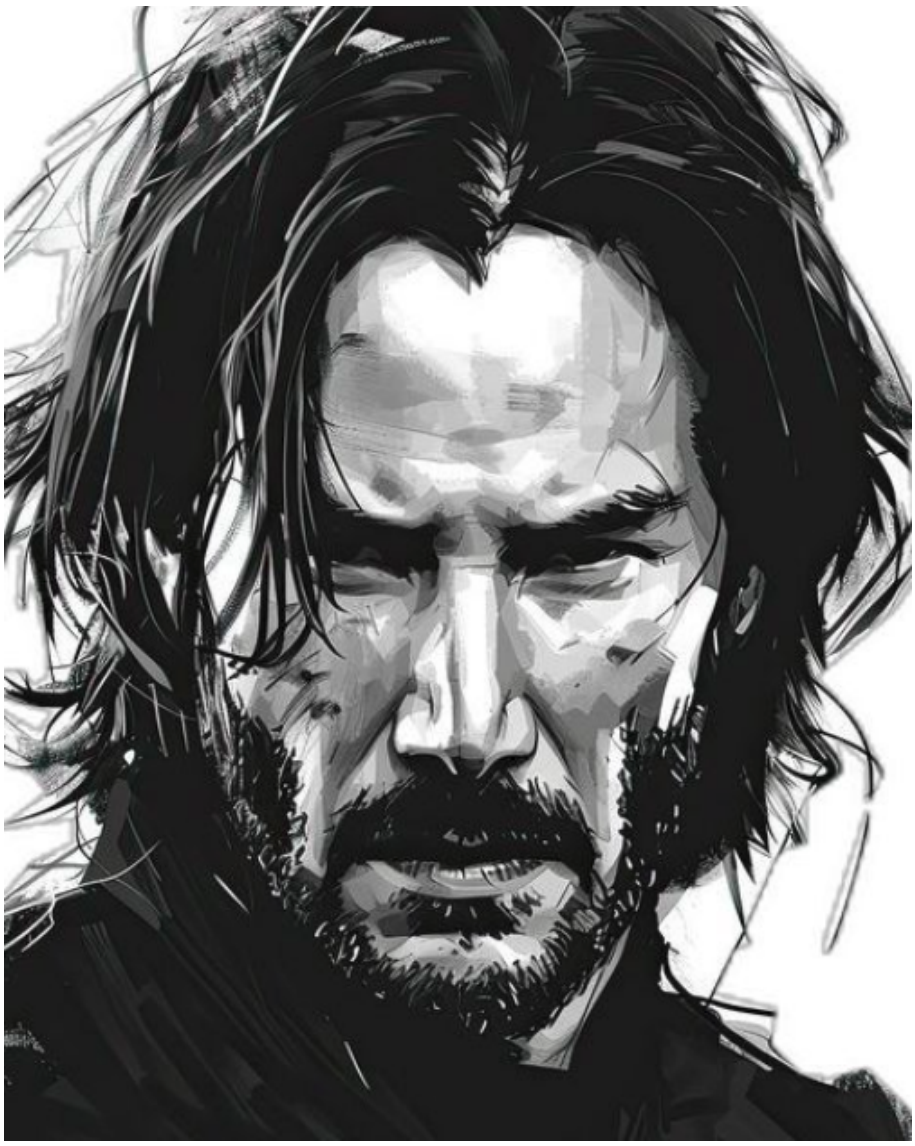
# Танц с огън

*Теодор Дишански*



**Tell them... Tell them all... Whoever comes, whoever it is...**

# Съдържание

# Теоретични Контролни

# 1 Задача

***(Напишете определението за група)*** Едно непразно множество $G$, снабдено с бинарна операция $*$ ($\forall\, a, b \in G : a * b \in G$) наричаме група, ако:

- Операцията $*$ е асоциативна ($\forall\, a, b, c \in G : (a * b) * c = a * (b * c)$).
- Съществува неутрален елемент относно операцията $*$ ($\exists\, e \in G\ \forall\, a \in G : a * e = e * a = a$).
- Всеки елемент на $G$ е обратим ($\forall\, a \in G\ \exists\, b \in G : a * b = b * a = e$).

***(Напишете определението за абелева група)*** Едно непразно множество $G$, снабдено с бинарна операция $*$ ($\forall\, a, b \in G : a * b \in G$) наричаме абелева група, ако:

- Операцията $*$ е асоциативна ($\forall\, a, b, c \in G : (a * b) * c = a * (b * c)$).
- Операцията $*$ е комутативна ($\forall\, a, b \in G : a * b = b * a$).
- Съществува неутрален елемент относно операцията $*$ ($\exists\, e \in G\ \forall\, a \in G : a * e = e * a = a$).
- Всеки елемент на $G$ е обратим ($\forall\, a \in G\ \exists\, b \in G : a * b = b * a = e$).

***(Дайте пример на абелева група)*** Примери за абелеви групи:

- Групата $(\mathbb{Z}, +)$ е безкрайна абелева група.
- Групата $(\mathbb{Q}, +)$ е безкрайна абелева група.
- Групата $(\mathbb{R}, +)$ е безкрайна абелева група.
- Групата $(\mathbb{C}, +)$ е безкрайна абелева група.

***(Дайте пример на неабелева група)*** $GL_n(\mathbb{F}) = \{A \in M_n(\mathbb{F}) \mid \det A \neq 0\}$ при $n \geq 2$, където $\mathbb{F}$ е числово поле, което е фиксирано, а бинарната операция е умножение на матрици.

***(Какво представлява симетричната група на едно множество)*** Нека $\Omega_n$ е множество. Със $S_\Omega$ означаваме множеството от всички биекции $f : \Omega \to \Omega$. Ако $f, g \in S_\Omega$, под произведение на $f$ и $g$ разбираме тяхната композиция, т.е. изображението $f \circ g : \Omega \to \Omega$, което действа по правилото $(f \circ g)(x) = f(g(x))$, $(x \in \Omega)$. С така въведената операция множеството $S_\Omega$ се превръща в група.

***(Напишете определението за пръстен)*** Нека $R$ е множество, в което са дефинирани две бинарни операции - събиране $(+)$ и умножение $(\cdot)$ ($\forall\, a, b \in R : a + b \in R, a \cdot b \in R$). Казваме, че $R$ е пръстен, ако $R$ е абелева група относно операцията събиране и освен това за всеки три елемента $a, b, c \in R$ е изпълнено:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \text{ (асоциативен закон)}$$
$$(a + b) \cdot c = a \cdot c + b \cdot c \text{ (дяснодистрибутивен закон)}$$
$$c \cdot (a + b) = c \cdot a + c \cdot b \text{ (ляводистрибутивен закон)}$$

***(Кога един пръстен е комутативен)*** Нека $R$ е множество, в което са дефинирани две бинарни операции - събиране $(+)$ и умножение $(\cdot)$ ($\forall\, a, b \in R : a + b \in R, a \cdot b \in R$). Казваме, че

$R$ е комутативен пръстен, ако $R$ е абелева група относно операцията събиране и освен това за всеки три елемента $a, b, c \in R$ е изпълнено:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \text{ (асоциативен закон)}$$
$$(a + b) \cdot c = a \cdot c + b \cdot c \text{ (дяснодистрибутивен закон)}$$
$$c \cdot (a + b) = c \cdot a + c \cdot b \text{ (ляводистрибутивен закон)}$$
$$a \cdot b = b \cdot a \text{ (комутативен закон)}$$

***(Кога един пръстен е с единица)*** Нека $R$ е множество, в което са дефинирани две бинарни операции - събиране $(+)$ и умножение $(\cdot)$ $(\forall\, a, b \in R : a + b \in R, a \cdot b \in R)$. Казваме, че $R$ е пръстен с единица, ако $R$ е абелева група относно операцията събиране, в $R$ има неутрален елемент относно умножението, който наричаме единица, бележейки го с $1_R$ $(\forall\, a \in R : a \cdot 1_R = 1_R \cdot a = a)$, и освен това за всеки три елемента $a, b, c \in R$ е изпълнено:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \text{ (асоциативен закон)}$$
$$(a + b) \cdot c = a \cdot c + b \cdot c \text{ (дяснодистрибутивен закон)}$$
$$c \cdot (a + b) = c \cdot a + c \cdot b \text{ (ляводистрибутивен закон)}$$

***(Кога един пръстен има делители на нулата)*** Нека $R$ е комутативен пръстен и $a \in R$. Казваме, че в пръстена $R$ $a$ е делител на нулата, ако съществува ненулев елемент $b \in R$, $b \neq 0_R$, такъв че $a \cdot b = 0_R$ или $b \cdot a = 0_R$.

***(Кога един пръстен е област на цялост)*** Нека $R$ е пръстен. Ако $R \neq (0)$, в $R$ няма ненулеви делители на нулата и $R$ е комутативен пръстен, то тогава казваме, че $R$ е област на цялост.

***(Кога един пръстен е поле)*** Нека $R$ е непразно множество, в което са дефинирани две бинарни операции - събиране $(+)$ и умножение $(\cdot)$. Казваме, че $R$ е поле, ако $R$ е комутативно тяло или ако $R$ е комутативен пръстен с единица (различна от нулата на пръстена), в който всеки ненулев елемент е обратим.

***(Кога един пръстен е тяло)*** Нека $R$ е непразно множество, в което са дефинирани две бинарни операции - събиране $(+)$ и умножение $(\cdot)$. Казваме, че $R$ е тяло, ако $R$ е пръстен с единица (различна от нулата на пръстена), в който всеки ненулев елемент е обратим.

***(Напишете необходимо и достатъчно условие едно подмножество на един пръстен да е негов подпръстен)*** Нека $(R, +, \cdot)$ е пръстен и $S \subseteq R$, $S \neq \emptyset$. Необходимо и достатъчно условие $S$ да е подпръстен на $R$ е за всеки два елемента $a, b \in S$ да следва, че $a - b, a \cdot b \in S$.

***(Напишете необходимо и достатъчно условие едно подмножество на едно поле да е негово подполе)*** Нека $(F, +, \cdot)$ е поле и $K \subseteq F$, $K \neq \emptyset$. Необходимо и достатъчно условие $K$ да е подполе е за всеки два елемента $a, b \in K$ да следва, че $a - b, a \cdot b^{-1} \in K$ $(b \neq 0)$.

***(Какво е подгрупата породена от едно подмножество на дадена група)*** Нека $G$ е група и $A \subseteq G$. Подгрупа на $G$, породена от $A$, е сечението на всички подгрупи на $G$, съдържащи $A$. Бележим с $\langle A \rangle$ и:

$$\langle A \rangle = \{a_1^{\epsilon_1} a_2^{\epsilon_2} ... a_n^{\epsilon_n} \mid n \in \mathbb{N}_0; a_i \in A; \epsilon_i = \pm 1; i = 1, ..., n\}$$

***(Какво е подпръстена породен от едно подмножество на даден пръстен)*** Нека $R$ е пръстен и $A \subseteq R$. Подпръстен на $R$, породен от $A$, е сечението на всички подпръстени на $R$, съдържащи $A$. Бележим с $S[A]$ и:

$$S[A] = \bigcap_{A \subseteq B \leq R} B = \{f(a_1, ..., a_n) \mid a_i \in A, 1 \leq i \leq n\} = \left\{ \sum_{i=1}^{n} \prod_{j=1}^{m_i} a_{ij} \mid n, m_i \in \mathbb{N}; a_{ij} \in A \right\}$$

Полиномите $f(a_1, ..., a_n)$ са полиноми на $n$ незадължително комутиращи променливи с коефициенти от $A$.

***(Какво е подполето породено от едно подмножество на дадено поле)*** Нека $F$ е поле и $A \subseteq F$. Подполето на $F$, породено от $A$, е сечението на всички подполета на $F$, съдържащи $A$. Бележим с $S(A)$ и:

$$S(A) = \bigcap_{A \subseteq B \leq F} B = \left\{ \frac{f(a_1, ..., a_n)}{g(a_1, ..., a_n)} \mid a_i \in A \right\}$$

Полиномите $f(a_1, ..., a_n)$ и $g(a_1, ..., a_n)$ са полиноми на $n$ комутиращи променливи с коефициенти от $A$. Също така трябва да е изпълнено, че полиномите $g(a_1, ..., a_n) \neq 0$.

