

Kolokwium 1

1. Ile biletów po 3 zł i po 5 zł można kupić za 149 zł, jeżeli należy wydać wszystkie pieniądze?
2. Wykorzystując kongruencję $100 \equiv -2 \pmod{51}$ wyprowadź cechę podzielności przez 51.
3. Zacytować dwa znane twierdzenia pozwalające wyznaczać $\text{ord}_p(n!)$, $n, p \in \mathbb{N}$, p - pierwsza. Korzystając z tych twierdzeń:
 - (a) rozstrzygnąć, iloma zerami kończy się rozwinięcie dziesiętne liczby $100!$,
 - (b) udowodnić, że $\text{ord}_p(n!) \leq \frac{n}{p-1}$.
4. Znajdź elementy odwracalne w pierścieniu $\mathbb{Z}[X]$ wielomianów o współczynnikach całkowitych.
5. Niech $S(3)$ oznacza grupę wszystkich bijekcji zbioru $\{1, 2, 3\}$ na siebie (ze składaniem), a $D(3)$ grupę wszystkich izometrii własnych trójkąta (ze składaniem). Udowodnić, że grupy te są izomorficzne.

Rozwiązania

1. Niech X oznacza liczbę biletów za 3 zł, a Y za 5 zł. Szukamy całkowitych rozwiązań równania:

$$3X + 5Y = 149.$$

Równanie to ma rozwiązanie, gdyż $\text{NWD}(3, 5) = 1 \mid 149$. Z algorytmu Euklidesa:

$$\begin{aligned} 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1, \end{aligned}$$

skąd:

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 = \\ &= 3 - (5 - 3 \cdot 1) \cdot 1 = 3 \cdot 2 + 5 \cdot (-1), \end{aligned}$$

a zatem:

$$149 = 3 \cdot (2 \cdot 149) + 5 \cdot (-1 \cdot 149) = 3 \cdot 398 + 5 \cdot (-149).$$

Wobec tego ogólnym rozwiązaniem jest $X = 298 - 5 \cdot t$, $Y = -149 + 3 \cdot t$. Oczywiście interesują nas tylko te rozwiązania, dla których $X \geq 0$ i $Y \geq 0$, czyli $298 - 5 \cdot t \geq 0$ i $-149 + 3 \cdot t \geq 0$. Rozwiązując stosowny układ nierówności otrzymujemy:

$$\begin{cases} 298 - 5 \cdot t \geq 0 \\ -149 + 3 \cdot t \geq 0 \end{cases} \Leftrightarrow \begin{cases} 298 \geq 5 \cdot t \\ 3 \cdot t \geq 149 \end{cases} \Leftrightarrow \begin{cases} 59\frac{3}{5} = \frac{298}{5} \geq t \\ t \geq \frac{149}{3} = 49\frac{2}{3} \end{cases}$$

Jedyne rozwiązania całkowite takiego układu to $t = 50, 51, 52, 53, 54, 55, 56, 57, 58, 59$. Wobec tego możliwe pary (X, Y) to $(48, 1)$, $(43, 4)$, $(38, 7)$, $(33, 10)$, $(28, 13)$, $(23, 16)$, $(18, 19)$, $(13, 22)$, $(8, 25)$, $(3, 28)$.

2. Niech $n = a_0 + a_1 10 + \dots + a_s 10^s$. Dzielimy liczbę n na dwucyfrowe „kawalki”, $x_k = a_{2k} + 10a_{2k+1}$, $k \in \{1, \dots, t\}$, gdzie $t = \lfloor \frac{s}{2} \rfloor$. Oczywiście $n = \sum_{k=0}^t x_k 100^k = x_0 + x_1 100 + \dots + x_t 100^t$. Zauważmy, że:

$$\begin{array}{llll} x_0 \equiv x_0 \pmod{51} & x_1 \equiv x_1 \pmod{51} & x_2 \equiv x_2 \pmod{51} & \dots \\ 100 \equiv -2 \pmod{51} & 100 \equiv -2 \pmod{51} & 100^2 \equiv 4 \pmod{51} & \dots \\ \vdots & \vdots & \vdots & \vdots \\ x_0 \equiv x_0 \pmod{51} & x_1 100 \equiv -2x_1 \pmod{51} & x_2 100^2 \equiv 4x_2 \pmod{51} & \dots \end{array}$$

