# Lista 1

## Arytmetyka modularna

**Zadanie 1** *Wykaż, że dla dla $n \in \mathbb{N}_+$ zachodzi*

$$\forall x \in \mathbb{Z} \exists! k \in \mathbb{Z} \exists! r \in \mathbb{Z}_n \;\; x = k \cdot n + r.$$

*gdzie $\mathbb{Z}_n = \{0, \ldots, n-1\}$. Jest to dzielenie z resztą. Jesli $x = k \cdot n + r$ i $r \in \mathbb{Z}_n$, to definiujemy $(x)_n = r$.*

***Zadanie 2*** *Dla dowolnych $a, b \in \mathbb{Z}$ i $n \in \mathbb{N}_+$ udowodnij, że*

1. $((a)_n)_n = (a))_n$,
2. $(a + b)_n = ((a)_n) + (b)_n)_n$,
3. $(a \cdot b)_n = ((a)_n) \cdot (b)_n)_n$,

***Zadanie 3*** *Dla dowolnych $x, y \in \mathbb{Z}$ i $n \in \mathbb{N}_+$ definiujemy*

$$x +_n y = (x + y)_n oraz x \cdot_n y = (x \cdot y)_n.$$

*Pokaż, że $(\mathbb{Z}_n, +_n)$ jest grupą abelową, tzn.*

1. $\forall x, y \in \mathbb{Z}_n \; x +_n y \in \mathbb{Z}_n$,
2. $\forall x, y, z \in \mathbb{Z}_n \; (x +_n y) +_n z = x +_n (y +_n z)$,
3. $\forall x \in \mathbb{Z}_n \; x +_n 0 = x = 0 +_n x$,
4. $\forall x \in \mathbb{Z}_n \exists y \in \mathbb{Z}_n \; x +_n y = 0 = y +_n x$,
5. $\forall x, y \in \mathbb{Z}_n \; x +_n y = y +_n x$.

***Zadanie 4*** *Pokaż, że jeżeli $1 < n \in \mathbb{N}_+$, to $(\mathbb{Z}_n, +_n, \cdot_n, 0, 1)$ jest pierścieniem przemiennym z jednością, tzn.*

1. $(\mathbb{Z}_n, +_n)$ *jest grupą abelową,*
2. $\cdot_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$,
3. $\forall x, y, z \in \mathbb{Z}_n \; (x \cdot_n y) \cdot_n z = x \cdot_n (y \cdot_n z)$,
4. $\forall x, y, z \in \mathbb{Z}_n \; (x +_n y) \cdot_n z = (x \cdot_n z) +_n (y \cdot_n z)$,
5. $\forall x \in \mathbb{Z}_n \; x \cdot_n 1 = 1 \cdot_n x$,
6. $\forall x, y \in \mathbb{Z}_n x \cdot_n y = y \cdot_n y$.

***Definicja 1*** *Dla dodatniej liczby naturalnej $n \in \mathbb{N}_+ = \mathbb{N} \setminus \{0\}$ definiujemy $(\mathbb{Z}, \equiv \mod n)$ jek następuje*

$$(\forall a, b \in \mathbb{Z}) \;\; (a \equiv b \mod n) \longleftrightarrow (n | (a - b)).$$

***Zadanie 5*** *Sprawdź, czy dla $n \in \mathbb{N}_+$ uporządkowana para $(\mathbb{Z}, \equiv \mod n)$ jest relacją równoważności na zbiorze liczb całkowitych.*

***Zadanie 6*** *Dla dowolnego $n \in \mathbb{N}_+$ wyznacz przestrzeń ilorazową*

$$\mathbb{Z}/_{\equiv \mod n} = \{[x] : x \in \mathbb{Z}\}$$

*gdzie $[x] = \{y \in \mathbb{Z} : x \equiv y \mod n\}$ jest klasą bstrakcji elementu $x \in \mathbb{Z}$ dla relacji $(\mathbb{Z}, \equiv \mod n)$.*

***Zadanie 7*** *Dla $n \in \mathbb{N}_+$ i $a, c \in \mathbb{Z}$ wykaż, że jeżeli $a \equiv b \mod n$ to*

1. $a + c \equiv b + c \mod n$,
2. $a \cdot c \equiv b \cdot c \mod n$,
3. *jeżeli* $0 < k \in \mathbb{N}$, *to* $a^k \equiv b^k \mod n$,
4. *ponadto* $a \equiv (a)_n \mod n$.