# 2 Задача

***(Кога едно изображение от една група в друга група е хомоморфизъм)*** Нека са дадени групи $(G_1, *_1)$ и $(G_2, *_2)$ и $\varphi : G_1 \to G_2$ е изображение. Казваме, че $\varphi$ е хомоморфизъм на групи, ако за всеки два елемента $a, b \in G_1$ е изпълнено $\varphi(a *_1 b) = \varphi(a) *_2 \varphi(b)$.

***(Кога едно изображение от една група в друга група е изоморфизъм)*** Нека са дадени групи $(G_1, *_1)$ и $(G_2, *_2)$ и $\varphi : G_1 \to G_2$ е изображение. Казваме, че $\varphi$ е изоморфизъм на

групи, ако за всеки два елемента $a, b \in G_1$ е изпълнено $\varphi(a *_1 b) = \varphi(a) *_2 \varphi(b)$ и $\varphi$ е биекция, т.е. $\varphi$ е инекция ($\forall\, a, b \in G_1 : \varphi(a) = \varphi(b) \implies a = b$) и сюрекция ($\forall\, b \in G_2\ \exists\, a \in G_1 : \varphi(a) = b$).

***(Кога едно изображение от един пръстен в друг е хомоморфизъм)*** Нека са дадени пръстени $(R_1, +_1, \cdot_1)$ и $(R_2, +_2, \cdot_2)$ и $\varphi : R_1 \to R_2$ е изображение. Казваме, че $\varphi$ е хомоморфизъм на пръстени, ако за всеки два елемента $a, b \in R_1$ е изпълнено $\varphi(a +_1 b) = \varphi(a) +_2 \varphi(b)$ и $\varphi(a \cdot_1 b) = \varphi(a) \cdot_2 \varphi(b)$.

***(Кога едно изображение от един пръстен в друг е изоморфизъм)*** Нека са дадени пръстени $(R_1, +_1, \cdot_1)$ и $(R_2, +_2, \cdot_2)$ и $\varphi : R_1 \to R_2$ е изображение. Казваме, че $\varphi$ е изоморфизъм на пръстени, ако за всеки два елемента $a, b \in R_1$ е изпълнено $\varphi(a +_1 b) = \varphi(a) +_2 \varphi(b)$ и $\varphi(a \cdot_1 b) = \varphi(a) \cdot_2 \varphi(b)$ и $\varphi$ е биекция, т.е. $\varphi$ е инекция ($\forall\, a, b \in R_1 : \varphi(a) = \varphi(b) \implies a = b$) и сюрекция ($\forall\, b \in R_2\ \exists\, a \in R_1 : \varphi(a) = b$).

***(Какво наричаме ядро на един хомоморфизъм на групи)*** Нека $\varphi : G_1 \to G_2$ е хомоморфизъм на групи. Множеството $Ker\varphi = \{a \in G_1 \mid \varphi(a) = e_{G_2}\} \subseteq G_1$ наричаме ядро на $\varphi$.

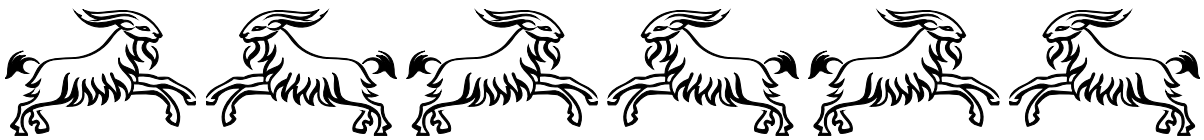
***(Какво наричаме ядро на един хомоморфизъм на пръстени)*** Нека $\varphi : R_1 \to R_2$ е хомоморфизъм на пръстени. Множеството $Ker\varphi = \{a \in R_1 \mid \varphi(a) = 0_{R_2}\} \subseteq R_1$ наричаме ядро на $\varphi$.

***(Какво наричаме образ на един хомоморфизъм на групи)*** Нека $\varphi : G_1 \to G_2$ е хомоморфизъм на групи. Множеството $Im\varphi = \{b \in G_2 \mid \exists\, a \in G_1 : \varphi(a) = b\} \subseteq G_2$ наричаме образ на $\varphi$.

***(Какво наричаме образ на един хомоморфизъм на пръстени)*** Нека $\varphi : R_1 \to R_2$ е хомоморфизъм на пръстени. Множеството $Im\varphi = \{b \in R_2 \mid \exists\, a \in R_1 : \varphi(a) = b\} \subseteq R_2$ наричаме образ на $\varphi$.

***(Какъв е образът на единичния елемент на една група при хомоморфизъм от нея в друга група)*** Нека $G_1$ и $G_2$ са групи, а изображението $\varphi : G_1 \to G_2$ е хомоморфизъм на групи. Тогава $\varphi(e_{G_1}) = e_{G_2}$.

***(Какъв е образът на нулевия елемент на един пръстен при хомоморфизъм от него в друг пръстен)*** Нека $R_1$ и $R_2$ са пръстени, а изображението $\varphi : R_1 \to R_2$ е хомоморфизъм на пръстени. Тогава $\varphi(0_{R_1}) = 0_{R_2}$.



# 3 Задача

***(Какво наричаме мултипликативна група на един пръстен)*** Нека $R$ е пръстен с единица. С $R^*$ означаваме множеството от всички обратими елементи на $R$. $R^*$ относно операцията умножение в пръстена наричаме мултипликативна група на $R$.

***(Какво наричаме адитивна група на един пръстен)*** Нека $R$ е пръстен. С $R^+$ означа-

ваме абелевата група $R$ относно операцията събиране в пръстена и я наричаме адитивна група на $R$.

***(Какво представлява мултипликативната група на пръстена от квадратните матрици с елементи от дадено поле)*** Нека $M_n(\mathbb{F})$ е пръстена от квадратните матрици с елементи от фиксираното поле $\mathbb{F}$. Тогава $(M_n(\mathbb{F}))^*$ е групата $GL_n(\mathbb{F})$ и това е множеството от обратимите квадратни матрици от ред $n$ с елементи от фиксираното поле $\mathbb{F}$. Тази група се нарича обща линейна група от ред $n$ над полето $\mathbb{F}$.

***(Какво представлява мултипликативната група на пръстена на целите числа)*** Нека $\mathbb{Z}$ е пръстена на целите числа. Тогава $\mathbb{Z}^* = \{-1, 1\}$.

***(Какво представлява мултипликативната група на поле)*** Нека $\mathbb{F}$ е поле. Тогава $\mathbb{F}^* = \mathbb{F}\backslash\{0\}$.

# 4 Задача

***(Какво наричаме 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 $H$.

***(Какво е необходимото и достатъчно условие два елемента на една група да са в един и същ съседен клас на групата по дадена нейна подгрупа)*** Нека $G$ е група, а $H \leq G$, като $g_1, g_2 \in G$. Необходимо и достатъчно условие $g_1H = g_2H$ е $g_1^{-1}g_2 \in H$. Необходимо и достатъчно условие $Hg_1 = Hg_2$ е $g_2g_1^{-1} \in H$.

***(Формулирайте теоремата на Лагранж)*** Нека $G$ е крайна група и $H \leq G$. Тогава е в сила равенството $|G| = |H|.|G : H|$, където $|G : H|$ е броят на левите или броят на десните съседни класове на групата $G$ по подгрупата $H$.

***(Напишете определението за нормална подгрупа на дадена група)*** Нека $G$ е група и $H \leq G$. Казваме, че $H$ е нормална подгрупа на $G$, ако за всеки елемент $g$ на $G$ е в сила равенството $gH = Hg$. Бележим това с $H \trianglelefteq G$ или $H \triangleleft G$.

***(Напишете необходимо и достатъчно условие една подгрупа на дадена група да е нормална)*** Необходимо и достатъчно условие една подгрупа $H$ на групата $G$ да е нормална подгрупа на групата $G$ е за всеки елемент $g \in G$ и за всеки елемент $h \in H$ да е изпълнено $ghg^{-1} \in H$.

***(Какво наричаме факторгрупа)*** Нека $G$ е група и $H \triangleleft G$. С $G/H$ означаваме множеството от всички леви (десни) съседни класове на $G$ по $H$. Дефинираме бинарната операция в $G/H$ $aH \cdot bH = abH$ ($\bar{a} \cdot \bar{b} = \overline{ab}$). Групата $G/H$ относно тази операция се нарича факторгрупа на групата $G$ по нормалната ѝ подгрупа $H$.

***(Формулирайте теоремата за хомоморфизмите за групи)*** Нека $G_1$ и $G_2$ са групи

и изображението $\varphi : G_1 \to G_2$ е хомоморфизъм на групи и $H = Ker\varphi$. Тогава $H \trianglelefteq G_1$ и $G_1/H \cong Im\varphi$.

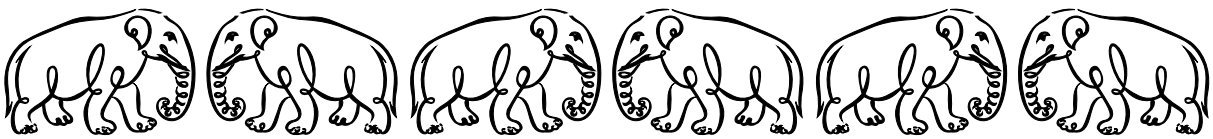
***(Какво наричаме идеал на даден пръстен)*** Нека $R$ е пръстен и $I \neq \emptyset$ е подмножество на $R$. Казваме, че $I$ е (двустранен) идеал на $R$, ако се изпълняват следните две условия:

- $a, b \in I \implies a - b \in I$;
- $a \in I, r \in R \implies ra \in I$ и $ar \in I$.

Бележим това с $I \trianglelefteq R$ или $I \triangleleft R$.

***(Какво наричаме факторпръстен на даден пръстен по негов идеал)*** Нека $R$ е пръстен и $I \trianglelefteq R$. С $R/I$ означаваме множеството от всички леви (десни) съседни класове на $(R, +)$ по $(I, +)$. Дефинираме бинарните операции в $R/I$ $\bar{a} + \bar{b} = \overline{a + b}$ и $\bar{a}\bar{b} = \overline{ab}$. Пръстенът $R/I$ относно тези операции се нарича факторпръстен на пръстена $R$ по идеала $I$.

***(Формулирайте теоремата за хомоморфизмите за пръстени)*** Нека $R_1$ и $R_2$ са пръстени и изображението $\varphi : R_1 \to R_2$ е хомоморфизъм на пръстени и $I = Ker\varphi$. Тогава $I \trianglelefteq R_1$ и $R_1/I \cong Im\varphi$.



# 5 Задача

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

***(Нека $G$ е група и $g \in G$. Какво е необходимото и достатъчно условие $g^k = e_G$ за $k \in G$)*** Необходимото и достатъчно условие $g^k = e_G$ е $r(g) \mid k$.

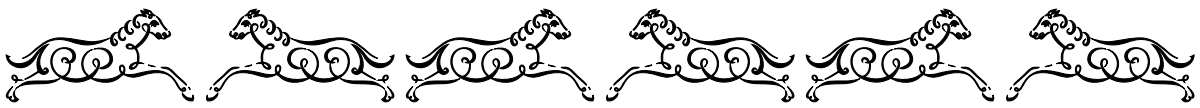
***(Нека $G$ е група и $g \in G$. Какво е необходимото и достатъчно условие $g^k = g^l$ за $k, l \in \mathbb{Z}$)*** Необходимото и достатъчно условие $g^k = g^l$ е $k \equiv l \pmod{r(g)}$.

