Висша Алгебра ТК1 Решения

Румен Димитров

February 2019

1. Формулирайте теоремата за делене с частно и остатък за цели числа

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

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

Казваме, че d е НОД на a, b, когато $d \mid a$ и $d \mid b$
и ако числото d_1 също е общ делител на a и b, то $d_1 \mid d$.

3. Напишете определението за наймалко общо кратно на две цели числа

Казваме, че d е НОК на a, b когато $a \mid d$ и $b \mid d$
и ако d_1 също е общо кратно на a и b, то $d \mid d_1$.

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

Нека (a, b) е НОД и $[a, b]$ е НОК на две цели числа a, b. Тогава е изпълнено $(a, b)[a, b] = ab$.

5. Напишете равенството на Безу за две цели числа

Ако a и b са две цели числа и $(a, b) = d$, то $\exists\, u, v \in \mathbb{Z}$, така че $ua + vb = d$.

6. Формулирайте основната теорема на аритметиката

Всяко $n > 1 \in \mathbb{N}$ се представя по единствен начин като произведение на прости числа, с точност до реда на множителите.

7. Напишете определението за пълна система остатъци по модул n

Пълна система остатъци по модул n е всяка система от n на брой несравними цели числа (Например $0, 1, ..., n-1 \mod n$).

8. Напишете определението за редуцирана система остатъци по модул n

Всяка система от $\phi(n)$ на брой ест. числа, несравними по модул n и взаимно прости с n. Например, $1, 5, 7, 11$ е редуцирана (приведена) система остатъци по модул 12.

9. Напишете определението за функция на Ойлер

Нека $n \in \mathbb{N}$. Броят на ест. числа, ненадминаващи n и взаимно прости с n обозначаваме $\phi(n)$ и наричаме функция на Ойлер. Например, $\phi(6) = 2$, защото от всички (естествени) числа преди 6, само 1 и 5 са взаимно прости с 6.

10. Формулирайте теоремата на Ойлер

Нека $n \in \mathbb{N}, r \in \mathbb{Z}$ и $(r, n) = 1$, тогава е изп. $r^{\phi(n)} \equiv 1 \mod n$.

11. Формулирайте теоремата на Ферма

Ако p е просто число и $a \nmid p$, то $a^{p-1} \equiv 1 \mod p$.

12. Напишете определението за това едно число да дели друго

Казваме, че b дели a, или $b \mid a$, когато $\exists q \in \mathbb{Z} : \ a = bq$.

13. Напишете определението за това числото a да е сравнимо с числото b по модул n

Нека $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Казваме, че a е сравнимо с b по модул n, или $a \equiv b \mod n \iff n \mid (a - b)$.

14. Формулирайте теоремата на Уилсън

Ако p е просто число, то е изп. $(p-1)! \equiv -1 \mod p$.

15. Докажете, че за всяко цяло число a е изпълнено, че a | a

По дефиниция искаме число q, така че $a = qa$.
$q = 1$ работи, значи дефиницията е изпълнена и $a \mid a$.

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

По дефиниция, $b = qa, \ |q| \geq 1$ (защото q трябва да е цяло число)
$\Longrightarrow$
$|b| = |qa| = |q||a|$.
Сега, ако $q = \pm 1$, то $|b| = |a|$. В противен случай, $|b| > |a|$.

17. Докажете, че ако a | b и b | c, то a | c

По дефиниция, $b = q_1 a$, $c = q_2 b \implies$
$c = q_1 q_2 a$, $q_1 q_2 \in \mathbb{Z}$. Значи $a \mid c$.

18. Докажете, че ако a | b и a | c, то a | b + c

По дефиниция, $b = q_1 a$, $c = q_2 a \implies$

$b + c = (q_1 + q_2)a$, $q_1 + q_2 \in \mathbb{Z}$. Значи $a \mid c$.

19. Докажете, че за всяко цяло число a е изпълнено a ≡ a (mod n)

Искаме $n \mid (a - a)$, т.е. $n \mid 0$
Търсим q, така че $0 = nq$. Очевидно $q = 0$ върши работа.

20. Докажете, че ако a ≡ b (mod n), то b ≡ a (mod n)

$a \equiv b \mod n \iff$
$n \mid (a - b) \iff$
$\exists\, q \in \mathbb{Z} : \ (a - b) = qn$
Умножаваме и двете страни по -1
$b - a = (-q)n$, $(-q) \in \mathbb{Z} \implies$
$n \mid (b - a) \implies$
$b \equiv a \mod n$.

