входит множителем либо в $q_1 - p_1$, либо в $q_2 * ... * q_s$. Но последнее невозможно, так как все $q_j > p_1$ ($p_1 < q_1$) и они простые.

Значит, p_1 входит множителем в $q_1 - p_1$, т.е. $(\mathbf{q_1} - \mathbf{p_1}) \vdots \mathbf{p_1} \Rightarrow q_1 - p_1 = p_1 h \Rightarrow q_1 = p_1(h+1)$, т.е. $\mathbf{q_1} \vdots \mathbf{p_1}$, чего быть не может. Противоречие. Ч.Т.Д.

1.1.2 Теорема Евклида

Th.2 (Теорема Евклида) Множество простых чисел бесконечно.

$\uparrow$ Доказательство проведем от противного. Предположим, что множество простых чисел конечно, т.е. $P = \{p_1, p_2, ...p_k\}$ — конечная совокупность простых чисел.

Рассмотрим число $p = p_1 * p_2 * ... * p_k + 1$.

Заметим, что $\forall\ i, i = 1, 2, ..., k$ это $p > p_i$, т.е. $p \notin P$, значит, оно составное и по ОТА может быть представлено в виде произведения простых множителей.

Но p не делится ни на какой p_i (при делении дает в остатке 1).

Значит, наше предположение о конечности системы простых чисел неверно. $\downarrow$

Утверждение. Существуют сколь угодно длинные участки натурального ряда, вовсе не содержащие простых чисел

$\uparrow$ Действительно, пусть $n \in \mathbb{N}, n > 1$. Рассмотрим ряд чисел: $n! + 2, n! + 3, ..., n! + n$.

$n = 2 : 2! + 2$ — одно число в ряду;	
$n = 3 : 3! + 2, 3! + 3$ — два числа в ряду;	чем больше n, тем больше в ряду
$n = 4 : 4! + 2, 4! + 3, 4! + 4$ — три числа в ряду;	чисел ($n - 1$ число).
и т.д.	

В этом ряду нет ни одного простого числа, так как $n! + 2$ делится на 2, $n! + 3$ делится на 3, $n! + n$ делится на n. Таким образом, при больших n такие участки натурального ряда могут быть очень большими. $\downarrow$

1.2 Каноническое разложение числа. НОД. НОК

1.2.1 Теорема Эйлера

Th.3 (Теорема Эйлера) Пусть $\tau(n)$ — количество простых чисел $\le n$. Тогда

$$\frac{\tau(n)}{n} \xrightarrow[n \to \infty]{} 0$$

Понятно, что $\tau(n)$ увеличивается (т.е. $\to \infty$) при $n \to \infty$ (это означает, что простые числа встречаются все реже и реже).

Мы показали, что любое натуральное число мы можем представить в виде произведения простых множителей (и такое представление единственно с точностью до перестановки множителей): $n = p_1 * p_2 * ... * p_r,\ p_1 \le p_2 \le ... \le p_r$. Используя обозначение степени, можем записать так:

$$\mathbf{n = p_1^{a_1} * p_2^{a_2} * ... * p_k^{a_k}},\ \text{(каноническое разложение)}$$

$$\text{где } p_1 < p_2 < ... < p_k \text{ — простые, } a_1, a_2, ..., a_k \text{ — натуральные числа.}$$

Замечание. Бывает полезно записать в разложение <u>все</u> простые числа $\le p_k$ и использовать показатель равный 0.

Если число m является делителем n, то несложно понять, что $\mathbf{m = p_1^{\beta_1} * p_2^{\beta_2} * ... * p_k^{\beta_k}}$, где $0 \le \beta_i \le a_i$.

Можно посчитать число всех натуральных делителей числа n. Любой делитель n имеет следующую структуру: $\mathbf{m = p_1^{0,1,2,...,a_1} * p_2^{0,1,...a_2} * ... * p_k^{0,1,...,a_k}}$

Для первого множителя $(a_1 + 1)$ возможность для второго $(a_2 + 1)$ возможностей и т.д. Таким образом, число всех делителей $(a_1 + 1) * (a_2 + 1) * ... * (a_k + 1)$.