***(Нека $G$ е група и $g \in G$. Какъв е редът на елемента $g^k$ за $k \in \mathbb{Z}$)*** Нека $r(g) = n$. Тогава $r(g^k) = \frac{n}{(n,k)}$.

***(Нека $G$ е група и $g \in G$. Какво е необходимото и достатъчно условие редът на $g^k$ да е равен на реда на $g$ за $k \in \mathbb{Z}$)*** Необходимо и достатъчно условие $r(g^k) = r(g)$ е $(r(g), k) = 1$.

***(Напишете достатъчно условие редът на произведението на два комутиращи елемента на една крайна група да е равен на най-малкото общо кратно на редовете на тези елементи)*** Нека $G$ е крайна група, където $a, b \in G$ са комутиращи елементи. Достатъчно условие за $|ab| = [|a|, |b|]$ е $\langle a \rangle \cap \langle b \rangle = \{e_G\}$.

***(Напишете достатъчно условие редът на произведението на два комутиращи елемента на една крайна група да е равен на произведението на редовете на тези елементи)*** Нека $G$ е крайна група, където $a, b \in G$ са комутиращи елементи. Достатъчно условие за $|ab| = |a|.|b|$ е $(|a|, |b|) = 1$.



# 6 Задача

***(Напишете определението за циклична група)*** Нека $G$ е група и $g \in G$. Подгрупата $\langle g \rangle$, породена от елемента $g$ и състояща се от всички степени на $g$, т.е. $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ (ако записът е адитивен, то $\langle g \rangle = \{ng \mid n \in \mathbb{Z}\}$), се нарича циклична група, породена от $g$, а $g$ се нарича неин пораждащ. Еквивалентна дефиниция е, че групата $G$ е циклична, ако съществува елемент $g \in G$, който поражда цялата група, т.е. $G = \langle g \rangle$.

***(На коя група е изоморфна всяка крайна циклична група от ред $n$)*** Всяка крайна циклична група от ред $n$ е изоморфна на групата $\mathbb{C}_n = \langle \omega_1 \rangle$.

***(На коя група е изоморфна всяка безкрайна циклична група)*** Всяка безкрайна циклична група е изоморфна на адитивната група на целите числа $\mathbb{Z}$.

***(Нека елементът $g$ поражда цикличната група от $G$ от ред $n$. Опишете всички пораждащи на групата $G$)*** Нека $G = \langle g \rangle$. Тогава, ако $r(g) = n$, то $G = \langle g^k \rangle$ точно тогава, когато $(k, n) = 1$.

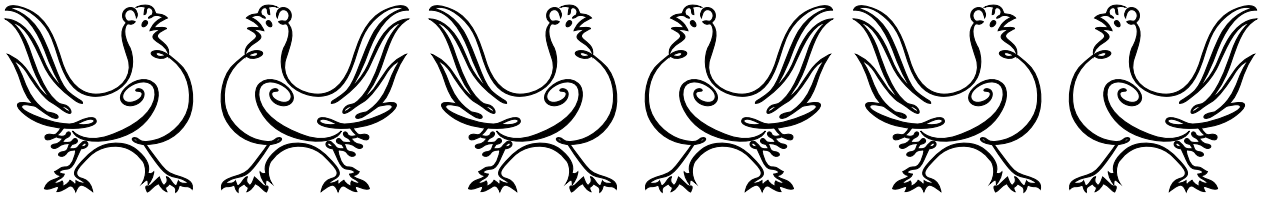
***(Нека елементът $g$ поражда безкрайната циклична група от $G$. Опишете всички пораждащи на групата $G$)*** Нека $G = \langle g \rangle$. Тогава, ако $|G| = \infty$, то $G = \langle g^k \rangle$ точно тогава, когато $k = \pm 1$ в мултипликативен запис, или $G = \langle kg \rangle$ точно тогава, когато $k = \pm 1$.

***(Какви са подгрупите на циклична група)*** Всяка подгрупа на циклична група също е циклична група.

***(Какви са редовете и пораждащите на подгрупите на безкрайна циклична група)*** Нека $G = \langle g \rangle$, $|G| = \infty$. Всички подгрупи са $e = \langle e \rangle$ и $\langle g^k \rangle = \langle g^{-k} \rangle$ за всяко $k \in \mathbb{N}$. Редът на всяка неединична подгрупа е $\infty$.

***(Какви са редовете и пораждащите на подгрупите на крайна циклична група)*** Нека $G = \langle g \rangle$, $|G| = n$. Тогава, $H < G$ е еквивалентно на това да съществува $d \mid n$, за което $H = \langle g^d \rangle$. Изпълнено е, че $|H| = \frac{n}{d}$ и съществува единствена такава група от този ред. Тук $|H| = \langle g^d \rangle$. Всички пораждащи за $\langle g^d \rangle$ са $\langle g^{dk} \rangle$ за $(k, \frac{n}{d}) = 1$.

***(Какво е необходимото и достатъчно условие една подгрупа на дадена циклична група да е подгрупа на друга подгрупа на групата)*** Нека $G = \langle g \rangle$, т.е. $G$ е крайна циклична група. Необходимо и достатъчно условие за $\langle g^k \rangle < \langle g^l \rangle < G$ е $|\langle g^k \rangle| \mid |\langle g^l \rangle|$. Знаем, че $r(g^k) = \frac{r(g)}{(r(g),k)}$ и $r(g^l) = \frac{r(g)}{(r(g),l)}$ или $l \mid k$ ($l \mid k \mid |g|$).



# 7 Задача

***(Формулирайте теоремата за делене с частно и остатък на две цели числа)*** За всеки две цели числа $a$ и $b$, $b \neq 0$, съществуват еднозначно определени цели числа $q$ и $r$, такива че $a = bq + r$ и $0 \leq r < |b|$.

***(Какви са идеалите в пръстена на целите числа)*** Идеалите в пръстена на целите числа $\mathbb{Z}$ са главни и се описват като $n\mathbb{Z}$, където $n \in \mathbb{N} \cup \{0\}$.

***(Какво е необходимото и достатъчно условие един идеал да е подмножество на друг идеал в пръстена на целите числа)*** Нека $(a) \trianglelefteq \mathbb{Z}$ и $(b) \trianglelefteq \mathbb{Z}$. Необходимо и достатъчно условие $(a) \subseteq (b)$ е да съществува $t \in \mathbb{Z}$, такова че $a = bt$, т.е $b \mid a$.

***(Кога две цели числа се делят взаимно)*** Нека $a, b \in \mathbb{Z}$. Ако $a \mid b$ и $b \mid a$, то $b = \pm a$. С други думи $(a) = (b)$ тогава и само тогава, когато $b = \pm a$.

***(Какво е необходимото и достатъчно условие $d$ да поражда идеала, който е сума на идеалите породени от $a$ и $b$ в пръстена на целите числа)*** Нека $a, b, d \in \mathbb{Z}$. Необходимо и достатъчно условие $(a) + (b) = (d)$ е:

- $d \mid a$ и $d \mid b$;
- ако $d' \mid a$ и $d' \mid b$, то $d' \mid d$.

***(Какво е необходимото и достатъчно условие $m$ да поражда идеала, който е сечение на идеалите породени от $a$ и $b$ в пръстена на целите числа)*** Нека $a, b, m \in \mathbb{Z}$. Необходимо и достатъчно условие $(a) \cap (b) = (m)$ е:

- $a \mid m$ и $b \mid m$;
- ако $a \mid m'$ и $b \mid m'$, то $m \mid m'$.

***(Как се изразява идеалът породен от най-големия общ делител на две цели числа в пръстена на целите числа чрез идеалите породени от тези числа)*** Нека $a, b \in \mathbb{Z}$. Тогава $d = (a, b)$ поражда идеал $(d)$ и за него е изпълнено $(d) = (a) + (b)$.

***(Как се изразява идеалът породен от най-малкото общо кратно на две цели числа в пръстена на целите числа чрез идеалите породени от тези числа)*** Нека $a, b \in \mathbb{Z}$. Тогава $m = [a, b]$ поражда идеал $(m)$ и за него е изпълнено $(m) = (a) \cap (b)$.

***(Формулирайте равенството на Безу за цели числа)*** За всеки две числа $a, b \in \mathbb{Z}$ съществуват числа $u, v \in \mathbb{Z}$, такива че е изпълнено $au + bv = (a, b)$.

# 8 Задача

***(Какво наричаме максимален идеал)*** Нека $R$ е пръстен и $I \triangleleft R$. Казваме, че $I$ е максимален идеал, ако $I \neq R$ и ако от $I \subseteq J \subseteq R$ следва, че $I = J$ или $J = R$.

***(Какво наричаме прост идеал)*** Нека $R$ е пръстен и $I \triangleleft R$. Казваме, че $I$ е прост идеал, ако от $I \neq R$ и ако от $ab \in I$ следва, че $a \in I$ или $b \in I$.

***(Какво наричаме неразложим елемент в комутативен пръстен с единица)*** Нека $R$ е комутативен пръстен с единица. Казваме, че $a \in R$ е неразложим елемент, ако $a \neq 0$, $a \notin R^*$ и от $a = bc$ за $b, c \in R$ следва, че $b \in R^*$ или $c \in R^*$.

***(Какво наричаме прост елемент в комутативен пръстен с единица)*** Нека $R$ е комутативен пръстен с единица. Казваме, че $a \in R$ е прост елемент, ако от $a \mid bc$ следва, че $a \mid b$ или $a \mid c$.

***(Какъв елемент е пораждащият на максимален идеал в област от главни идеали)*** Нека $R$ е област на главни идеали и $(a) \triangleleft R$ е максимален идеал. Тогава елементът $a$ е неразложим.

***(Какъв елемент е пораждащият на прост идеал в област от главни идеали)*** Нека $R$ е област на главни идеали и $(a) \triangleleft R$ е прост идеал. Тогава елементът $a$ е прост.

***(Какъв идеал е идеалът породен от неразложим елемент в област от главни идеали)*** Нека $R$ е област от главни идеали и $a \in R$ е неразложим елемент. Тогава идеалът $(a) \triangleleft R$ е максимален.

***(Какъв идеал е идеалът породен от прост елемент в област от главни идеали)*** Нека $R$ е област от главни идеали и $a \in R$ е прост елемент. Тогава идеалът $(a) \triangleleft R$ е прост.

***(За какъв идеал на комутативен пръстен с единица факторпръстенът е поле)*** Нека $R$ е комутативен пръстен с единица. Ако $I \triangleleft R$ и $R/I$ е поле, то $I \triangleleft R$ е максимален идеал.

***(За какъв идеал на комутативен пръстен с единица факторпръстенът е област на цялост)*** Нека $R$ е комутативен пръстен с единица. Ако $I \triangleleft R$ и $R/I$ е област, то $I \triangleleft R$ е прост идеал.

***(Какъв пръстен е факторпръстенът на комутативен пръстен с единица по максимален идеал)*** Нека $R$ е комутативен пръстен с единица и $I \triangleleft R$ е максимален идеал. Тогава факторпръстенът $R/I$ е поле.

***(Какъв пръстен е факторпръстенът на комутативен пръстен с единица по прост идеал)*** Нека $R$ е комутативен пръстен с единица и $I \triangleleft R$ е прост идеал. Тогава факторпръстенът $R/I$ е област на цялост.

# 9 Задача

***(Формулирайте основната теорема на аритметиката на целите числа)*** За всяко число $a \in \mathbb{Z}$, $a \neq 0$ съществуват прости числа $p_1, ..., p_k$ и $\epsilon = \pm 1$, които удовлетворяват следното: $a = \epsilon.p_1...p_k$. Това представяне на числото $a$ е единствено с точност до реда на множителите.

***(Докажете, че съществуват безбройно много прости числа)*** Допускаме, че не съществуват безбройно много прости числа. Нека означим с $p_1, ..., p_k$ всички прости числа и да разгледаме числото $P = p_1...p_k + 1$. Естественото число $P$ се дели на някое просто число $p$, което трябва да е измежду $p_1, ..., p_k$. Но тогава и числото 1 се дели на $p$, което е противоречие.