21. Докажете, че ако a ≡ b (mod n) и b ≡ c (mod n), то a ≡ c (mod n)

По дефиниция, $n \mid (a - b)$, $n \mid (b - c) \implies$
$n \mid (a - b) + (b - c) \implies$
$n \mid (a - c) \implies a \equiv c \mod n$.

22. Докажете, че ако a ≡ b (mod n) и c ≡ d (mod n), то a ± c ≡ b ± d (mod n)

$n \mid (a-b), \quad n \mid (c-d) \implies$
$n \mid (a-b)+(c-d) \implies$
$n \mid (a+c)-(b+d) \implies (a+c) \equiv (b+d) \mod n$. Също,

$n \mid (a-b)-(c-d) \implies$
$n \mid a-b-c+d \implies$
$n \mid (a-c)-(b-d) \implies (a-c) \equiv (b-d) \mod n$.

23. Дайте пример за крайна група

$\{-1, 1\}$ относно умножението

24. Дайте пример за безкрайна група

$(\mathbb{Z}, +)$

25. Дайте пример за абелева група

Горните две, също C_n etc

26. Дайте пример за неабелева група

$GL_n(F) = \{A \in M_{n,n} \mid detA \neq 0\}$ е неабелева за $n \geq 2$. Например, $GL_3(F)$ е неабелева.

27. Дайте пример за крайна циклична група

$C_4 = \{\pm i, \pm 1\}$ или
Z_4 - Адитивна циклична група от ред 4

28. Дайте пример за безкрайна циклична група

$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

29. Напишете определението за циклична група

G е циклична, когато $\exists\, a \in G$, такъв че $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\} = G$.

30. Напишете определението за ред на елемент от дадена група

Нека G е група и $g \in G$. Най-малкото естествено число r, за което $g^r = e$ наричаме ред на елемента g. Бележим го с $r(g)$ или $|g|$. Ако не съществува, казваме, че g не е от краен ред и пишем $r(g) = \infty$.

31. Напишете определението за съседен клас на група по нейна подгрупа

Нека G е група, $H \leq G$, $g \in G$. Тогава $gH = \{gh \mid h \in H\}$ наричаме ляв съседен клас на G по H, а $Hg = \{hg \mid h \in H\}$ - десен съседен клас на G по H.

32. Напишете определението за индекс на подгрупа на дадена група в групата

Нека G е крайна група и $H \leq G$. Броя на левите (или десните) съседни класове на G по H наричаме индекс на H в G и бележим $|G : H|$.

33. Формулирайте теоремата на Лагранж

Нека G е група, $|G| < \infty$, $H \leq G$. Тогава е изп. $|G| = |H||G : H|$.

34. Напишете определението за нормална подгрупа на дадена група

Нека G е група и $H \leq G$. Ако $\forall g \in G$ е изп. $gH = Hg$, то H наричаме нормална подгрупа на G.

35. Напишете определението за факторгрупа на дадена група по нейна нормална подгрупа

Нека G е група, $H \trianglelefteq G$. Групата, дефинирана по следния начин се нарича факторгрупа на G по H:
$G/H = \{gH \mid g \in G\}$ с операция $g_1Hg_2H = (g_1g_2)H$.

36. Напишете определението за ядро на хомоморфизъм на групи

Нека $\phi : G \to G'$ е хомоморфизъм на групи. Ядро на ϕ дефинираме по следния начин: $Ker\phi = \{a \in G \mid \phi(a) = e\} \subseteq G$.

37. Напишете определението за образ на хомоморфизъм на групи

$\phi : G \to G'$ хомоморфизъм. $Im\phi = \{b = G' \mid \exists a \in G \ : \ \phi(a) = b\} \subseteq G'$

38. Формулирайте теоремата за хомоморфизмите за групи

$\phi : G \to G'$ хомоморфизъм, нека $H = Ker\phi$. Тогава $H \trianglelefteq G$ и $G/H \cong Im\phi$.

39. Формулирайте втората теорема за хомоморфизмите за групи

Нека G е група, $H \trianglelefteq G$, $A \leq G$. Тогава $AH/H \cong A/A \cap H$.

40. Формулирайте третата теорема за хомоморфизмите за групи

Нека G е група, $H \trianglelefteq G$, $A \trianglelefteq G$ и $H \leq A$. Тогава $A/H \trianglelefteq G/H$ и $(G/H)/(A/H) \cong G/A$.