Пример. Сколько делителей у числа 120 (включая 1 и само число)?

$$\begin{array}{r|l} 120 & 2 \\ 60 & 2 \\ 30 & 2 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array}$$

$120 = 2^3 * 3^1 * 5^1$. Значит, число всех делителей $= (3 + 1) * (1 + 1) * (1 + 1) = 4 * 2 * 2 = 16$.

Определение. d — общий делитель a и $b \Leftrightarrow \mathbf{a \vdots d}$ и $\mathbf{b \vdots d}$.

Определение. Наибольший общий делитель чисел a и b обозначается НОД(a, b).

Определение. Наименьшее общее кратное НОК$(a, b) = k$ — наименьшее натуральное число такое, что $\mathbf{k \vdots a}$ и $\mathbf{k \vdots b}$.

Пусть $\mathbf{a = p_1^{a_1} * p_2^{a_2} * ... * p_k^{a_k}},\ \mathbf{b = p_1^{\beta_1} * p_2^{\beta_2} * ... * p_k^{\beta_k}}$

Здесь использовали показатель 0 для тех простых множителей, которые входят только в одно из разложений.

Тогда

$$\text{НОД}(a, b) = p_1^{min(a_1,\beta_1)} * p_2^{min(a_2,\beta_2)} * ... * p_k^{min(a_k,\beta_k)}$$
$$\text{НОК}(a, b) = p_1^{max(a_1,\beta_1)} * p_2^{max(a_2,\beta_2)} * ... * p_k^{max(a_k,\beta_k)}$$
$$\text{НОД}(a, b) * \text{НОК}(a, b) = a * b$$

Пример. $a = 2 * 3^3 * 5^2 * 7,\ b = 2^2 * 3 * 7^2 * 11 \Rightarrow a = 2^1 * 3^3 * 5^2 * 7^1 * 11^0,\ b = 2^2 * 3^1 * 5^0 * 7^2 * 11^1 \Rightarrow$ НОД$(a, b) = 2^1 * 3^1 * 5^0 * 7^1 * 11^0$, НОК$(a, b) = 2^2 * 3^3 * 5^2 * 7^2 * 11^1$.

Чтобы получить каноническое разложение полезно помнить признаки делимости.

1) на 2 и 5. Легко.

2) на 4. $n = \overline{a_k a_{k-1} ... a_1 a_0} = 100 * \overline{a_k a_{k-1} ... a_2} + \overline{a_1 a_0}$. $\quad 100 \vdots 4$. $\Rightarrow n \vdots 4 \Leftrightarrow \overline{a_1 a_0} \vdots 4$.

3) на 8. $n \vdots 8 \Leftrightarrow \overline{a_2 a_1 a_0} \vdots 8$.

4) на 3. $n = \overline{a_k a_{k-1} ... a_1 a_0} = a_k 10^k + a_{k-1} 10^{k-1} + ... + a_1 10 + a_0 = a_k(\underbrace{999...9}_{k} + 1) + a_{k-1}(\underbrace{999...9}_{k-1} + 1) + ... + a_1(9 + 1) + a_0 = (a_k \underbrace{999...9}_{k} + a_{k-1} \underbrace{999...9}_{k-1} + ... + a_1 9) + (a_k + a_{k-1} + ... + a_1 + a_0)$

Аналогично для 9.