***Zadanie 8*** *W zbiorze $\mathbb{Z}/_{\equiv \mod n}$ $(n \in \mathbb{N}_+)$ definiujemy działania: dla dowolnych $x, y \in \mathbb{Z}$*

$$[x] \boxplus_n [y] = [x + y], \quad [x] \boxdot_n [y] = [x * y].$$

*Udowodnij, że istnieje bijekcja $f : \mathbb{Z}_n \to \mathbb{Z}/_{\equiv \mod n}$ taka, że dla dowolnych $x, y \in \mathbb{Z}_n$ zachodzi warunek:*

$$f(x +_n y) = f(x) \boxplus_n f(y), \quad f(x \cdot_n y) = f(x) \boxplus_n f(y).$$

***Zadanie 9*** *Na podstawie poprzedniego zadania, wykaż, że dla $1 < n \in \mathbb{N}_+$ $(\mathbb{Z}/_{\equiv \mod n}, \boxplus_n, \boxdot_n, [0], [1])$ jest przemiennym pierścieniem z jednością.*

# Lista 2

## Elementy teorii liczb

***Zadanie 1*** *Stosując rozszerzony algorytm Euklidesa, proszę znaleźć rozwiązanie następującego równania diofantycznego (w liczbach całkowitych)*

$$128 \cdot x + 89 \cdot y = 15.$$

***Zadanie 2*** *Proszę znaleźć wszystkie rozwiązania, następującego równania diofantycznego*

$$2012 \cdot x + 1999 \cdot y = 1000.$$

***Zadanie 3*** *Proszę rozwiązać następujące równanie diofantyczne*

$$2 \cdot x + 3 \cdot y + 5 \cdot z = 7.$$

***Zadanie 4*** *Niech $n \in \mathbb{N} \setminus \{0\}$ będzie dodatnią liczbą naturalną oraz $f \in \mathbb{Z}[x]$ wielomianem jednej zmiennej o współczynnikach całkowitych. Proszę udowodnić*

$$(\forall a, b \in \mathbb{Z})\ (a \equiv b \mod n \longrightarrow f(a) \equiv f(b) \mod n).$$

***Zadanie 5*** *Niech będzie dana liczba* $n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots a_m 10^m$*, gdzie* $a_k \in \mathbb{Z}_{10} \wedge k \in \mathbb{Z}_{m+1}$ *będzie liczbą naturalną zapisana w układzie dziesiętnym. Proszę udowodnić, że* $n$ *jest podzielna przez* $9$ *wtedy i tylko wtedy gdy suma cyfr* $a_0 + \ldots + a_m \equiv 0 \mod 9$*. Jaka jest cecha podzielności liczby naturalnej przez liczbę* $3$*?*

***Zadanie 6*** *Proszę udowodnić, że każda liczba zapisana w układzie* $10$*-tnym jest podzielna przez* $11$ *wtedy i tylko wtedy gdy* $a_0 - a_1 + a_2 - a_3 + \ldots + (-1)^m a_m \equiv 0 \mod 11$*. Dla jakich* $n \in \mathbb{N}$*, liczba* $10^n + 1$ *jest podzielna przez* $11$*?*

***Zadanie 7*** *Proszę wyznaczyć przedostatnią cyfrę liczby* $3^{2012} + 11^{2011}$*, zapisanej w układzie dziesiętnym.*

***Zadanie 8*** *Nie korzystając z twierdzenia o multiplikatywności funkcji Eulera* $\varphi$*, proszę udowodnić że, jeśli* $p, q$ *są dwiema różnymi liczbami pierwszymi, to* $\varphi(pq) = \varphi(p)\varphi(q)$*.*

***Zadanie 9*** *Proszę wyznaczyć. wszystkie rozwiązania układu równań diofantycznych:*

$$\begin{cases} x \equiv & 12 \mod 5 \\ x \equiv & 33 \mod 7 \\ x \equiv & 76 \mod 9 \\ x \equiv & 22 \mod 13 \end{cases}$$

# Lista 3

## Grupy, podgrupy

**Oznaczenie:** $H \leq G$ *oznacza, że* $H$ *jest podgrupą grupy* $G$*.*

***Zadanie 1*** *Proszę sprawdzić, czy następujące wzory określają działanie na zbiorze. Jeśli tak, sprawdzić łączność oraz przemienność działań.*

1. $m \odot n = m^n$ *na* $\mathbb{N}$*,*
2. $m \odot n = NWD(m, n)$ *na* $\mathbb{N}$*,*
3. $a \odot b = \frac{a-b}{3}$ *na* $\mathbb{Q}$*,*
4. $x \vee y = \max\{x, y\}$*,* $x \wedge y = \min\{x, y\}$ *na* $\mathbb{R}$*,*
5. $f \vee g = \max\{f, g\}$*,* $f \wedge g = \min\{f, g\}$ *na* $C(\mathbb{R})$*,*
6. $f \vee g = \max\{f, g\}$*,* $f \wedge g = \min\{f, g\}$ *na* $C_1([0, 1])$ *(- zbiór wszystkich funkcji o ciągłej pochodnej na* $[0, 1]$*).*