***(Как се намира най-големият общ делител на две числа, ако са известни каноничните им разлагания на прости множители)*** Нека $a, b \in \mathbb{N}$ и $a = p_1^{\alpha_1}...p_k^{\alpha_k}$, където $\alpha_i \geq 0, i = 1, ...k$, и $b = p_1^{\beta_1}...p_k^{\beta_k}$, където $\beta_i \geq 0, i = 1, ..., k$. Тогава $d = (a, b) = p_1^{\gamma_1}...p_k^{\gamma_k}$, където $\gamma_i = \min\{\alpha_i, \beta_i\}, i = 1, ..., k$.

***(Как се намира най-малкото общо кратно на две числа, ако са известни каноничните им разлагания на прости множители)*** Нека $a, b \in \mathbb{N}$ и $a = p_1^{\alpha_1}...p_k^{\alpha_k}$, където $\alpha_i \geq 0, i = 1, ..., k$, и $b = p_1^{\beta_1}...p_k^{\beta_k}$, където $\beta_i \geq 0, i = 1, ..., k$. Тогава $m = [a, b] = p_1^{\gamma_1}...p_k^{\gamma_k}$, където $\gamma_i = \max\{\alpha_i, \beta_i\}, i = 1, ..., k$.

***(Как се намира броят на положителните делители на естествено число, ако е известно каноничното му разлагане на прости множители)*** Нека $n \in \mathbb{N}$ и $n = p_1^{\beta_1}...p_k^{\beta_k}$, където $p_1, ..., p_k$ са различни прости числа, а $\beta_1, ..., \beta_k > 0$. Тогава броят на положителните делители на числото $n$ е $(\beta_1 + 1)(\beta_2 + 1)...(\beta_k + 1)$.

***(Как изглежда делител на естествено число, ако е известно каноничното му разлагане на прости множители)*** Нека $n \in \mathbb{N}$ и $n = p_1^{\alpha_1}...p_k^{\alpha_k}$, където $p_1, ..., p_k$ са различни прости числа, а $\alpha_1, ..., \alpha_k > 0$. Тогава, ако $d \mid n$, то $d = p_1^{\beta_1}...p_k^{\beta_k}$, $0 \leq \beta_i \leq \alpha_i$ за всяко $i = 1, ..., k$.

***(Какво представлява функцията на Ойлер)*** Нека $n$ е естествено число. С $\varphi(n)$ бележим броя на естествените числа, ненадминаващи $n$ и взаимно прости с $n$. Функцията $\varphi(n)$ се нарича функция на Ойлер.

***(Колко елемента има мултипликативната група на пръстена от класовете остатъци по модул $n$)*** Нека $\mathbb{Z}_n$ е пръстена на класовете остатъци по модул $n$. Тогава $|\mathbb{Z}_n^*| = \varphi(n)$.

***(Кога един елемент на пръстена от класовете остатъци по модул $n$ е обратим)*** Нека $\bar{a} \in \mathbb{Z}_n$. $\bar{a}$ е обратим тогава и само тогава когато $(a, n) = 1$.

***(Кога един елемент на пръстена от класовете остатъци по модул $n$ е делител на нулата)*** Нека $\bar{a} \in \mathbb{Z}_n$. $\bar{a}$ е делител на нулата тогава и само тогава, когато $(a, n) \neq 1$.

***(Кога един елемент на пръстена от класовете остатъци по модул $n$ не е обратим)*** Нека $\bar{a} \in \mathbb{Z}_n$. $\bar{a}$ не е обратим тогава и само тогава, когато $(a, n) \neq 1$.

***(Кога един елемент на пръстена от класовете остатъци по модул $n$ не е делител на нулата)*** Нека $\bar{a} \in \mathbb{Z}_n$. $\bar{a}$ не е делител на нулата тогава и само тогава, когато $(a, n) = 1$.

***(Формулирайте теоремата на Ойлер)*** Нека $n \in \mathbb{N}$ и $r \in \mathbb{Z}$, като $(r, n) = 1$. Тогава $r^{\varphi(n)} \equiv 1 \pmod{n}$.

***(Формулирайте теоремата на Ферма)*** Нека $r \in \mathbb{Z}$ и $p$ е просто число, като $p \nmid r$. Тогава $r^{p-1} \equiv 1 \pmod{p}$.

# 10 Задача

***(Докажете, че редът на всяка подгрупа на крайна група дели реда на групата)*** Нека $G$ е крайна група и $H < G$. От теоремата на Лагранж имаме, че $|G| = |H|.|G : H|$. Но $|G : H| \in \mathbb{Z}$. Тогава $|H| \mid |G|$.

***(Докажете, че индексът на крайна група по нейна подгрупа дели реда на групата)*** Нека $G$ е крайна група и $H < G$. От теоремата на Лагранж имаме, че $|G| = |H|.|G : H|$. Но $|H| \in \mathbb{Z}$. Тогава $|G : H| \mid |G|$.

***(Докажете, че редът на произволен елемент на крайна група дели реди на групата)*** Нека $G$ е крайна група и $g \in G$. Знаем, че $r(g) = |\langle g \rangle| = r$, т.е. $r$ е най-малкото естествено число, за което $g^r = e$. Нека $H = \langle g \rangle$ е цикличната подгрупа на $G$, породена от $g$. Тогава $|H| = |\langle g \rangle| = |g| = r$. От теоремата на Лагранж имаме, че $|G| = |H|.|G : H|$. Но $|G : H| \in \mathbb{Z}$. Тогава $|H| \mid |G|$.

***(Докажете, че всеки елемент на крайна група на степен реда на групата дава единичния елемент на групата)*** Нека $G$ е крайна група и $g \in G$. Нека $r(g) = r$, т.е. $r$ е най-малкото естествено число, за което $g^r = e$. Нека $H = \langle g \rangle$ е цикличната подгрупа на $G$, породена от $g$. Тогава $|H| = |\langle g \rangle| = |g| = r$. От теоремата на Лагранж имаме, че $|G| = |H|.|G : H|$. Но $|G : H| \in \mathbb{Z}$. Тогава $|H| \mid |G|$, т.е. $r \mid |G|$. Нека $|G : H| = k$. Получаваме, че $g^{|G|} = g^{rk} = (g^r)^k = e_G^k = e_G$.

***(Докажете, че всяка група от ред просто число е циклична)*** Нека $G$ е крайна група от ред $p$, където $p$ е просто число. Щом $|G| = p \geq 2$, то съществува елемент $g \in G$, такъв че $g \neq e$. $\langle g \rangle$ е цикличната група, породена от $g$. От теоремата на Лагранж следва, че $|\langle g \rangle| \mid |G|$ и тъй като $p$ е просто число, а $g \neq e$, то следва, че $|\langle g \rangle| \geq 2$, а оттук $|\langle g \rangle| = p = |G|$. Но $\langle g \rangle \leq G$, тоест достигаме до извода, че $G = \langle g \rangle$, с други думи $G$ е крайна циклична група от ред $p$, откъдето $G \cong \mathbb{C}_p$.

***(Докажете, че всяка крайна група, която няма собствени подгрупи, е циклична от прост ред)*** Нека $G \neq \{e\}$ е крайна група, която няма собствени подгрупи, т.е. $G$ няма подгрупи, различни от $\{e\}$ и $G$. Нека $g \in G$ е такъв, че $g \neq e$. Тогава $\langle g \rangle \leq G$ и $\langle g \rangle \neq \{e\}$, откъдето следва, че $\langle g \rangle = G$ и $G$ е циклична група. Групата $G$ е крайна и тогава $|G| = p$ за $p \in \mathbb{N}$. Знаем, че в този случай $G \cong \mathbb{C}_p$. Ако $p$ не е просто число, то съществува число $d \in \mathbb{N}$, $d \neq 1$, такова че $d \mid p$ и $\mathbb{C}_d \leq \mathbb{C}_p$ е нетривиална подгрупа на $\mathbb{C}_p$, което би означавало, че $G$ също притежава нетривиални подгрупи. Стигнахме до противоречие, следователно числото $p$

е просто.

***(Докажете теоремата на Ойлер)*** Ако елементите $x, y \in \mathbb{Z}$, то $x \equiv y \pmod{n}$ е еквивалентно на $\bar{x} = \bar{y}$ в пръстена $\mathbb{Z}_n$. Тогава, ако изберем $a \in \mathbb{Z}$, такова че $(a, n) = 1$, тогава $\bar{a}$ е обратим в $\mathbb{Z}_n$, тоест $\bar{a} \in \mathbb{Z}_n^*$. От теоремата на Лагранж имаме, че $\bar{a}^{|\mathbb{Z}_n^*|} = 1$ или $\bar{a}^{\varphi(n)} = \bar{1}$, което е еквивалентно на $a^{\varphi(n)} \equiv 1 \pmod{n}$.

***(Докажете теоремата на Ферма)*** Нека $p \in \mathbb{Z}$. Ако елементите $x, y \in \mathbb{Z}$, то $x \equiv y \pmod{p}$ е еквивалентно на $\bar{x} = \bar{y}$ в пръстена $\mathbb{Z}_p$. Тогава, ако изберем $a \in \mathbb{Z}$, такова че $(a, p) = 1$, тогава $\bar{a}$ е обратим в $\mathbb{Z}_p$, тоест $\bar{a} \in \mathbb{Z}_p^*$. От теоремата на Лагранж имаме, че $\bar{a}^{\mathbb{Z}_p^*} = \bar{1}$ или $\bar{a}^{\varphi(p)} = \bar{1}$, което е еквивалентно на $a^{\varphi(p)} \equiv 1 \pmod{p}$ или $a^{p-1} \equiv 1 \pmod{p}$. По-общо формулирано: $a^p \equiv a \pmod{p}$, за всяко $a \in \mathbb{Z}$.

# 11 Задача

***(Кога една числова функция е мултипликативна)*** Функцията $f : \mathbb{N} \to \mathbb{C}$ е мултипликативна, ако $\forall\, a, b \in \mathbb{N}$ е изпълнено, че от $(a, b) = 1$ следва $f(ab) = f(a)f(b)$.

***(Как се дефинира функцията на Мьобиус)*** Нека $n$ е естествено число. Функцията

$$\mu(n) = \begin{cases} 1, \text{ ако } n = 1, \\ 0, \text{ ако } n \text{ се дели на квадрат на просто число}, \\ (-1)^s, \text{ ако } n \text{ е произведение на } s \text{ различни прости числа} \end{cases}$$

се нарича функция на Мьобиус.

***(Ако с $\mu$ сме означили функцията на Мьобиус, на колко е равна сумата $\sum_{d|n} \mu(d)$ за естествено число $n$)*** Нека $M(n) = \sum_{d|n} \mu(d)$. Тогава $M(n) = 1$ при $n = 1$ и $M(n) = 0$ при $n > 1$.

***(Формулирайте формулата за обръщане на Мьобиус)*** Нека е дадена $f : \mathbb{N} \to \mathbb{N}$ и $F(n) = \sum_{d|n} f(d)$, където $n \in \mathbb{N}$. Тогава е изпълнено, че $f(n) = \sum_{d|n} F(d)\mu(\frac{n}{d}) = \sum_{d|n} F(\frac{n}{d})\mu(d)$.

***(Ако с $\varphi$ сме означили функцията на Ойлер, на колко е равна сумата $\sum_{d|n} \varphi(d)$ за естествено число $n$)*** Изпълнено е, че $\sum_{d|n} \varphi(d) = n$.

***(На колко е равна функцията на Ойлер за естествено число, ако е известно каноничното му разлагане на прости числа)*** Нека $n \in \mathbb{N}$ и каноничното му разлагане на прости числа е $n = p_1^{\alpha_1}...p_k^{\alpha_k}$. Тогава $\varphi(n) = n.(1 - \frac{1}{p_1})...(1 - \frac{1}{p_k})$.