5) на 6. $n \vdots 2$ и $n \vdots 3 \Rightarrow$ (так как 2 и 3 взаимно просты) $n \vdots 6$

6) на 11.

$$n = \overline{a_k a_{k-1} ... a_1 a_0} = a_0 + a_1 10 + a_2 100 + a_3 + 1000 + ... + a_k 10^k =$$

$$= a_0 + a_1(11-1) + a_2(99+1) + a_3(1001-1) + a_4(9999+1) + a_5(100001-1) + ... + a_k 10^k =$$
$$= (a_0 - a_1 + a_2 - a_3 + a_4 - ...) + (a_1 11 + a_3 1001 + a_5 100001 + ... + a_{2l+1} 1\underbrace{00...0}\,1_{2l} + ...) +$$
$$+(a_2 99 + a_4 9999 + ... + a_{2m}\underbrace{99...99}_{2m} + ...)$$

А) числа, состоящие из четного числа 9-ок, делятся на 11, т.е. последняя скобка $\vdots 11$;

Б) заметим, что $1001 = (1100-99)\vdots 11$, $\quad 100001 = (110000-9999)\vdots 11$, $\quad 1\underbrace{00...00}_{2l}1 = (11\underbrace{00...00}_{2l} - \underbrace{99...99}_{2l}\vdots 11)$.

1.2.2 Алгоритм Евклида нахождения НОД(a,b)

Пусть требуется найти НОД(a,b). Будем считать, что $|a| > |b|$.

1) Разделим a на b с остатком:

$$a = q_1 b + r_1, \ 0 \le r_1 < |b| \quad (1)$$

Заметим, что любой делитель пары a и b будет делителем r_1, а значит пары b и r_1. С другой стороны, любой делитель пары (b, r_1) будет делителем a, а значит пары (a,b). Таким образом (равенство множеств), множество делителей пары (a,b) совпадает с множеством делителей пары (b,r_1), а значит и НОД$(a,b) =$ НОД(b,r_1).

2) Разделим b на r_1 с остатком:

$$b = q_2 r_1 + r_2, \ 0 \le r_2 < r_1 \quad (2)$$

При этом получаем, что НОД$(b, r_1) =$ НОД(r_1, r_2)

3) Разделим r_1 на r_2 с остатком:

$$r_1 = q_3 r_2 + r_3, \ 0 \le r_3 < r_2 \quad (3)$$

При этом НОД$(r_1,r_2) =$ НОД(r_2,r_3).
И т.д.

Посмотрим на остатки. $|b| > r_1 > r_2 > r_3 > ... \ge 0$. Получили строго убывающую последовательность неотрицательных целых чисел. Эта последовательность конечна. Существует $r_{k+1} = 0$, т.е.

k+1)

$$r_{k-1} = q_{k+1} r_k + 0 \quad (k+1)$$

При этом НОД$(a,b) =$ НОД$(b,r_1) =$ НОД$(r_1,r_2) =$ НОД$(r_2,r_3) = ... =$ НОД$(r_{k-1}, r_k) = r_k$.
Таким образом, НОД(a,b) равен последнему ненулевому остатку в алгоритме Евклида.

Весь алгоритм:	**Пример.** НОД(5083,3553)-?
1) $a = q_1 b + r_1, \ 0 \le r_1 < \lvert b \rvert$	$5083 = 1 * 3553 + 1530$
2) $b = q_2 r_1 + r_2, \ 0 \le r_2 < \lvert r_1 \rvert$	$3553 = 2 * 1530 + 493$
3) $r_1 = q_3 r_2 + r_3, \ 0 \le r_3 < \lvert r_2 \rvert$	$493 = 9 * 51 + 34$
...	$51 = 1 * 34 + 17$
k) $r_{k-2} = q_k r_{k-1} + r_k$	$34 = 2 * 17 + 0 \Rightarrow$ НОД$(5083, 3553) = 17$
k+1) $r_{k-1} = q_{k+1} r_k + 0$	
НОД$(a,b) = r_k$	

Элементы теории чисел. Теория сравнений.

Ученик 10-4 класса Оконешников Д.Д. по лекции к.ф.-м.н. Протопоповой Т.В.

от 20 января 2021 г.

