ВА Контролна 06.05.

Група по ВА1, гет, сряда 13-15
603 ХФ

Деление на цели числа с частно и остатък, НОД, НОК основна теорема на аритметиката

Деф
Естественото число $p > 1$ е просто, ако единствените му естествени делители са 1 и p

Лема
Ако p е просто число и $a_1 \ldots a_n$ са цели числа, то от делимост произведението на $a_1 \ldots a_n$ ($p / a_1 \ldots a_n$) следва че p дели поне едно a_i

Лок
Ако $p / a_1 \ldots a_n$ и $p \nmid a_1$ (p - не дели a_1) p НОД $(p, a_1) = (p, a_1) = \pm 1$ По следствие от тук на безу отук $\Rightarrow$ че $p / a_2 \ldots a_n$. С индукция по n и отук $\Rightarrow$ $p /$ някое a_i $\square$

Основна теорема на аритметиката
$\forall$ естествено число $n > 1$ има единствено с точност до реда на множителите разлагане $n = p_1 \ldots p_k$ в произведение на краен брой прости числа p_i.

Док

Съществуване - индукция по n
Естественото число $n=2$ е просто и
представя себе разлагане.
В общия случай, ако $n>1$ е просто
то n е свое разлагане в произведение
Ако $n>1$ е съставно, то $\exists n_1, n_2 > 1$
и $n_1, n_2 < n$ естествени числа с
$n = n_1 \cdot n_2$. По индукционно
предположение $n_1 = p_1 \cdot p_m$ и $n_2 = p_{m+1} \cdots p_k$ в произв.
на прости множители p_i. Тогава
$n_1 \cdot n_2 = n = p_1 \cdots p_m, p_{m+1} \cdots p_k$ е
произведение на прости множители
Единственост:
Нека $p_1 \cdots p_k = q_1 \cdots q_m$ са две
разлагания в произведение от
прости множители с условието
$k \leq m$. Тогава $p_k / q_1 \cdots q_m$, от където
p_k / q_i за някое $1 \leq i \leq m$. След
преномериране на $q_1 \cdots q_m$ можем
да считаме че p_k / q_m. Понеже q_m
$\in \mathbb{N}$ е просто число и $p_k \in \mathbb{N}, p_k > 1$
тогава $p_k = q_m$. След подходящо делене
с $p_k = q_m$ получаваме че $p_1 \cdots p_{k-1} = q_1 \cdots q_{m-1}$
С индукция по k можем да считаме
че $k-1 = m-1$ и $p_i = q_i$ за
$\forall i \leq k-1 = m-1$ след подходящо
преномериране на $q_1 \cdots q_{m-1}$. Сега
$k = m$ и $p_i = q_i$ за $\forall 1 \leq i \leq m$ - КО

среда 11-12, 529, каспарян българи

Деф Числови сравнения
Ако $n \in \mathbb{N} > 1$ и $a, b \in \mathbb{Z}$, то
a е сравнимо с b по модул n
ако n дели a-b. Записваме
$a \equiv b \pmod n$. Еквивалентно $a = b \pmod n$
точно когато a и b имат еднъи
същи остатък при делене с n
Св-ва на числовите сравнения
1) Рефлексивност
$a \equiv a \pmod n$ за $\forall a \in \mathbb{Z}, \forall n \in \mathbb{N}, n > 1$
2) Симетричност
Ако $a \equiv b \pmod n$ то $b \equiv a \pmod n$
защото от $n \mid a-b$ следва $n \mid b-a$
3) Транзитивност
Ако $a \equiv b \pmod n$ и $b \equiv c \pmod n$
то $a \equiv c \pmod n$. По-точно ако
$n \mid a-b$ и $n \mid b-c$, то $n \mid (a-b)+(b-c)$
$= a-c$ $n \mid a-c$
Съгласно св-ва 1) 2) 3)
сравнимостта по mod n е
релация на еквивалентност в $\mathbb{Z}$
Т-т точно и класа на еквив
относно сравнимост по mod n
защото остатъците $0 \le r \le n-1$
при делене с n са n на брой
Въвеждане събиране на остатъци
по mod n
$a \pmod n + b \pmod n = a+b \pmod n$
Означаване с $\mathbb{Z}_n$ множеството
на остатъците $r \pmod n$, $0 \le r \le n-1$
при делене с n