Zatem $n = x_0 + x_1 100 + \dots + x_t 100^t \equiv x_0 - 2x_1 + 4x_2 + \dots + (-2)^t \pmod{51}$, czyli liczba n daje taką samą resztę z dzielenia przez 51 jak suma dwucyfrowych liczb, na które można ją podzielić, mnożonych przez kolejne potęgi -2.

3. Twierdzenia, o które chodzi w treści zadania to:

Tw. A Niech $p \in \mathbb{P}$, $n \in \mathbb{N}$. Wówczas:

$$\text{ord}_p(n!) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right].$$

Tw. B Niech $p \in \mathbb{P}$, $n = a_0 + a_1 p + a_2 p^2 + \dots + a_l p^l \in \mathbb{N}$. Wówczas:

$$\text{ord}_p(n!) = \frac{n - (a_0 + a_1 + \dots + a_l)}{p - 1}.$$

Rozwiązujemy kolejne podpunkty zadania:

- (a) Oczywiście ilość zer na końcu $100!$ to wykładnik potęgi, z jaką 10 dzieli $100!$. Ponieważ $10 = 2 \cdot 5$, więc jest to mniejsza z liczb $\text{ord}_2(100!)$ i $\text{ord}_5(100!)$. W iloczynie $1 \cdot 2 \cdot 3 \cdot \dots \cdot 100$ występuje więcej liczb podzielnych przez 2 niż przez 5, więc w rozkładzie $100!$ na czynniki pierwsze występuje więcej dwójek niż piątek, a zatem $\text{ord}_2(100!) \geq \text{ord}_5(100!)$. Na podstawie twierdzenia **A** obliczamy $\text{ord}_5(100!)$:

$$\text{ord}_5(100!) = \left[\frac{100}{5} \right] + \left[\frac{100}{25} \right] + \left[\frac{100}{125} \right] + \dots = 20 + 4 = 24.$$

- (b) Niech $p \in \mathbb{P}$, $n = a_0 + a_1p + a_2p^2 + \dots + a_l p^l \in \mathbb{N}$. Ponieważ $a_0 + a_1 + \dots + a_l \geq 0$ (równość zachodzi tylko wtedy, gdy $n = 0$), więc na podstawie twierdzenia **B**:

$$\frac{n}{p-1} \geq \frac{n - (a_0 + a_1 + \dots + a_l)}{p-1} = \text{ord}_p(n!).$$

4. Pokażemy, że $\{1, -1\} = U(\mathbb{Z}[X])$, gdzie 1 i -1 rozumiemy jako wielomiany stałe równe 1 i -1 . Oczywiście jedynką pierścienia $\mathbb{Z}[X]$ jest wielomian stały równy 1. Inkluzja $(\subset)$ jest oczywista (bo $1 \cdot 1 = 1$ i $(-1) \cdot (-1) = 1$). Aby pokazać inkluzję przeciwną $(\supset)$ ustalmy wielomian $f(X) \in \mathbb{Z}[X]$ i założmy, że $f(X) \notin \{1, -1\}$. Wystarczy pokazać, że $f(X) \notin U(\mathbb{Z}[X])$.