2 Лекция №13

2.1 Каноническое разложение числа. НОД. НОК

Весь алгоритм:
1) $a = q_1 b + r_1$
2) $b = q_2 r_1 + r_2$
3) $r_1 = q_3 r_2 + r_3$
...
k) $r_{k-2} = q_k r_{k-1} + r_k$
k+1) $r_{k-1} = q_{k+1} r_k + 0$
НОД$(a,b) = r_k$

Пример. НОД(5083,3553)-?
$\Rightarrow r_1 = a - q_1 b = A_1 a + B_1 b$
$\Rightarrow r_2 = b - q_2 r_1 = b - q_2(A_1 a + B_1 b) = -q_2 A_1 a + (1 - B_1 q_2) b = A_2 a + B_2 b$
$\Rightarrow r_3 = r_1 - q_3 r_2 = A_1 a + B_1 b - q_3(A_2 a + B_2 b) =$
$= (A_1 - q_3 A_2) a + (B_1 - q_3 B_2) b = A_3 a + B_3 b$
$r_k = A_k a + B_k b$ или НОД$(a,b) = Aa + Bb$, где $A,\ B$ — целые

Утверждение. Если $d =$ НОД(a,b), то существуют целые A и $B : d = Aa + Bb$.

Замечание. Если НОД$(a,b) = 1$ (т.е. a и b взаимно просты), то существуют целые A и $B : 1 = Aa + Bb$.

2.2 Доказательство свойств делимости 8 и 9

Свойство 8. Если $ab \vdots m$ и НОД$(a,m) = 1$, то $b \vdots m$

$\uparrow$ Имеем НОД$(a,m) = 1 \Rightarrow \exists A,\ M : Aa + Mm = 1$.

Домножим последнее равенство на $b : \underset{\vdots m}{Aab} + \underset{\vdots m}{Mmb} = b \Rightarrow b \vdots m \downarrow$

Свойство 9. Если $a \vdots m,\ a \vdots k$ и НОД$(m,k) = 1$, то $a \vdots mk$

$\uparrow$

1) $a \vdots m \Rightarrow a = mq_1$

2) $a \vdots k \Rightarrow mq_1 \vdots k$

3) из 2) и НОД$(m,k) = 1 \Rightarrow$ по свойству 8 $q_1 \vdots k \Rightarrow q_1 = kq_2$

4) $a = mq_1 = mkq_2$, т.е. $a \vdots mk \downarrow$

2.3 Решение уравнений $\mathbf{ax + by = c}$

Определение. Диофантово уравнение первой степени - уравнение вида $ax + by = c$, где a, b, c, x, y — целые числа.

Пусть НОД$(a,b) = d$.

1) Если $c \vdots d$, то делим на d правую и левую части уравнения и получаем $a_1 x + b_1 y = c_1$, где НОД$(a_1, b_1) = 1$.
2) Если c не делится на d, то уравнение решений не имеет.

Таким образом, будем рассматривать уравнения (*) $ax + by = c,$ НОД$(a,b) = 1$.

Так как НОД$(a,b) = 1$, то по следствию из алгоритма Евклида $\exists$ целые $A,\ B : Aa + Bb = 1$.
Домножим равенство на $c : Aca + Bcb = c$.
Видим, что пара целых чисел $(x_0, y_0) = (Ac, bc)$ является решением уравнения.
Мы нашли частное (одно из) решение нашего уравнения. Найдем все решения (x,y).

$$\begin{cases} ax_0 + by_0 = c, \\ ax + by = c. \end{cases} \quad \Rightarrow a(x - x_0) + b(y - y_0) = 0,\ a(x - x_0) = -b(y - y_0)$$

НОД$(a,b)=1$, значит $(x-x_0)\vdots b$, т.е. $x-x_0=bt$ или $x=x_0+bt$, где t — целое.
Тогда $y-y_0=\frac{-a(x-x_0)}{b}=-at$ или $y=y_0-at$.
Таким образом, все пары вида (x_0+bt, y_0-at), где t — целое, являются решениями (*).

Замечание. Общее решение диофантова уравнения представляет собой сумму частного решения уравнения и решения соответствующего однородного уравнения (уравнения $ax+by=0$).