***Zadanie 2*** *Czy istnieje działanie* $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$*, które spełnia warunki:*

1. $\forall x \in \mathbb{Z} \;\; f(x, 0) = x = f(0, x)$*,*
2. $\forall x \in \mathbb{Z} \;\; x \neq 0 \longrightarrow |\{y \in \mathbb{Z} : \;\; f(x, y) = 0 = f(y, x)\}| = \aleph_0$*.*

***Zadanie 3*** *Czy istnieje działanie $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, które spełnia warunki:*

1. $\forall x \in \mathbb{Z} \;\; f(x,0) = x = f(0,x)$,
2. $\forall x \in \mathbb{Z} \;\; |\{y \in \mathbb{Z} : \;\; f(x,y) = 0 = f(y,x)\}| = \aleph_0$,.

***Zadanie 4*** *Proszę sprawdzić, które zbiory z działaniami stanowią grupę:*

1. $\{3n : \; n \in \mathbb{Z}\}$ *z mnożeniem,*
2. $\{3n : \; n \in \mathbb{Z}\}$ *z dodawaniem,*
3. $(P(X), \cap)$,
4. $(P(X), \cup)$,
5. $(P(X), \triangle)$, *gdzie* $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

***Zadanie 5*** *Proszę zbudować tabelkę działań dla następujących grup izometrii:*

1. *trójkąta równobocznego,*
2. *kwadratu,*
3. *prostokąta, który nie jest kwadratem,*
4. *sześciokąta foremnego.*

***Zadanie 6*** *Proszę udowodnić:* $(G, \cdot)$ *jest grupą wtedy i tylko wtedy gdy*

$0$ $\cdot \in G^{G \times G}$,

$1$ $\cdot$ *jest łączne,*

$2$ $(\forall a, b \in G)(\exists! x \in G)\; a \cdot x = b$,

$3$ $(\forall a, b \in G)(\exists! y \in G)\; y \cdot a = b$,

***Zadanie 7*** *Niech $X$-dowolny niepusty zbiór, $G = \{f \in X^X : \; f - bijekcja\}$ oraz $(f \odot g)(x) = f(g(x))$ jest składaniem funkcji. Proszę pokazać, że $(G, \odot)$ jest grupą.*

***Zadanie 8*** *Niech $\emptyset \neq X_0 \subset X$. Czy zbiór*

$$\{f \in X^X : \; f - bijekcja \wedge f \restriction_{X_0} = id\}$$

*stanowi grupę ze względu na superpozycję (składanie) funkcji?*

***Zadanie 9*** *Niech $(G, \cdot)$ będzie grupą. Ponadto, niech $\emptyset \neq \mathscr{G} \subseteq \{H \in P(G) : H \leq G\}$ o następującej własności:*

$$(\forall A, B \in \mathscr{G})(\exists C \in \mathscr{G}) \;\; A \subseteq C \wedge B \subseteq C.$$

*Proszę udowodnić że $\bigcup \mathscr{G} \leq G$.*

***Zadanie 10*** *Niech $(G, \cdot)$ będzie grupą, proszę sprawdzić, czy podzbiór*

$$Z(G) = \{g \in G : \; (\forall x \in G)\; g \cdot x = x \cdot g\}$$

*stanowi podgrupę grupy $G$. $Z(G)$ nazywamy centrum grupy.*

***Zadanie 11*** *Niech $(G,\cdot)$ będzie grupą, $a \in G$, proszę sprawdzić, czy podzbiór*

$$C_a = \{g \in G : \ g \cdot a = a \cdot g\}$$

*stanowi podgrupę grupy $G$. $C_a$ nazywamy centralizatoorem elementu $a$.*

***Zadanie 12*** *Niech $(G,\cdot)$ będzie grupą macierzy rzeczywistych odwracalnych stopnia 2 z mnożeniem macierzy. Niech*

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbb{R} \wedge a \neq 0 \right\}.$$

*Czy $H \leq G$*

***Zadanie 13*** *Niech będzie dana tabelka działania grupy skończonej. Proszę udowodnić, że każdy wiersz (kolumna) w tabelce składa się z różnych elementów.*

***Zadanie 14*** *Proszę wyznaczyć wszystkie tabelki działań dla grupy mocy 4.*

***Zadanie 15*** *Niech będą dane dwie macierze*

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ oraz } B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

*Czy zbiór*

$$G = \{A^m \cdot B^n : \ \ m, n \in \mathbb{Z}\}$$

*ze zwykłym mnożeniem macierzy stanowi grupę?*

*Robert Rałowski*