Теория 1

Валентин Стоянов

април 2018

Задача 1.

Формулирайте теоремата за делене с частно и остатък за цели числа

$\forall a, b \in \mathbb{Z} : b \neq 0, \exists q, r \in \mathbb{Z} : a = bq + r, \quad 0 \leq r \leq b$

Напишете определението за най-голям общ делител на две цели числа

Нека $a, b \in \mathbb{Z} : a \neq 0 \vee b \neq 0$. Най-голям общ делител(НОД) на a и b е числото $d = (a, b)$, ако:

- $d \mid a$, $d \mid b$
- $d_1 \mid a$, $d_1 \mid b$, то $d_1 \mid d$.

Напишете определението за най-малко общо кратно на две цели числа

Нека $a, b \in \mathbb{Z} : a \neq 0 \vee b \neq 0$. Най-малко общо кратно(НОК) на a и b е числото $d = [a, b]$, ако:

- $a \mid d$, $b \mid d$
- $a \mid d_1$, $b \mid d_1$, то $d \mid d_1$.

Каква е връзката между най-голям общ делител и най-малко общо кратно на две цели числа

Нека $a, b \in \mathbb{Z} : a \neq 0 \vee b \neq 0$
Тогава $[a, b](a, b) = ab$

Напишете равенството на Безу за две цели числа

Нека $a, b \in \mathbb{Z} : a \neq 0 \vee b \neq 0$
Ако $(a, b) = d$, то $\exists u, v \in \mathbb{Z} : au + bv = d$
В частност, ако $(a, b) = 1$, то $au + bv = 1$

Формулирайте основната теорема на аритметиката

Всяко естествено число $n > 1$ се представя по единствен начин(с точност до реда на множителите) като произведение на прости числа.
$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$

Задача 2.

Какво означава едно число да е сравнимо с друго по даден модул

Нека $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Казваме, че a е сравнимо с b по модул n (пише се $a \equiv b \pmod{n}$), ако $n \mid (a - b)$.

Какво представлява класът остатъци $\bar{m} \in \mathbb{Z}_n$

Това са всички цели числа, които при деление на n дават остатък m.

За какви числа n пръстенът $\mathbb{Z}_n$ е поле)

$\mathbb{Z}_n$ е поле точно когато n е просто число.

За какви числа k класът остатъци $k \in \mathbb{Z}_n$ е обратим елемент на пръстена $\mathbb{Z}_n$

?????????????????????????????????

Задача 3.

Напишете определението за пълна система остатъци по модул n

Всяко множество от n цели числа, които са представители на различни класове(тоест несравними две по две) по модул n.

Напишете определението за редуцирана система остатъци по модул n

Всяко множество от $\varphi(n)$ цели числа, които са две по две несравними по модул n.

Напишете определението за функция на Ойлер

Нека $n \in \mathbb{N}$. Функция на Ойлер се бележи с $\varphi(n)$ и представлява броят на естествените числа, които ненадминават n и са взаимно прости с n. Тя е мултипликативна, тоест ако $(a, b) = 1$, то $\varphi(ab) = \varphi(a)\varphi(b)$.

Формулирайте теоремата на Ойлер

Нека $n \in \mathbb{N}$, $z \in \mathbb{Z}$. Тогава $z^{\varphi(n)} \equiv 1 \pmod{n}$.

Формулирайте теоремата на Ферма

Ако $a \in \mathbb{Z}$, p е просто число и $(a, p) = 1$, то $a^{p-1} \equiv 1 \pmod{p}$

Задача 4.

Напишете определението за това едно число да дели друго

Ненулево число b дели a (пише се $b \mid a$), ако съществува число q, такова че $a = bq$. Ясно е, че остатъкът при делението на a с b е равен на 0.

Задача 5.

Формулирайте теоремата на Уилсън

Ако p е просто число, то $(p-1)! \equiv -1 \pmod{n}$.

Задача 6.

Докажете, че за всяко цяло число a е изпълнено, че $a \mid a$

$a = aq + r$, където $q = 1, r = 0$, т.е $a = a.1 \Rightarrow a \mid a$

Докажете, че ако $a \mid b$ и $b \neq 0$, то $|a| \leq |b|$

Докажете, че ако $a \mid b$ и $b \mid c$, то $a \mid c$

Докажете, че ако $a \mid b$ и $a \mid c$, то $a \mid b + c$

Докажете, че за всяко цяло число a е изпълнено $a \equiv a \pmod{n}$

Докажете, че ако $a \equiv b \pmod{n}$, то $b \equiv a \pmod{n}$

Докажете, че ако $a \equiv b \pmod{n}$ и $b \equiv c \pmod{n}$, то $a \equiv c \pmod{n}$

Докажете, че ако $a \equiv b \pmod{n}$ и $c \equiv d \pmod{n}$, то $a \pm c \equiv b \pm d \pmod{n}$

Задача 7.

Нека M е множество и $\circ : M \times M \to M$

Напишете определението за асоциативна операция

Операцията $\circ$ е асоциативна, ако $\forall a, b, c \in M, \quad a \circ (b \circ c) = (a \circ b) \circ c$

Напишете определението за комутативна операция

Операцията $\circ$ е комутативна, ако $\forall a, b \in M, \quad a \circ b = b \circ a$

Напишете определението за неутрален елемент

$\exists e \in M : \quad \forall a \in M, \quad a \circ e = e \circ a = a$

Напишете определението за подгрупа

Нека $(G, \circ)$ е група и $H \subseteq G, H \neq \emptyset$. H е подгрупа на G ако H е затворено относно операцията в G и обратният за всеки елемент от H е също в H.