Легко понять, что решениями однородного уравнения являются все пары вида $(bt, -at)$, где t — целое.

Пример. 7x - 23y = 131 Проверка решения: $c \vdots$ НОД$(a,b) \Rightarrow$ имеет решения.
Можно угадать частное решение (22,1), так как 154 - 23 = 131.
Тогда все решения — $(22-33t, 1-7t)$, $t \in \mathbb{Z}$.

2.4 Сравнения

Основная идея теории сравнений заключается в том, что два числа a и $b(\in \mathbb{Z})$, имеющие при делении на $m \in \mathbb{N}$ один и тот же остаток, обнаруживают целый ряд одинаковых свойств по отношению к m.

Так по отношению к 2 мы выделяем четные и нечетные числа. Знаем, например, что сумма/разность четных - четное число, произведение четных - четное и т.д.

Определение. Целые числа a и b называются сравнимыми по модулю $m(a \equiv b(mod\ m))$, если при делении на m они дают одинаковые остатки. **(1)**

Пример. $8 \equiv 3(mod\ 5) \equiv 103(mod\ 5) \equiv -2(mod\ 5) \equiv -17(mod\ 5)$ и т.д.

Определение. $a \equiv b(mod\ m) \Leftrightarrow (a-b)\vdots m$. **(2)**

Докажем эквивалентность определений 1 и 2.
$\uparrow$
1) **(1)** $\Rightarrow$ **(2)**. Пусть остатки одинаковы, т.е. $a=q_1m+r,\ b=q_2m+r \Rightarrow a-b=m(q_1-q_2),\ (q_1-q_2)\in\mathbb{Z}$, т.е. $(a-b)\vdots m$;
2) **(2)** $\Rightarrow$ **(1)**. От противного.
Пусть остатки разные, т.е. $a=q_1m+r_1,\ b=q_2m+r_2$, где $0\le r_1<|m|,\ 0\le r_2<|m|\ (-|m|<-r_2\le 0)$.

Тогда $a-b=m(q_1-q_2)+r_1-r_2$ и $-|m|<r_1-r_2<|m|\ (|r_1-r_2|<|m|\ \mathbf{(3)}) \Rightarrow (r_1-r_2)\vdots m$
Но тогда по свойству делимости 4, если $r_1-r_2\neq 0$, то $|r_1-r_2|\ge|m|$, противоречие с **(3)**. Таким образом, $r_1=r_2$. $\downarrow$

2.5 Свойства сравнений

1) $a\equiv a(mod\ m)$
2) $a\equiv b(mod\ m)\Rightarrow b\equiv a(mod\ m)$
3) $a\equiv b(mod\ m),\ b\equiv c(mod\ m)\Rightarrow a\equiv c(mod\ m)$

$$\uparrow \begin{cases}(a-b)\vdots m,\\ (b-c)\vdots m.\end{cases} \Rightarrow a-c=\underbrace{(a-b)}_{\vdots m}+\underbrace{(b-c)}_{\vdots m}\vdots m\downarrow$$

Далее считаем, что $a\equiv b(mod\ m),\ c\equiv d(mod\ m)$

4/5) $a\pm c\equiv b\pm d(mod\ m)$

$$\uparrow \begin{cases}(a-b)\vdots m,\\ (c-d)\vdots m.\end{cases} \Rightarrow (a+c)-(b+d)=\underbrace{(a-b)}_{\vdots m}+\underbrace{(c-d)}_{\vdots m}\vdots m\downarrow$$

6) $ac\equiv bd(mod\ m)$

$$\begin{cases}(a-b)\vdots m,\\ (c-d)\vdots m.\end{cases} \Rightarrow ac-bd=ac-bc+bc-bd=c\underbrace{(a-b)}_{\vdots m}+b\underbrace{(c-d)}_{\vdots m}\vdots m\downarrow$$

7) $a^k \equiv b^k$

Следствие. Пусть $P(x)$ — любой многочлен с целыми коэффициентами, т.е. $P(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0$, тогда из $x \equiv y(mod\ m) \Rightarrow P(x) \equiv P(y)(mod\ m)$.