# 12 Задача

***(Какво е необходимото и достатъчно условие едно линейно диофантово уравнение с две неизвестни да има решение)*** Нека $a, b, c \in \mathbb{Z}$. Необходимо и достатъчно условие линейното диофантово уравнение $ax + by = c$ с две неизвестни $x, y$ да има решение е $d = (a, b)$, $d \mid c$.

***(Как изглеждат всички решения на едно линейно диофантово уравнение с две неизвестни, ако е известно едно негово решение)*** Нека $a, b, c \in \mathbb{Z}$. Ако $(x_0, y_0)$ е решение на диофантовото уравнение $ax + by = c$ с неизвестни $x, y$, то всички решения са $x = x_0 - \frac{b}{d}t$, $y = y_0 + \frac{a}{d}t$, където $d = (a, b)$ и $t \in \mathbb{Z}$.

***(Какво е необходимото и достатъчно условие едно линейно сравнение с едно неизвестно да има решение)*** Нека $a, b, c \in \mathbb{Z}$. Необходимо и достатъчно условие линейното сравнение $ax \equiv c \pmod b$ да има решение е $(a, b) \mid c$.

***(Как изглеждат всички решения на едно линейно сравнение с едно неизвестно, ако е известно едно негово решение)*** Нека $a, b, c \in \mathbb{Z}$ и $x_0$ е едно решение на сравнението $ax \equiv c \pmod b$. Тогава всички решения са $(a, b)$ на брой и имат вида $x_0 + t.\frac{b}{(a,b)}$, където $t = 0, ..., (a, b) - 1$.

***(Кога два идеала в комутативен пръстен с единица са взаимно прости)*** Нека $R$ е комутативен пръстен с единица и $I \triangleleft R$ и $J \triangleleft R$. Идеалите $I, J$ са взаимно прости, ако $I + J = R$.

***(Формулирайте китайската теорема за остатъците за два идеала в комутативен пръстен с единица)*** Нека $R$ е комутативен пръстен с единица и $I \triangleleft R$, $J \triangleleft R$, като идеалите $I, J$ са взаимно прости. Тогава $R/IJ \cong (R/I) \times (R/J)$.

***(Формулирайте китайската теорема за остатъците за пръстена на целите числа)*** Нека $n_1, ..., n_k$ са две по две взаимно прости числа. Тогава Китайската теорема за остатъците гласи, че $\mathbb{Z}_{n_1...n_k} \cong \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k}$.

# 13 Задача

***(Коя пермутация наричаме цикъл)*** Нека $\Omega_n = \{1, 2, ..., n\}$. Нека $i_1, i_2, ..., i_{k-1}, i_k$ са различни числа от $\Omega_n$, а $\sigma$ е пермутацията, действаща по правилото: $\sigma(i_1) = i_2,\ \sigma(i_2) = i_3,\ ...,\ \sigma(i_{k-1}) = i_k,\ \sigma(i_k) = i_1$, а всички останали числа от $\Omega_n$ остават на място под действието на $\sigma$. Такава пермутация наричаме цикъл, а числото $k$ - дължина на цикъла.

***(Кои цикли наричаме независими)*** Два цикъла $(i_1 i_2 ... i_k)$ и $(j_1 j_2 ... j_s)$ наричаме независими, ако $\{i_1, i_2, ..., i_k\} \cap \{j_1, j_2, ..., j_s\} = \emptyset$.

***(Какъв е редът на произведението на два независими цикъла)*** Редът на произведението на два независими цикъла е равен на най-малкото общо кратно от редовете на двата независими цикъла.

***(Комутират ли циклите)*** Два независими цикъла $\sigma$ и $\tau$ комутират. В общия случай циклите, които не са независими, не комутират.

***(Комутират ли независимите цикли)*** Независимите цикли комутират винаги.

***(Какво е сечението на цикличните групи породени от независими цикли)*** Нека $\sigma, \tau \in S_n$ са независими цикли. Тогава $\langle\sigma\rangle \cap \langle\tau\rangle = \{id\}$.

***(Какво се получава като спрегнем цикъл с произволна пермутация)*** Нека $\sigma \in S_n$. Тогава за пермутацията $\tau = (i_1 ... i_k)$ е изпълнено, че $\sigma\tau\sigma^{-1} = (\sigma(i_1)...\sigma(i_k))$.

***(Какво наричаме транспозиция)*** Цикъл с дължина 2 наричаме транспозиция.

***(Всеки ли цикъл се представя като произведение на транспозиции)*** Всеки цикъл се представя като произведение на транспозиции.

***(Всеки ли цикъл се представя като произведение на независими транспозиции)*** НЕ всеки цикъл се представя като произведение на независими транспозиции.

***(Ако идентитетът е представен като произведение на транспозиции, какво можем да кажем за броя им)*** Ако идентитетът е представен като произведение на транспозиции, то броят им е четно число.

***(Какво наричаме знак на пермутация)*** Нека $\sigma \in S_n$ и $\sigma = \tau_1 ... \tau_k$, където $\tau_i$ са транспозиции, то $sign\sigma = (-1)^k$ наричаме знак на пермутацията $\sigma$.

***(Какво представлява алтернативната група)*** Множеството от всички четни пермутации е подгрупа $S_n$ и се нарича алтернативна група от степен $n$, като я бележим с $A_n$. Също

така $|A_n| = \frac{1}{2}n!$.

## 14 Задача

***(Кога казваме, че една група действа върху дадено множество)*** Нека $G$ е група, а $M$ е множество. Казваме, че $G$ действа върху $M$, ако съществува изображение $\Phi : G \times M \to M$, което на всеки елемент $g \in G$ и на всеки елемент $m \in M$ съпоставя елемент $g \circ m \in M$, като се изпълняват следните две условия:

1. $e \circ m = m$, $\forall m \in M$ ($e$ е единичният елемент на групата $G$);
2. $(g_1 g_2) \circ m = g_1 \circ (g_2 \circ m)$, $\forall g_1, g_2 \in G$, $\forall m \in M$.

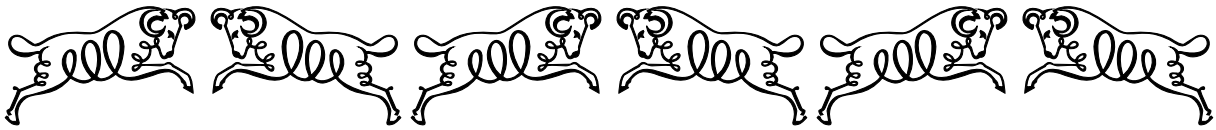
***(Какво е необходимото и достатъчно условие група да действа върху множество)*** Нека $G$ е група и $M$ е множество. Необходимо и достатъчно условие $G$ да действа върху $M$ е да съществува хомоморфизъм на групи $\varphi : G \to S_M$.

***(Какво наричаме стабилизатор на елемент на множество при действие на група върху това множество)*** Нека $G$ е група, която действа върху множеството $M$. Стабилизатор на елемент $m \in M$ наричаме $St_G(m) = \{g \in G \mid g \circ m = m\}$.

***(Какво наричаме орбита на елемент на множество при действие на група върху това множество)*** Нека $G$ е група, която действа върху множеството $M$. Орбита на елемент $m \in M$ наричаме $O_G(m) = \{g \circ m \mid g \in G\}$.

***(Какво наричаме дължина на орбита при действие на група върху множество)*** Нека $G$ е група, която действа върху множеството $M$. Дължина на орбита на елемент $m \in M$ наричаме $|O_G(m)|$.

***(Как се изразява дължината на орбитата при действие на крайна група върху множество)*** Нека $G$ е група, която действа върху множеството $M$, като $m \in M$. Тогава е изпълнено, че $|O_G(m)| = |G : St_G(m)|$.



## 15 Задача

***(Кое действие на група върху множество наричаме спрягане)*** Нека $G$ е група и $M = G$. Тогава изображението $\circ : G \times G \to G$ наричаме спрягане и то действа, като $g \circ m = gmg^{-1}$.

***(Какво представлява един клас спрегнати елементи)*** Нека $G$ е група и $M = G$. Тогава, при действието спрягане, за елемента $m \in M$, клас спрегнати с $m$ елементи наричаме $O(m) = \{gmg^{-1} \mid g \in G\}$.

***(Какво наричаме централизатор на елемент на група)*** Нека $G$ е група и $M = G$. Тогава, при действието спрягане, за елемента $m \in M$, централизатор на $m$ наричаме $St(m) = \{g \mid gmg^{-1} = m\} = \{g \mid gm = mg\} = C(m)$.

***(Какво наричаме център на група)*** Нека $G$ е група и $M = G$. Тогава, при действието спрягане, център на групата $G$ наричаме $Z(G) = \bigcap_{m \in G} St(m) = \{z \in G \mid \ \forall g \in G : zg = gz\}$.

***(Напишете формулата за класовете)*** Нека $G$ е група и $M = G$. Тогава формулага за класовете е $|G| = |Z(G)| + \sum_{i=1}^{s} |G : C(m_i)|$, $m_i$ са представители на различните неедноелементни орбити.

***(Какво можем да кажем за центъра на $p$-група)*** Нека $G$ е група и $|G| = p^k$, където $p$ е просто число, $p \in \mathbb{N}$. Тогава $Z(G) \neq \{e_G\}$, т.е. $G$ има нетривиален център.

***(Какво можем да кажем за група от ред квадрат на просто число)*** Нека $G$ е група и $|G| = p^2$, където $p$ е просто число. Тогава групата $G$ е абелева група.

***(Формулирайте теоремата на Поанкаре)*** Нека $G$ е крайна група и $H < G$, като $|G : H| = n$. Тогава съществува хомоморфизъм от $G$ в симетричната група $S_n$, чието ядро $N$ е сечението на всички спрегнати с $H$ подгрупи на $G$, и $N \trianglelefteq G$, $N \leq H$ и $n \mid |G : N| \mid n!$.

***(Формулирайте теоремата на Кейли)*** Всяка крайна група от ред $n$ е изоморфна на подгрупа на симетричната група $S_n, n \in \mathbb{N}$.

# 16 Задача

***(Какво наричаме пръстен от формални степенни редове на една променлива с коефициенти от даден пръстен)*** Нека $R$ е пръстен. Тогава пръстен от формални степенни редове на една променлива с коефициенти от $R$ наричаме $R[[x]] = \{a = (a_0, a_1, ..., a_n, ...) \mid a_i \in R\}$ със следните две операции:

$$a + b = c;\ \forall i : c_i = a_i + b_i$$

$$a.b = d;\ \forall k : d_k = \sum_{i+j=k} a_i b_j = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{j=0}^{k} a_{k-j} b_j.$$

***(Какво наричаме пръстен от полиноми на една променлива с коефициенти от даден пръстен)*** Нека $R$ е пръстен. Тогава пръстен от полиноми на една променлива с коефициенти от $R$ наричаме $R[x] = \{a = (a_0, a_1, ..., a_n, ...) \mid c_i \in R : \exists k\ \forall n > k : a_n = 0\}$ със следните две операции:

$$a + b = c;\ \forall i : c_i = a_i + b_i$$

$$a.b = d;\ \forall k : d_k = \sum_{i+j=k} a_i b_j = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{j=0}^{k} a_{k-j} b_j.$$

***(Кога два полинома са равни в алгебричен смисъл)*** Два полинома $a, b \in R[x]$ са равни в алгебричен смисъл, ако $\forall i : a_i = b_i$.

***(Кога два полинома са равни във функционален смисъл)*** Два полинома $a, b \in R[x]$ са равни във функционален смисъл, ако $\forall r \in R : a(r) = b(r)$.