Определението е коректно, т.е
не зависи от избора на
цели представители a и b на
остатъците $a(\mathrm{mod}\, n)$, $b(\mathrm{mod}\, n)$
$\in \mathbb{Z}_n$. С други думи, ако $a_1 (\mathrm{mod}\, n)$
$= a(\mathrm{mod}\, n)$, $b_1 = b(\mathrm{mod}\, n)$, тогава
$a_1 + b_1 = a + b (\mathrm{mod}\, n)$
Наистина, $(a_1 + b_1) - (a+b) = (a_1 - a) + (b_1 - b)$
$\in n\mathbb{Z}$ (множ на n цели кратни на n)
$= \{nz \mid z \in \mathbb{Z}\}$ т.к. $a_1 - a, b_1 - b \in n\mathbb{Z}$
Аналогично, умн на остатъци
$[a(\mathrm{mod}\, n)][b(\mathrm{mod}\, n)] = ab(\mathrm{mod}\, n)$ е
коректно зададено, т.е. не зависи
от избора на цели представители
a и b. Наистина ако $a_1 = a(\mathrm{mod}\, n)$
и $b_1 = b(\mathrm{mod}\, n)$, то $a_1 b_1 - ab =$
$a_1 b_1 - a_1 b + a_1 b - ab = a_1(b_1 - b) + b(a_1 - a) \in$
$\in n\mathbb{Z}$. Тъй като $b_1 - b, a_1 - a \in n\mathbb{Z}$
Ако $ac = a_1 c$ и $c \neq$, то $a = a_1$
Ако $c \in \mathbb{Z} \setminus \{0\}$ и $ca = ca_1 (\mathrm{mod}\, n)$ то
$a = a_1 (\mathrm{mod}\, \frac{n}{(nc)})$ По-точно, ако
$d = (nc) \in \mathbb{N}$ $n_1 = \frac{n}{d}$, $q = \frac{c}{d}$ то
от $c = (a_1 - a) = nq$ следва $q_1 = (a_1 - a)$
$= n_1 q$ след цяло делене с d и
$n_1 \mid a_1 - a$ или $a_1 = a (\mathrm{mod}\, n_1 = \frac{n}{d})$

Групи – Определение, примери
основни св-ва
Деф.

Непразното множ. G е група ако в него е определена бинарна операция $G * G \to G$
$(a, b) \mapsto ab$ със св-вата

1) асоциативност
$(ab)c = abc$ за $\forall a, b, c \in G$

2) $\exists$ не на неутрален елемент $e \in G$, т.е. $eg = ge = g$ за $\forall g \in G$

3) $\exists$ не на обратен $g^{-1} \in G$ за $\forall g \in G$, т.е $gg^{-1} = e$

Примери

1) $(\mathbb{Z}, +)$ неутрален елемент 0
обратният в адитивен запис е противоположен
$z + (-z) = (-z) + z = 0$

2) Нека F е числово поле
Тогава $(F, +)$ - адитивна група на полето F

3) $(F^* := F \setminus \{0\}, \cdot)$ - мултипликативна група на F

4) Неутрален елемент 1

4) Ако V е линейно пр-во над поле F, то $(V, +)$ е адитивната група на пр-то V
И-те аксиоми вакат (линейно пр-во)

5) Нека F е числово поле, $n \in \mathbb{N}$. Тогава
$GL_n(F) = \{A \in Mat_n(F) \mid \det(A) \neq 0\}$
е група относно умн на матр, като е нарича обща линейна група
(неутралният елемент E_n)

6) Множеството S_n на взаимно еднозн. сами в себе изображения $\delta: \{1, \dots, n\} \to \{1, \dots, n\}$ е гр относно последователното изпълнение и се нарича симетрична гр от степен n

Асоциативност

$(\sigma\tau)\rho = \sigma(\tau\rho)$

$(\sigma\tau)\rho(i) = (\sigma\tau)(\rho(i)) = \sigma(\tau(\rho(i)))$

$\sigma(\tau\rho)(i) = \sigma((\tau\rho)(i)) = \sigma(\tau(\rho(i)))$

за $\forall\, 1 \le i \le n \Rightarrow (\sigma\tau)\rho = \sigma(\tau\rho)$

Неутрален елемент $\varepsilon = Id_{\{1,\dots,n\}}$

Деф кр и безкр гр

Ако група G има краен (безкр) брой елементи казваме че G е крайна (безкрайна) група

Ако е G е кр. гр. то броят $|G|$ на елементите на G се нарича ред на тази група

С разглежданите примери само S_n е крайна група и $|S_n| = n!$ защото за всяко еднозначно изображение $\sigma: \{1,\dots,n\} \to \{1,\dots,n\}$ има n - възможности за $\sigma(1)$ Еле фиксиране на $\sigma(1)$ има $n-1$ възможности за $\sigma(2)$ и т. н. Групите на $(\mathbb{Z},+)$, $(F,+)$ $(F^*,\cdot)$ за числово поле F, $F \supseteq \mathbb{Q}$, $(V,+)$ за лин. пр. во $V \neq \{0\}$ над безкр поле F и $GL_n(F)$ над безкр поле F са безкр групи.