8) Если $ac \equiv bc(mod\ m)$ и НОД$(c, m) = 1$, то $a \equiv b(mod\ m)$.

$\uparrow ac - bc = c(a - b)$. Так как левая часть делится на m и НОД$(c, m) = 1$, то $(a - b)\vdots m \downarrow$

9) Если $a \equiv b(mod\ m)$ и $\exists\ k \in \mathbb{Z} : a = ka_1,\ b = kb_1,\ m = km_1$, то $a_1 \equiv b_1(mod\ m_1)$.

$\uparrow a - c = k(a_1 - b_1)$, т.е. $k(a_1 - b_1)\vdots km_1 \Rightarrow (a_1 - b_1)\vdots m_1 \downarrow$

Примеры.

1) Признак делимости на 3

$\forall n \in \mathbb{N} \quad n = a_k 10^k + a_{k-1}10^{k-1} + ... + a_1 10 + a_0$. Так как $10 \equiv 1(mod\ 3)$, то $10^k \equiv 1(mod\ 3) \Rightarrow n(mod\ 3) = (a_k + a_{k-1} + ... + a_1 + a_0)(mod\ 3)$.

2) Признак делимости на 11

Так как $10 \equiv -1(mod\ 11)$, то $10^k \equiv (-1)^k(mod\ 11)$.
Тогда $n(mod\ 11) = ((-1)^k a_k + ... + a_2 - a_1 + a_0)(mod\ 11)$

3) Найти остаток от деления на 3 числа $n = (1^2 + 1)(2^2 + 1)(3^2 + 1)...(1000^2 + 1)$

$n(mod\ 3) = \{(4^2 + 1) = (1^2 + 1)(mod\ 3),\ (4^2 + 1) = (1^2 + 1)(mod\ 3),\ 1000 : 3 = 333 * 3 + 1\} = (1^2 + 1)^{334}(2^2 + 1)^{333}(3^2 + 1)^{333}(mod\ 3) \equiv (2)^{334}(2)^{333}(1)^{333}(mod\ 3) \equiv (2)^{667}(mod\ 3) \equiv (-1)^{667}(mod\ 3) \equiv -1(mod\ 3) \equiv 2(mod\ 3)$.

4) При каких натуральных n число $8n + 3$ делится на 13?

То есть при каких n $8n + 3 \equiv 0(mod\ 13)$?

$8n \equiv -3(mod\ 13)$
$8n \equiv 10(mod\ 13)$
$4n \equiv 5(mod\ 13)$
$12n \equiv 15(mod\ 13)$
$-n \equiv 2(mod\ 13)$
$n \equiv -2(mod\ 13)$
$n = 13t - 2,\ t \in \mathbb{N}$ или $n = 13t + 11,\ t \in \mathbb{N}$

5) Найти все пары целых чисел x и y, удовлетворяющих уравнению $7x - 23y = 131$.

Избавимся от одного неизвестного: рассмотрим уравнение, например, по модулю 7.

$-23y \equiv 131(mod\ 7)$
$-2y \equiv 5(mod\ 7)$
$2y \equiv -5(mod\ 7)$
$2y \equiv 2(mod\ 7)$
$y \equiv 1(mod\ 7) \Rightarrow y = 7t + 1,\ t \in \mathbb{Z}$
$x = \frac{131+23y}{7} = \frac{131+23*7t+23}{7} = \frac{154+23*7t}{7} = 22 + 23t$
Ответ: $(22 + 23t, 1 + 7t), t \in \mathbb{Z}$.

2.6 Классификация чисел по данному модулю

Все числа сравнимые с данным a (а значит, сравнимые между собой) по модулю m в один класс.

Остатками при делении на m могут быть $0, 1, 2, ..., m - 1$.

Значит, можно выделить ровно m классов по модулю m.