Напишете определението за хомоморфизъм на групи

Нека $(G_1, \circ_{G_1}))$ и $(G_2, \circ_{G_2})$ са групи и $\varphi : G_1 \to G_2$ е изображение. φ е хомоморфизъм на групи, ако за всеки два елемента $a, b \in G_1$ е изпълнено, че $\varphi(a \circ_{G_1} b) = \varphi(a) \circ_{G_2} \varphi(b)$.

Напишете определението за подгрупа породена от подмножество на дадена група

Нека $(G, \circ)$ е група и $H \subseteq G$. С $\langle H \rangle$ бележим множеството от всички елементи на G, които могат да се представят като произведение(сума) на елементи от H или техните обратни(противоположни). $\langle H \rangle \leq G$. Казваме, че $\langle H \rangle$ се поражда от множеството H.

Напишете определението за циклична група

Нека $(G, \circ)$ е група и $g \in G$. Подгрупата $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$, породена от елемента g се състои от всички степени на g. $\langle g \rangle$ се нарича циклична група, породена от g, а g се нарича неин пораждащ.

Напишете определението за ред на елемент от дадена група

Нека $(G, \circ)$ е група и $g \in G$. Най-малкото естествено число r(ако съществува), за което $g^r = e_G$, се нарича ред на елемента g и се бележи с $r(g)$ или $|g|$. Ако не съществува такова число, то g не е от краен ред и се записва $r(g) = \infty$.

Задача 8.

Дайте пример за крайна група

S_3

Дайте пример за безкрайна група

$\mathbb{R}$

Дайте пример за абелева група

$\mathbb{Q}$

Дайте пример за неабелева група

$GL_3(F)$

Дайте пример за крайна циклична група

$\mathbb{Z}/5\mathbb{Z}$

Дайте пример за безкрайна циклична група

$\mathbb{Z}$

Задача 9.

Напишете определението за съседен клас на група по нейна подгрупа

Нека G е група, $H \leq G$ и $g \in G$. Множествата $gH = \{gh \mid h \in H\}$ и $Hg = \{hg \mid h \in H\}$ се наричат съответно ляв и десен съседен клас на G по подгрупата H. Всеки елемент на $gH(Hg)$ се нарича представител на този съседен клас.

На пишете определението за индекс на подгрупа на дадена група в групата

Нека G е крайна група и $H \leq G$. Броят на левите(десните) съседни класове на G по H, се нарича индекс на H в G и се бележи с $|G : H|$

Формулирайте теоремата на Лагранж

Нека G е крайна група и $H \leq G$. Тогава $|G| = |H||G : H|$

Напишете определението за нормална подгрупа на дадена група

Нека G е група и $H \leq G$. Тогава H се нарича нормална подгрупа на G(бележи се с $H \trianglelefteq G$), ако за всеки елемент $g \in G$ е изпълнено, че $gH = Hg$.

Напишете определението за факторгрупа на дадена група по нейна нормална подгрупа

Нека G е група и $H \trianglelefteq G$. G/H е множеството от всички леви(десни) съседни класове на G по H. $\bullet$ е бинарна операция: $\quad \forall a, b \in G : aH \bullet bH = abH$.

Напишете определението за ядро на хомоморфизъм на групи

Нека $\varphi : G \to G'$ е хомоморфизъм на групи. Множеството $Ker\varphi = \{g \in G \mid \varphi(g) = e\} \subseteq G$ се нарича ядро на φ.

Напишете определението за образ на хомоморфизъм на групи

Нека $\varphi : G \to G'$ е хомоморфизъм на групи. Множеството $Im\varphi = \{a \in G' \mid \exists b \in G : \quad a = \varphi(b)\} \subseteq G'$ се нарича образ на φ.

Формулирайте теоремата за хомоморфизмите за групи

Нека $\varphi : G \to G'$ е хомоморфизъм на групи. Тогава $Ker\varphi \trianglelefteq G$ и $G/Ker\varphi \cong Im\varphi$.

Формулирайте втората теорема за хомоморфизмите за групи

Формулирайте третата теорема за хомоморфизмите за групи

Задача 10.

Нека Ω е множество, а G е група.

Напишете определението за действие на група върху множество

G действа върху Ω, ако:

- $e \in G, \forall x \in \Omega : \quad ex = xe = x$
- $\forall g_1, g_2 \in G, \forall x \in \Omega : \quad (g_1 g_2)x = g_1(g_2 x)$

Напишете определението за стабилизатор на елемент от множество при действието на група върху това множество

Нека $x \in \Omega$. Стабилизатор на x в G е множеството
$St_G(x) = \{g \in G \mid gx = x\}$.

Напишете определението за орбита на елемент от множество при действието на група върху това множество

Нека $x \in \Omega$. Орбита на x е множеството $O(x) = \{gx \mid g \in G\}$.

Напишете как се изразява дължината на орбитата на елемент от множество при действие на група върху това множество чрез редовете на групата и на стабилизатора на елемента

Нека $x \in \Omega$. Тогава $|O(x)| = |G : St_G(x)| \Rightarrow |O(x)| \mid |G|$.

Напишете определението за клас спрегнати елементи на елемент от дадена група

Нека $a, b \in G$. a и b се наричат спрегнати, ако съществува $g \in G : \quad b = g^{-1}ag$.

Напишете определението за централизатор на елемент от дадена група

Централизатор на елемента $a \in G$ е множеството от елементи на G, които комутират с a. $C_G(a) = \{g \in G \mid ag = ga\} \leq G$

Напишете определението за център на група

Множеството $Z(G) = \{a \in G \mid \forall g \in G : ga = ag\}$ се нарича център на групата G. $Z(G) = G \Leftrightarrow G$ е абелева група.

Напишете формулата за класовете

Формулирайте теоремата на Кейли

Всяка крайна група от ред n е изоморфна на подгрупа на симетричната група S_n.