***(Дайте пример на полиноми равни във функционален смисъл, но различни в алгебричен)***

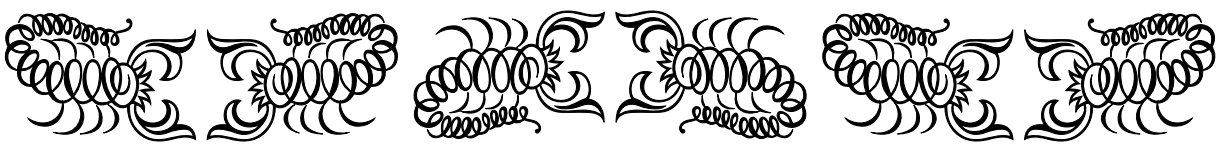
1. Полиномите от вида $x^p - x \in \mathbb{Z}_p[x]$, където $p$ е просто число, и полинома 0. Имаме, че за $\forall a \in \mathbb{Z}_p$ е изпълнено, че $a^p - a = 0$, следователно $x^p - x = 0$ във функционален смисъл, но $x^p - x \neq 0$ в алгебричен смисъл.
2. Нека $K = \{0, 1\}$ е пръстенът, състоящ се само от два елемента нула и единица. Тогава полиномите $x^2 + 1$ и $x^4 + 1$ над пръстена $K$ са равни във функционален смисъл, защото $0^2+1 = 0^4+1 = 1$ и $1^2+1 = 1^4+1 = 1+1 = 0$ над пръстена $K$, но не са равни в алгебричен смисъл.

***(Какво наричаме степен на полином)*** Нека $A[x]$ е пръстен от полиноми на една променлива $x$ с коефициенти от $A$. Тогава, ако $f \in A[x]$ и $f \neq 0$, то степента на полинома $f$ бележим с $\deg f$ и $\deg f = \max\{i \mid f_i \neq 0\}$. Ако $f \in A[x]$ и $f = 0$, то $\deg f = -\infty$.

***(Какво можем да кажем за степента на сумата на два полинома, ако знаем степените им)*** Нека $A[x]$ е пръстен от полиноми на една променлива $x$ с коефициенти от $A$. Тогава, ако $f, g \in A[x]$, то $\deg(f + g) \leq \max\{\deg f, \deg g\}$.

***(Какво можем да кажем за степента на произведението на два полинома с коефициенти от даден пръстен, ако знаем степените им)*** Нека $A[x]$ е пръстен от полиноми на една променлива $x$ с коефициенти от $A$. Тогава, ако $f, g \in A[x]$, то $\deg(fg) \leq \deg f + \deg g$.

***(Какво можем да кажем за степента на произведението на два полинома с коефициенти от област на цялост, ако знаем степените им)*** Нека $A[x]$ е пръстен от полиноми на една променлива $x$ с коефициенти от $A$, като нека и $A$ е област на цялост. Тогава, ако $f, g \in A[x]$, то $\deg(fg) = \deg f + \deg g$.



# 17 Задача

***(Какво наричаме корен на полином)*** Нека $\mathbb{F}$ е поле и $f \in \mathbb{F}[x]$, $\alpha \in \mathbb{F}$. Тогава $\alpha$ е корен на полинома $f$, ако $f(\alpha) = 0$.

***(Напишете необходимо и достатъчно условие елемент на пръстен да е корен на полином с коефициенти от този пръстен)*** Нека $F$ е комутативен пръстен с единица и $f \in F[x]$, $\alpha \in F$. Тогава $\alpha$ е корена на $f$, ако $f = (x - \alpha).q$ за някой полином $q \in F[x]$.

***(Напишете достатъчно условие два полинома от степен не надвишаваща*** $n$ ***да са равни в алгебричен смисъл)*** Нека $R$ е поле и $f, g \in R[x]$. Ако $\deg f, \deg g \leq n$, то необходимо и достатъчно условие полиномите $f = g$ в алгебричен смисъл е $\exists$ различни $\alpha_1, ..., \alpha_{n+1} \in R : f(\alpha_i) = g(\alpha_i)$за $i = 1, ..., n + 1$.

***(Формулирайте принципа за сравняване на коефициентите)*** Нека $K$ е област и $g_1, g_2 \in K[x]$. Нека $\deg g_1, \deg g_2 \leq n$ и съществуват два по два различни елемента $\alpha_1, ..., \alpha_{n+1}$ от $K$, за които $g_1(\alpha_i) = g_2(\alpha_i)$, $i = 1, ..., n + 1$. Тогава $g_1 = g_2$.

# 18 Задача

***(Какво наричаме характеристика на поле)***

1. Нека $\mathbb{F}$ е поле. Ако за всеки две различни цели числа $m$ и $n$ е изпълнено $m1 \neq n1$ (1 е единицата на полето $\mathbb{F}$), казваме, че $\mathbb{F}$ е поле с характеристика 0 и пишем $char\mathbb{F} = 0$. Ако съществуват различни цели числа $m$ и $n$, за които $m1 = n1$ и, например $m > n$, то за естественото число $m-n$ е изпълнено $(m-n)1 = 0$. В този случай най-малкото естествено число $p$ със свойството $p1 = 0$ наричаме характеристика на полето $\mathbb{F}$ и пишем $char\mathbb{F} = p$.
2. Нека $\mathbb{F}$ е поле. Тогава характеристиката на полето $\mathbb{F}$ наричаме $char\mathbb{F} = 0$, ако $|1|_{(\mathbb{F},+)} = \infty$ или $char\mathbb{F} = n$, ако $|1|_{(\mathbb{F},+)} = n$, където 1 е единицата на пръстена $\mathbb{F}$.

***(Какво число може да бъде характеристиката на едно поле)*** Характеристиката на едно поле може да бъде или 0, или просто число.

***(Нека характеристиката на полето*** $\mathbb{F}$ ***е нула. Какво е необходимото и достатъчно условие*** $n.a = 0$ ***за*** $a \in \mathbb{F}$***)*** Необходимото и достатъчно условие $n.a = 0$ е $n = 0$ или $a = 0$.

***(Нека характеристиката на полето*** $\mathbb{F}$ ***е различна от нула. Какво е необходимото и достатъчно условие*** $n.a = 0$ ***за*** $a \in \mathbb{F}$***)*** Нека $char\mathbb{F} = p$. Необходимото и достатъчно условие $n.a = 0$ е $p \mid n$ или $a = 0$.

***(Нека характеристиката на полето*** $\mathbb{F}$ ***е нула. Изоморфен образ на кое поле е подполе на*** $\mathbb{F}$***)*** Изоморфен образ е на полето $\mathbb{Q}$.

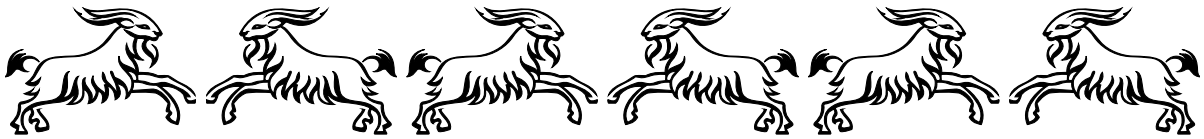
***(Нека характеристиката на полето $\mathbb{F}$ е различна от нула. Изоморфен образ на кое поле е подполе на $\mathbb{F}$)*** Изоморфен образ е на полето $\mathbb{Z}_p$, където $p = char\mathbb{F}$.

***(Кое поле е просто)*** Казваме, че едно поле $P$ е просто поле, ако няма собствени (т.е. различни от $P$) подполета.

***(Изоморфно на кои полета може да бъде едно просто поле)*** Едно просто поле може да бъде изоморфно на $\mathbb{Q}$ или на $\mathbb{Z}_p$, където $p = char\mathbb{F}$.

***(Ако характеристиката на едно поле е нула, на кое поле е изоморфно простото му подполе)*** Простото му подполе е изоморфно на $\mathbb{Q}$.

***(Ако характеристиката на едно поле е различна от нула, на кое поле е изоморфно простото му подполе)*** Простото му подполе е изоморфно на $\mathbb{Z}_p$, където $p$ е просто число.



# 19 Задача

***(Формулирайте теоремата за делене с частно и остатък на полиноми)*** Нека $\mathbb{F}$ е поле и $f, g \in \mathbb{F}[x], g \neq 0$. Тогава съществува единствена двойка полиноми $q, r \in \mathbb{F}[x]$, такива че $f = gq + r$ и $\deg r < \deg q$.

***(Какви са идеалите в пръстен от полиноми на една променлива с коефициенти от поле)*** Ако $\mathbb{F}$ е поле, то всеки идеал $I$ в пръстена $\mathbb{F}[x]$ е главен.

***(Какво е необходимото и достатъчно условие един идеал да е подмножество на друг идеал в пръстена от полиноми на една променлива с коефициенти от дадено поле)*** Нека $\mathbb{F}$ е поле и $f, g \in \mathbb{F}[x]$. Необходимо и достатъчно условие $(g) \subseteq (f)$ е $f \mid g$.

***(Какво е необходимото и достатъчно условие два идеала да са равни в пръстена от полиноми на една променлива с коефициенти от дадено поле)*** Нека $\mathbb{F}$ е поле и $f, g \in \mathbb{F}[x]$. Необходимо и достатъчно условие $(g) = (f)$ е $f \mid g$ и $g \mid f$, тоест да съществува $c \in \mathbb{F}^*$, такава че $g = cf$.

***(Какво наричаме най-голям общ делител на два полинома с коефициенти от дадено поле)*** Нека $\mathbb{F}$ е поле и $f, g \in \mathbb{F}[x]$ и поне единият от двата полинома $f$ и $g$ е ненулев. Казваме, че един полином $d$ е най-голям общ делител на $f$ и $g$, ако $(d) = (f) + (g) = ((f, g))$.

***(Какво наричаме най-малко общо кратно на два полинома с коефициенти от дадено поле)*** Нека $\mathbb{F}$ е поле и $f, g \in \mathbb{F}[x]$, $f \neq 0$, $g \neq 0$. Казваме, че един полином $k$ е най-малко общо кратно на $f$ и $g$, ако $(k) = (f) \cap (g) = ([f, g])$.

***(Какво е необходимото и достатъчно условие един полином да е най-голям общ делител на два полинома с коефициенти от дадено поле)*** Нека $\mathbb{F}$ е поле и $f, g \in \mathbb{F}$. Необходимо и достатъчно условие полиномът $d$ да е най-голям общ делител на полиномите $f$ и $g$ е да удовлетворява следните условия:

- $d \mid f$, $d \mid g$;
- ако $d_1 \mid f$, $d_1 \mid g$, то $d_1 \mid d$.

.

***(Какво е необходимото и достатъчно условие един полином да е най-малко общо кратно на два полинома с коефициенти от дадено поле)*** Нека $\mathbb{F}$ е поле и $f, g \in \mathbb{F}$. Необходимо и достатъчно условие полиномът $k$ да е най-малко общо кратно на полиномите $f$ и $g$ е да удовлетворява следните условия:

- $f \mid k$, $g \mid k$;
- ако $f \mid k_1$, $g \mid k_1$, то $k \mid k_1$.

***(Напишете равенството на Безу за полинома с коефициенти от дадено поле)*** Нека $\mathbb{F}$ е поле и за всеки два полинома $f, g \in \mathbb{F}[x]$ съществуват полиноми $u, v \in \mathbb{F}[x]$: $uf + vg = (f, g)$.

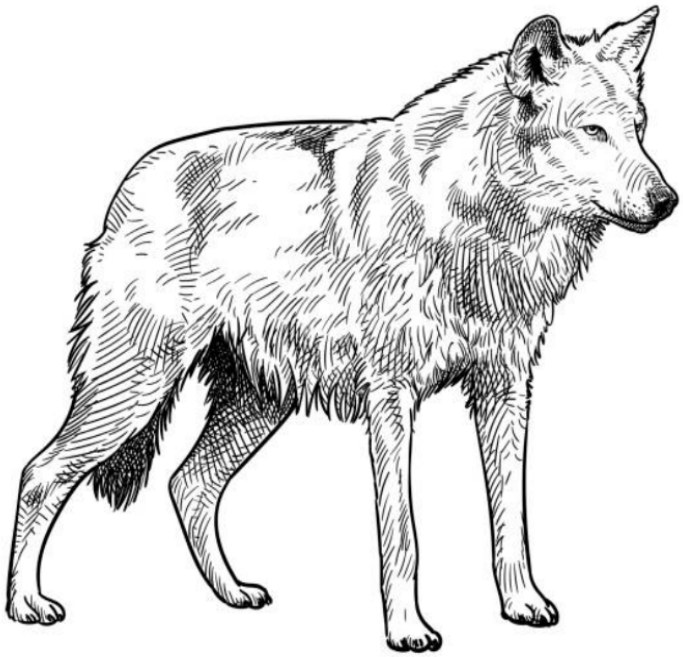
***(Какво наричаме неразложим полином в пръстен от полиноми на една променлива с коефициенти от дадено поле)*** Нека $f \in \mathbb{F}[x]$ и $\deg f > 0$, където $\mathbb{F}$ е поле. Казваме, че полиномът $f$ е неразложим над полето $\mathbb{F}$, ако не може да се представи като произведение на два полинома от $\mathbb{F}[x]$, чиито степени са по-малки от степента на $f$.