Класс характеризуется остатком: $a = mt + r,\ t \in \mathbb{Z},\ 0 \le r \le m - 1$. Фактически, каждый класс — арифметическая прогрессия со множителем m.

Выберем произвольным образом по одному числу в каждом классе. Такую группу назовем *полной системой вычетов по модулю* m(ПСВ(m)). Для данного m таких систем существует бесконечно много.

Пример. По mod 3: ПСВ(3) = (0,1,2); ПСВ(3) = (10,11,12); ПСВ(3) = (-4,6,-5).

Числовые последовательности и их пределы

Ученик 10-4 класса Паньков М.А. по лекции к.ф.-м.н. Протопоповой Т.В.

от 16 марта 2021 г.

3 Лекция №21

Определение. Будем говорить, что x_n сходится к $a(\lim_{n\to\infty} x_n = a)$, если $\forall\varepsilon > 0\ \exists\ N = N(\varepsilon) : \forall n > N,\ |x_n - a| < \varepsilon$

Геометрический смысл:
а — предел x_n, $a - \varepsilon < x_n < a + \varepsilon$
$O_a = (a - \varepsilon,\ a + \varepsilon)$ — ε-окрестность т. а

Примеры:

1. Док-ть $\lim_{n\to\infty} \frac{1}{n} = 0$

   $\forall\varepsilon > 0\ \exists\ N = N(\varepsilon) : \forall n > N,$ док-ть: $\left|\frac{1}{n} - 0\right| < \varepsilon$
   $\left|\frac{1}{n} - 0\right| = \left|\frac{1}{n}\right| = \frac{1}{n} < \varepsilon,\ n > \frac{1}{\varepsilon} \Rightarrow N = \frac{1}{\varepsilon}$
   $N = [\frac{1}{\varepsilon}] + 1 \in \mathbb{N}$([x] — выделение целой части)

   $[x] \le x < [x] + 1$
   $\frac{1}{[x]+1} < \frac{1}{x}$

   действительно:
   $\frac{1}{n} < \frac{1}{N} = \frac{1}{[\frac{1}{\varepsilon}]+1} < \frac{1}{\frac{1}{\varepsilon}} = \varepsilon$, ч.т.д.

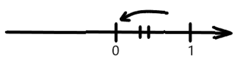
2. Док-ть $\lim_{n\to\infty} \frac{n}{n+1} = 1$

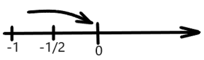
   $\forall\varepsilon > 0\ \exists\ N = N(\varepsilon) : \forall n > N,$ док-ть: $\left|\frac{n}{n+1} - 1\right| < \varepsilon$

   $\left|\frac{n}{n+1} - 1\right| = \left|\frac{n-n-1}{n+1}\right| = \frac{1}{n+1} < \frac{1}{n} < \varepsilon$, ч.т.д. ($N = [\frac{1}{\varepsilon} - 1] + 1$)

3. α — б.д.д.
   α_n — приближение б.д.д. по недостатку с точностью до $\frac{1}{10^n}$
   Покажем, что $\alpha_n \longrightarrow_{n\to\infty} \alpha$
   $\forall\varepsilon > 0\ \exists\ N : \forall n > N,\ |\alpha_n - \alpha| < \varepsilon$
   $|\alpha_n - \alpha| = |a,\ a_1,\ a_2, ...,\ a_n - a,\ a_1,\ a_2, ...,\ a_n,\ a_{n+1},\ a_{n+2}....| = 0,\underbrace{0\ ....\ 0}_{n},\ a_{n+1},\ a_{n+2}.... < \frac{1}{10^n} < \frac{1}{9n} <$
   $< \varepsilon$
   $10^n = (1 + 9)^n > 9n \qquad n > \frac{1}{9\varepsilon}$
   $N = [\frac{1}{9\varepsilon}] + 1$

   Сходимость может быть разной

   $x_n = \frac{1}{n}$ 

   $x_n = -\frac{1}{n}$ 

   $x_n = \frac{(-1)^n}{n}$