Деф

Ако G е група с $ab = ba$ за $\forall a,b \in G$ казваме че G е абелева гр. С разглежданите примери $(\mathbb{Z},+)$ $(F,+)$ $(F^*,\cdot)$, $(V,+)$ са абелеви групи Общата линейна група $GL_n(F)$ не е абелева за $n \ge 2$.

e - неутрален елемент

Симетричната гр S_n не е абелева за $n \geq 3$

Нека бъде $\sigma: \{1 \dots n\} \xrightarrow{1:1} \{1, \dots, n\}$ е биекция

записваме като $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$

Вземаме $\sigma = (1\,2\,3\,4 \dots n) \in S_n$ и $n \geq 3$ и $\tau (2\,1\,3\,4 \dots n)$ не комутират $\sigma\tau = (1\,3\,2\,4 \dots n)$, $\tau\sigma = (2\,1\,3\,4 \dots n) \Rightarrow \sigma\tau \neq \tau\sigma$ Не е абелева

Т6:

Нека G е непразно мн-во с асоц-на бинарна операция $G \times G \to G, (a,b) \mapsto ab$

В такъв случай G е група тогава $\Leftrightarrow$ за $\forall a, b \in G$ ур-ята $ax = b$ и $ya = b$ имат единствени реш $x_0 \in G$, съответно $y_0 \in G$

Док

Ако G е гр $a, b \in G$, то $x_0 := a^{-1}b \in G$ е реш на ур-то $ax = b$, защото $a(a^{-1}b) \overset{\text{асоц}}{=} (aa^{-1})b = eb = b$. Аналогично $y_0 := ba^{-1} \in G$ е реш на $ya = b$, защото $(ba^{-1})a = b(a^{-1}a) = be = b$. Ако $x_1 \in G$ е реш на $ax = b$ то $ax_1 = b$ и следователно мн-во a^{-1} имаме

$$x_1 = ex_1 = (a^{-1}a)x_1 = a^{-1}(ax_1) = a^{-1}b = x_0$$

Следователно $ax = b$ има 1 реш $x_0 \in G$

Аналог. доказ. че $ya = b$ с a^{-1} има

$$y_1 = y_1 e = y_1(aa^{-1}) = (y_1 a)a^{-1} = ba^{-1} = y_0$$

Следователно $ya = b$ има единствено $y_0 \in G$

Обратно

Нека за $\forall a, b \in G$ y - от вида $ax = b$, $ya = b$ имат единствени решения в G

Тогава за $\forall m \in G$ y - от $mx = m$ има единствено решение e_m, т.ч. $me_m = m$, т.е. e_m е десен неутрален за m.

Аналогично $\forall$ елемент $m \in G$ има ляв неутр. елемент $e_m \in G$, определен като единственото решение на $y_m = m$ в G. Последното умн на $me_m = m$ с $e_m = m$ дава (1) $me_m e_m = me_m$

За $\forall u, v_1, v_2 \in G$ твърдим че $uv_1 = uv_2$ е достатъчно за $v_1 = v_2$ и $v_1 u = v_2 u$ е достатъчно за $v_1 = v_2$

Нанасяме y - от $ux = uv_1$ има единствено решение в G и ако $uv_2 = uv_1$ то v_1 и v_2 са негови решения

Аналогично ако $v_1 u = v_2 u$ то v_1 и v_2 са реш на $xu = v_1 u$ и съгласно единствеността на решението следва $v_1 = v_2$. Съкращаваме e_m в (1) и получаваме (2) $e_m e_m = e_m$

Лявото послед умн. на $e_m = e_m$ с e_m дава $e_m^2 = e_m (e_m e_m) = e_m e_m = e_m$ $\Rightarrow$ (2) чрез e_m дава (3) $e_m e_m = e_m (e_m e_m)$ съкр. отдясно e_m

Ln и твърдение (1)

$e_n = l_n$ за $\forall n, n \in G$ следват.

$\exists$ универ неутр елемент $\tilde{e} = l_n = l_m$ за $m, n \in G$ $\Leftrightarrow$ т.е. $me = m$ за $\forall m \in G$ и $en = n$ за $\forall n \in G$

За произвол $a \in G$ $\exists$ $ax = e$ има единствено решение $a_L \in G$ което е сесн обратен за a

Аналогично, $\exists a = e$ има ! реш $a_R \in G$ което е дяв обратен на a

От $a_L = ea_L = (a_R a)a_L = a_R e = a_R$

Следователно $\forall a \in G$ има обратен $a^{-1} = a_L = a_R$), т. е. $aa^{-1} = a^{-1}a = e$ и G ер