***(Какво е необходимото и достатъчно условие един полином да е неразложим в пръстен от полиноми на една променлива с коефициенти от дадено поле)*** Нека $\mathbb{F}$ е поле и $f \in \mathbb{F}[x]$. Необходимо и достатъчно условие полиномът $f$ да е неразложим над $\mathbb{F}$ е факторпръстенът $\mathbb{F}[x]/(f(x))$ да е поле.

***(Формулирайте основната теорема на аритметиката на полиномите с коефициенти от дадено поле)*** Всеки неконстантен полином $f \in \mathbb{F}[x]$ се разлага в произведение на неразложими над полето $\mathbb{F}$ полиноми. Ако $f = p_1...p_k = q_1...q_s$ са две такива разлагания, то $k = s$ и след евентуално преномериране на множителите, за всяко $i = 1, ..., k$ е изпълнено, че $p_i = a_i q_i$, $0 \neq a_i \in \mathbb{F}$.

***(Формулирайте схемата на Хорнер)*** Нека $f = a_0x^n + ... + a_n$, $g = x - \alpha$, $g \in F[x]$, където $F$ е пръстен с единица. Нека $f = gq + r$, където $\deg r < \deg q$, т.е. $r \in F$ и $q = b_0x^{n-1} + ... + b_{n-1}$. Тогава коефициентите на частното $q$ и остатъка $r$ се получават по формулите:

$$
\begin{aligned}
b_0 &= a_0, \\
b_1 &= a_1 + \alpha.b_0, \\
b_2 &= a_2 + \alpha.b_1, \\
&... \\
b_{n-1} &= a_{n-1} + \alpha.b_{n-2}, \\
r &= a_n + \alpha.b_{n-1}
\end{aligned}
$$



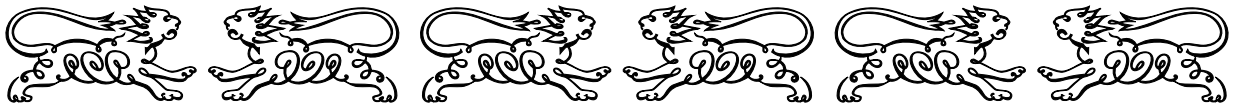
## 20 Задача

***(Ако един полином с коефициенти от поле $\mathbb{F}$ е неразложим над $\mathbb{F}$, посочете поле изоморфно на разширение на $\mathbb{F}$, в което разширение полиномът има корен)*** Нека $f \in \mathbb{F}[x]$ е неразложим над $\mathbb{F}$. Тогава поле, което е изоморфно на разширение на $\mathbb{F}$, в което разширение полиномът $f$ има корен, е $\mathbb{F}[x]/(f(x))$.

***(Какво наричаме поле на разлагане на полином с коефициенти от дадено поле)*** Нека $f \in \mathbb{F}[x]$, $\deg f > 0$ и $\mathbb{L}$ е разширение на полето $\mathbb{F}$, което съдържа всички корени на полинома $f$. Сечението на всички подполета на $\mathbb{L}$, съдържащи полето $\mathbb{F}$ и всички корени на полинома $f$, наричаме поле на разлагане на $f$ над полето $\mathbb{F}$.

***(Напишете формулите на Виет)*** Нека $\mathbb{F}$ е поле и $f \in \mathbb{F}[x]$ е такъв, че $f = a_0x^n + ... + a_n$ и $\alpha_1, \alpha_2, ..., \alpha_n$ са корените на $f$ (лежащи в подходящо разширение на полето $\mathbb{F}$). Тогава:

$$\alpha_1 + ... + \alpha_n = -\frac{a_1}{a_0}$$
$$\alpha_1\alpha_2 + ... + \alpha_{n-1}\alpha_n = \frac{a_2}{a_0}$$
$$...$$
$$\alpha_1\alpha_2...\alpha_n = (-1)^n\frac{a_n}{a_0}$$



## 21 Задача

***(Какво наричаме $k$-кратен корен на полином)*** Нека $f \in \mathbb{F}[x]$, $\mathbb{K}$ е разширение на $\mathbb{F}$ и $\alpha \in \mathbb{K}$. Казваме, че $\alpha$ е $k$-кратен корен на $f$ $(k \geq 1)$, ако $f = (x-\alpha)^k g$, $g \in \mathbb{K}[x]$ и $g(\alpha) \neq 0$. При $k = 1$ казваме, че $\alpha$ е прост корен на $f$, а при $k > 1$ - че е кратен корен на $f$.

***(Какво е необходимото и достатъчно условие елемент на поле с характеристика нула да е $k$-кратен корен на полином с коефициенти от това поле)*** Нека $\mathbb{F}$ е поле, като $char\mathbb{F} = 0, f \in \mathbb{F}[x]$, $\mathbb{K}$ е разширение на $\mathbb{F}$ и $\alpha \in \mathbb{K}$. Тогава $\alpha$ е $k$-кратен корен на $f$ точно когато $f(\alpha) = f'(\alpha) = ... = f^{(k-1)}(\alpha) = 0$ и $f^{(k)}(\alpha) \neq 0$.

***(Какво е необходимото и достатъчно условие елемент на поле да е кратен корен на полином с коефициенти от това поле)*** Нека $f \in \mathbb{F}[x]$. Тогава $f$ има кратен корен $\alpha$ тогава и само тогава, когато $f(\alpha) = f'(\alpha) = 0$, тоест има общ корен с производната си.

## 22 Задача

***(Какво наричаме пръстен от полиноми на $n$ променливи с коефициенти от област)*** Нека $A$ е област. Тогава пръстенът от полиноми на $n$ променливи с коефициенти от $A$ се дефинира индуктивно по следния начин: $A[x_1, ..., x_n] = (A[x_1, ..., x_{n-1}])[x_n] = ... = A[x_1][x_2]...[x_{n-1}][x_n]$.

***(Какво представлява лексикографската наредба)*** Нека $F$ е пръстен и $F[x_1, ..., x_n]$ е пръстенът на полиномите на $n$ променливи, $n \in \mathbb{N}$. Нека $u, v \in F[x_1, ..., x_n]$, като $u = ax_1^{i_1}...x_n^{i_n}$,

$v = bx_1^{j_1}...x_n^{j_n}$ са два неподобни едночлена ($a, b \in F, a \neq 0, b \neq 0$). Казваме, че $u \succ v$, ако съществува естествено число $k \leq n$, такова че $i_1 = j_1, ..., i_{k-1} = j_{k-1}$, но $i_k > j_k$.

***(Формулирайте лемата за старшия едночлен за полиноми на** $n$ **променливи с коефициенти от област)*** Нека $A$ е област и $f, g \in A[x_1, ..., x_n], f \neq 0, g \neq 0$. Тогава старшият едночлен на полинома $fg$ е равен на произведението от старшите едночлени на $f$ и $g$.

***(Какво наричаме симетричен полином)*** Нека $A$ е пръстен и $f = (x_1, ..., x_n), f \in A[x_1, ..., x_n]$. Казваме, че $f$ е симетричен полином, ако за всяка пермутация $\sigma$ от симетричната група $S_n$ е изпълнено равенството $f(x_1, ..., x_n) = f(x_{\sigma(1)}, ..., x_{\sigma(n)})$.

***(Кои полиноми наричаме елементарни симетрични полиноми)*** Елементарните симетрични полиноми на $n$ променливи са следните симетрични полиноми:

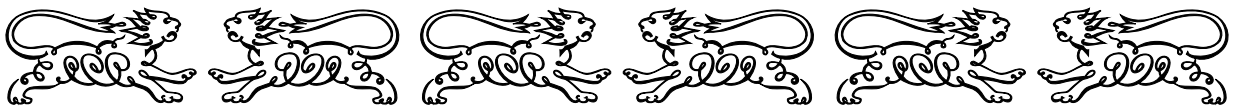
$$\sigma_1 = \sigma_1(x_1, ..., x_n) = x_1 + x_2 + ... + x_n,$$
$$\sigma_2 = \sigma_2(x_1, ..., x_n) = x_1x_2 + x_1x_3 + ... + x_{n-1}x_n,$$
$$\sigma_3 = \sigma_3(x_1, ..., x_n) = x_1x_2x_3 + x_1x_2x_4 + ... + x_{n-2}x_{n-1}x_n,$$
$$...$$
$$\sigma_n = \sigma_n(x_1, ..., x_n) = x_1x_2...x_n.$$

***(Формулирайте основната теорема за симетричните полиноми)*** Нека $A$ е област и $f = f(x_1, ..., x_n) \in A[x_1, ..., x_n]$ е симетричен полином. Тогава съществува единствен полином $g$ на $n$ променливи с коефициенти от $A$, такъв че $f(x_1, ..., x_n) = g(\sigma_1, ..., \sigma_n)$.

***(Формулирайте следствието от основната теорема за симетричните полиноми)*** Нека $\mathbb{F}$ е поле, $f = a_0x^n + ... + a_n \in \mathbb{F}[x]$ и $\alpha_1, ..., \alpha_n$ са всички корени на $f$ (лежащи в подходящо разширение на $\mathbb{F}$). Тогава, ако $h(x_1, ..., x_n) \in \mathbb{F}[x_1, ..., x_n]$ е симетричен полином, то $h(\alpha_1, ..., \alpha_n) \in \mathbb{F}$.

***(Кои полиноми наричаме степенни сборове)*** Нека $A$ е пръстен и $f \in A[x_1, ..., x_n]$, където $n \in \mathbb{N}$. Тогава $S_k = x_1^k + x_2^k + ... + x_n^k$, $k = 0, 1, 2, ...$ се нарича степенен сбор. По определение $S_0 = n$.

***(Напишете формулите на Нютон за връзката между елементарните симетрични полиноми и степенните сборове)*** Нека $S_k = x_1^k + x_2^k + ... + x_n^k$, където $n \in \mathbb{N}$ и $k = 0, 1, 2, ...$ е степенният сбор на $n$ променливи, а $\sigma_1, ..., \sigma_k$ са елементарните симетрични полиноми. Тогава равенството от вида $S_k - \sigma_1 S_{k-1} + \sigma_2 S_{k-2} - ... + (-1)^{k-1}\sigma_{k-1}S_1 + (-1)^k k\sigma_k = 0$ се наричат формули на Нютон.



# 23 Задача

***(Кое поле наричаме алгебрически затворено)*** Ще казваме, че едно поле $\mathbb{F}$ е алгебрически затворено, ако всеки неконстантен полином с коефициенти от $\mathbb{F}$ има корен в $\mathbb{F}$.

***(Какво е полето, ако всеки полином с коефициенти от него се разлага на линейни множители)*** Ако за полето $\mathbb{F}$ е изпълнено, че за всеки полином $f \in \mathbb{F}[x]$ корените на $f$ са от $\mathbb{F}$, т.е. $f$ се разлага в произведение на линейни множители, то полето $\mathbb{F}$ е алгебрически затворено.