Założmy najpierw, że $f(X) \neq \text{const}$, powiedzmy $f(X) = a_0 + a_1X + \dots + a_nX^n$, $a_n \neq 0$, $n \geq 1$. Ustalmy dowolny wielomian $g(X) \in \mathbb{Z}[X]$, powiedzmy $g(X) = b_0 + b_1X + \dots + b_mX^m$, $b_m \neq 0$, $m \geq 1$. Bez trudu sprawdzamy, że jeśli:

$$f(X) \cdot g(X) = c_0 + c_1X + \dots + c_{n+m}X^{n+m}$$

to:

$$c_k = \sum_{i+j=k} a_i b_j.$$

Zatem $c_{n+m} = a_n \cdot b_m \neq 0$, więc $f(X) \cdot g(X) \neq 1$.

Założmy teraz, że $f(X) = \text{const}$, powiedzmy $f(X) = a$ i $a \notin \{-1, 1\}$. Ustalmy dowolny wielomian $g(X) \in \mathbb{Z}[X]$, powiedzmy $g(X) = b_0 + b_1X + \dots + b_mX^m$, $b_m \neq 0$, $m \geq 1$. Mamy:

$$f(X) \cdot g(X) = ab_0 + ab_1X + \dots + ab_mX^m$$

i skoro $a_0 \notin \{-1, 1\}$, to $ab_0 \neq 1$ i tym samym $f(X) \cdot g(X) \neq 1$.

5. Rozważmy grupę $S(3)$. Dla uproszczenia zapisu odwzorowanie $\phi : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$ takie, że - przykładowo - $\phi(1) = 1$, $\phi(2) = 3$ i $\phi(3) = 2$ będziemy zapisywać $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. Oznaczmy więc $id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\phi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $\phi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\phi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\phi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\phi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Oczywiście:

$$S(3) = \{id, \phi_1, \phi_2, \phi_3, \phi_4, \phi_5\}$$

i budujemy tabelkę działań w $S(3)$:

$\circ$	id	ϕ_1	ϕ_2	ϕ_3	ϕ_4	ϕ_5
id	id	ϕ_1	ϕ_2	ϕ_3	ϕ_4	ϕ_5
ϕ_1	ϕ_1	ϕ_2	id	ϕ_5	ϕ_3	ϕ_4
ϕ_2	ϕ_2	id	ϕ_1	ϕ_4	ϕ_5	ϕ_3
ϕ_3	ϕ_3	ϕ_4	ϕ_5	id	ϕ_1	ϕ_2
ϕ_4	ϕ_4	ϕ_5	ϕ_3	ϕ_2	id	ϕ_1
ϕ_5	ϕ_5	ϕ_3	ϕ_4	ϕ_1	ϕ_2	id

Rozważmy grupę $D(3)$. Dla uproszczenia zapisu izometrię i taką, że - przykładowo - $i(A) = A$, $i(B) = C$ i $i(C) = B$, gdzie A , B i C są wierzchołkami trójkąta, będziemy zapisywać $\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$. Oznaczmy więc $id = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$, $O_{120} = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$, $O_{240} = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$, $S_A = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$, $S_B = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$, $S_C = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$. Oczywiście:

$$D(3) = \{id, O_{120}, O_{240}, S_A, S_B, S_C\}$$

i budujemy tabelkę działań w $D(3)$:

$\circ$	id	O_{120}	O_{240}	S_A	S_B	S_C
id	id	O_{120}	O_{240}	S_A	S_B	S_C
O_{120}	O_{120}	O_{240}	id	S_C	S_A	S_B
O_{240}	O_{240}	id	O_{120}	S_B	S_C	S_A
S_A	S_A	S_B	S_C	id	O_{120}	O_{240}
S_B	S_B	S_C	S_A	O_{240}	id	O_{120}
S_C	S_C	S_A	S_B	O_{120}	O_{240}	id

Widzimy, że obydwie tabelki są takie same, tak więc odwzorowanie $\Phi : S(3) \rightarrow D(3)$ dane wzorem:

$$\Phi(id) = id, \Phi(\phi_1) = O_{120}, \Phi(\phi_2) = O_{240}, \Phi(\phi_3) = S_A, \Phi(\phi_4) = S_B, \Phi(\phi_5) = S_C$$

będzie szukanym izomorfizmem.