***(На какви множители се разлага полином с коефициенти от алгебрически затворено поле над това поле)*** Нека $\mathbb{F}$ е поле и $f \in \mathbb{F}[x]$. Тогава $f$ се разлага на линейни множители с коефициенти от полето $\mathbb{F}$ над самото поле $\mathbb{F}$.

***(Кои са неразложимите полиноми с коефициенти от поле, ако полето е алгебрически затворено)*** Нека $\mathbb{F}$ е поле, което е алгебрически затворено. Тогава неразложимите полиноми с коефициенти от полето $\mathbb{F}$ са полиномите от първа степен (линейни полиноми от $\mathbb{F}[x]$)

***(Какво е полето, ако единствените неразложими полиноми с коефициенти от това поле са полиномите от първа степен)*** Полето $\mathbb{F}$, в което единствените неразложими полиноми с коефициенти от $\mathbb{F}$ са полиномите от първа степен, е алгебрически затворено.

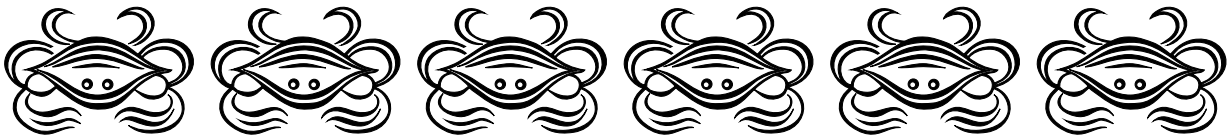
***(Какво е полето на разлагане на полином с коефициенти от алгебрически затворено поле)*** Нека $\mathbb{F}$ е алгебрически затворено поле. Тогава полето на разлагане на полином с коефициенти от $\mathbb{F}$ съвпада с $\mathbb{F}$.

***(Формулирайте лемата на Гаус за полиноми с реални коефициенти)*** Всеки неконстантен полином с реални коефициенти има поне един комплексен корен.

***(Формулирайте теоремата на Даламбер)*** Полето на комплексните числа $\mathbb{C}$ е алгебрически затворено.

***(Кои са неразложимите полиноми над полето на комплексните числа)*** Неразложимите полиноми над полето на комплексните числа са полиномите от първа степен.

***(Кои са неразложимите полиноми над полето на реалните числа)*** Неразложимите полиноми над полето на реалните числа са полиномите от първа степен и полиномите от втора степен с отрицателна дискриминанта.



# 24 Задача

***(Напишете определението за примитивен полином)*** Нека $f = a_0x^n + ... + a_n \in \mathbb{Z}[x]$. Казваме, че $f$ е примитивен полином, ако най-големият общ делител на коефициентите му $a_0, ..., a_n$ е равен на 1, т.е. коефициентите му са (в съвкупност) взаимно прости.

***(Как се представя полином с рационални коефициенти чрез примитивен полином)*** Ако $g \in \mathbb{Q}[x]$, то $g$ може да се представи във вида $g = \frac{r}{q}f$, където $f \in \mathbb{Z}[x]$ е примитивен полином, $r, q \in \mathbb{Z}$.

***(Напишете необходимо и достатъчно условие един полином с цели коефициенти да е примитивен)*** Необходимо и достатъчно условие $f \in \mathbb{Z}[x]$ да е примитивен полином

е за всяко просто число $p$ полиномът $\overline{f} \in \mathbb{Z}_p[x]$ е ненулев.

***(Формулирайте лемата на Гаус за полиноми с цели коефициенти)*** Произведение на два примитивни полинома също е примитивен полином.

***(Какво можем да кажем, ако произведението на примитивен полином с рационално число е полином с цели коефициенти)*** Нека $h \in \mathbb{Z}[x]$ е примитивен полином, $c \in \mathbb{Q}$ и $ch \in \mathbb{Z}[x]$. Тогава $c \in \mathbb{Z}$.

***(Напишете необходимо и достатъчно условие полином с цели коефициенти да е неразложим над полето на рационалните числа)*** Нека $f \in \mathbb{Z}[x]$. Необходимо и достатъчно условие полиномът $f$ да е неразложим над полето $\mathbb{Q}$ е да е неразложим над пръстена $\mathbb{Z}$.

***(Напишете необходимо и достатъчно условие полином с цели коефициенти да е неразложим над пръстена на целите числа)*** Нека $f \in \mathbb{Z}[x]$. Необходимо и достатъчно условие полиномът $f(x)$ да е неразложим над пръстена на целите числа е полиномът $f(ax+b)$ да е неразложим над пръстена на целите числа, $a, b \in \mathbb{Z}$, $a \neq 0$. **Забележка: Възможно тълкуване на този въпрос е да бъде приет като дуален на предишния, откъдето трябва да се посочи, че необходимото и достатъчно условие е полиномът да е неразложим над рационалните числа. Препоръчително е да се напише второто, а първото да се знае за задачи.**

***(Напишете необходимо и достатъчно условие полином с цели коефициенти да е разложим над полето на рационалните числа)*** Нека $f \in \mathbb{Z}[x]$. Необходимо и достатъчно условие полиномът $f$ да е разложим над полето $\mathbb{Q}$ е да е разложим над пръстена $\mathbb{Z}$.

***(Напишете необходимо и достатъчно условие полином с цели коефициенти да е разложим над пръстена на целите числа)*** Нека $f \in \mathbb{Z}[x]$. Необходимо и достатъчно условие полиномът $f(x)$ да е разложим над пръстена на целите числа е полиномът $f(ax+b)$ да е разложим над пръстена на целите числа, $a, b \in \mathbb{Z}$, $a \neq 0$. **Забележка: Възможно тълкуване на този въпрос е да бъде приет като дуален на предишния, откъдето трябва да се посочи, че необходимото и достатъчно условие е полиномът да е разложим над рационалните числа. Препоръчително е да се напише второто, а първото да се знае за задачи.**

***(Напишете необходимо и достатъчно условие едно рационално число да е корен на полином с цели коефициенти)*** Нека $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$, $a_n \neq 0$, $\alpha = \frac{p}{q}$, където $p, q \in \mathbb{Z}$, $(p, q) = 1$. Необходимо и достатъчно условие числото $\alpha$ да е корен на полинома $f$ е:

- $p \mid a_n$ и $q \mid a_0$;
- $\forall m \in \mathbb{Z} : (p - mq) \mid f(m)$.

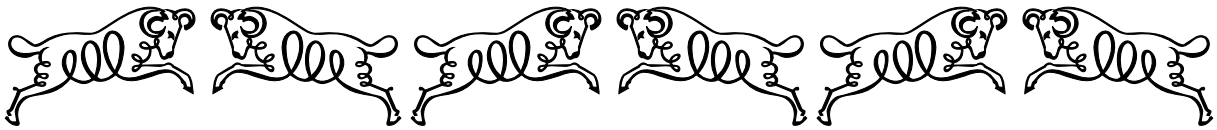
***(Формулирайте критерия на Айзенщайн)*** Нека $f = a_0x^n + ... + a_n \in \mathbb{Z}[x]$ и съществува просто число $p$, удовлетворяващо следните условия:

- $p \nmid a_0$;

- $p \mid a_1, ..., a_n$;
- $p^2 \nmid a_n$.

Тогава полиномът $f$ е неразложим над $\mathbb{Q}$.

***(Формулирайте редукционния критерий)*** Нека $f = a_0x^n + ... + a_n \in \mathbb{Z}[x]$. Ако $p$ е просто число, което не дели $a_0$ и редукционният полином $\overline{f(x)} \in \mathbb{Z}_p[x]$ е неразложим над $\mathbb{Z}_p$, то $f(x)$ е неразложим над $\mathbb{Q}$.



# 25 Задача

***(Какъв може да е броят на елементите на крайно поле)*** Нека $F$ е крайно поле и $charF = p$. Тогава $|F| = p^n$ за някое естествено число $n$.

***(Какво е необходимото и достатъчно условие за дадено естествено число да съществува крайно поле, чийто брой на елементите е това число)*** Нека $n \in \mathbb{N}$. Необходимо и достатъчно условие да съществува поле $\mathbb{F}$, за което $|\mathbb{F}| = n$ е числото $n$ да е степен на просто число.

***(Колко крайни полета с фиксиран брой елементи съществуват с точност до изоморфизъм)*** За всяко просто число $p$ и за всяко число $k \in \mathbb{N}$ съществува единствено с точност до изоморфизъм поле с $p^k$ елемента.

***(Каква е мултипликативната група на крайно поле)*** Мултипликативната група на всяко крайно поле е циклична.

***(Какво е необходимото и достатъчно условие едно крайно поле да е подполе на друго крайно поле)*** Нека $\mathbb{F}$ е крайно поле и $\mathbb{K}$ е също крайно поле, за които е изпълнено, че $|\mathbb{F}| = p^n$ и $|\mathbb{K}| = q^m$, за $p, q$ - прости числа и $n, m \in \mathbb{N}$. Необходимо и достатъчно условие за $\mathbb{K} < \mathbb{F}$ е $charK = charF$, т.е. $p = q$ и $m \mid n$.

# 26 Задача

***(Напишете определението за циклотомичен полином)*** Нека $\zeta_1, ..., \zeta_{\varphi(n)}$ са примитивните $n$-ти корени на единицата. Полинома $\Phi_n = \Phi_n(x) = \prod_{k=1}^{\varphi(n)} (x - \zeta_k) \in \mathbb{C}$ ще наричаме $n$-ти циклотомичен полином.

***(Как се представя полиномът $x^n - 1$ (за някое естествено число $n$), като произведение на циклотомични полиноми)*** За всяко естествено число $n$ е в сила равенството

$$x^n - 1 = \prod_{d|n} \Phi_d$$

където произведението е взето по всички естествени делители на числото $n$.

***(Как се изразява $\Phi_n$ $(n \in \mathbb{N})$, чрез $\Phi_k$ за $k = 1, ..., n-1$)*** Полиномът $\Phi_n$ се изразява по следния начин:

$$\Phi_n = \frac{x^n - 1}{\prod_{\substack{k|n \\ k<n}} \Phi_k}.$$

***(Какви числа са коефициентите на даден циклотомичен полином)*** За всяко естествено число $n$ полиномът $\Phi_n$ е с цели коефициенти.

***(Как се изразява циклотомичен полином, като се използва функцията на Мъобиус)*** За всяко естествено число $n$ е в сила равенството

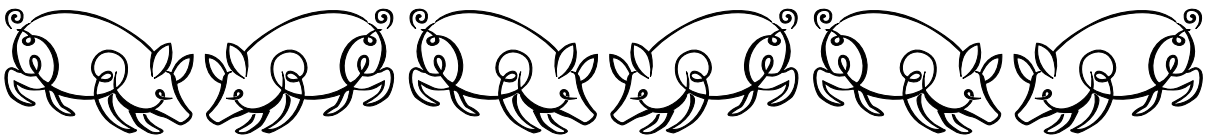
$$\Phi_n = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}.$$

***(Разложим или неразложим е даден циклотомичен полином над полето на рационалните числа)*** За всяко естествено число $n$ полиномът $\Phi_n(x)$ е неразложим над полето $\mathbb{Q}$.

***(Разложим или неразложим е даден циклотомичен полином над пръстена на целите числа)*** За всяко естествено число $n$ полиномът $\Phi_n(x)$ е неразложим над пръстена $\mathbb{Z}$.

***(Как се разлага на неразложими полиноми полиномът $x^n - 1$ (за някое естествено число $n$))*** Равенството $x^n - 1 = \prod_{d|n} \Phi_d(x)$ е разлагането на полинома $x^n - 1$ в произведение на неразложими над $\mathbb{Q}$ множители.

***(Формулирайте теоремата на Ведербърн)*** Всяко крайно тяло е поле.



# Благодарности

Специални благодарности на **Емилиян Рогачев**, който се погрижи да прочете и редактира файла грижливо, където беше необходимо. Специални благодарности на колегите от специалност **Информатика, 1 курс**, които бяха до автора дори в моментите, в които авторът обмисляше прекратяването на дейността си по този файл и неговото развитие.