# Lista 13

**Zadanie 1.** Rozważmy grupę $G$ i zdefiniujmy w niej *sprzężenie* (względem elementy $g$) $\varphi_g : G \to G$:

$$\varphi_g(x) = gxg^{-1} \quad .$$

Pokaż, że

- $\varphi_{ab} = \varphi_a\varphi_b$;
- $\varphi_a$ jest izomorfizmem z $G$ w $G$;
- jeśli $H \leq G$ to $\varphi_a(H) \leq G$ (podgrupa sprzężona).

**Zadanie 2 (Nie liczy się do podstawy).** *Typem* permutacji $\sigma \in S_n$ nazywamy ciąg $(n_1, \dots, n_n)$, gdzie $n_i$ to liczba cykli długości $i$ w rozkładzie $\sigma$ na cykle rozłączne.

Pokaż, że dla dwóch permutacji $\sigma, \tau$ permutacja $\tau^{-1}\sigma\tau$ ma taki sam typ, jak permutacja $\sigma$.

Wywnioskuj z tego, że jeśli dla $H \leq G \leq S_n$ mamy, że dla każdego możliwego rozkładu na cykle $H$ zawiera albo wszystkie, albo żadne elementy danego typu z $G$, to $H \trianglelefteq G$.

Korzystając z tego faktu pokaż, że podgrupa $\{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \leq S_4$ jest podgrupą normalną (w $S_4$).

*Wskazówka:* Jak wygląda rozkład na cykle elementów w grupie sprzężonej?

**Zadanie 3.** Znajdź wszystkie podgrupy normalne w grupie obrotów i odbić kwadratu. Dla którejś z nietrywialnych podaj tabelę działań w grupie ilorazowej (tj. grupie warstw podgrupy normalne).

*Wskazówka:* Co wiesz o grupach rzędu 4?

**Zadanie 4.** Wykonaj poniższe obliczenia modulo $3, 5$ oraz 15. Oznaczenie $62^{-1}$ oznacza element odwrotny do $62 \mod m$ w odpowiednim $\mathbb{Z}_m$.

- $-(125 \cdot 18 + 32 \cdot 49)^{-1} \cdot (75 \cdot 27 - 16 \cdot 7) + (77 \cdot 22^{-1} - 18 \cdot 255)$;
- $15^7 - 343^{12} \cdot 241^4 + 175 \cdot 123 - (176^{-1})^4 \cdot 121^2$.

**Zadanie 5.** Rozpatrz działanie algorytmu Euklidesa na dwóch kolejnych liczbach Fibonacciego. Jak wygląda para liczb trzymanych po $k$-tym kroku? Udowodnij, że dla pary liczb $(F_{n+1}, F_{n+2})$ algorytm wykonuje przynajmniej $n$ kroków.

Pokaż, że algorytm Euklidesa (w którym zastępujemy $a$ przez $a \bmod b$, a nie $a$ przez $a - b$) wykonuje $\mathcal{O}(\log(a) + \log(b))$ kroków.

*Wskazówka:* Pokaż, że w jednym kroku któraś z liczb zmniejsza się o połowę.

**Zadanie 6.** Uogólnij algorytm Euklidesa dla większej liczby liczb $m_1, m_2, \dots, m_k$. Pokaż, że $\mathrm{nwd}(m_1, \dots, m_k) = \sum_{i=1}^{k} x_i m_i$ dla pewnych liczb całkowitych $x_i$.

*Wskazówka:* Rozważ, co zwraca algorytm Euklidesa dla dwóch liczb $m_1$ oraz $m_2m_3\cdots m_k$. Rekurencyjnie postępuj dla $m_2m_3\cdots m_k$.

**Zadanie 7.** Pokaż, że dla niezerowych liczb całkowitych $a, b$ istnieją dokładnie dwie pary liczb całkowitych $(x, y)$, takich że:

- $xa + yb = \mathrm{nwd}(a, b)$ oraz
- $|x| < \frac{b}{\mathrm{nwd}(a,b)}$, $|y| < \frac{a}{\mathrm{nwd}(a,b)}$.

Pokaż ponadto, że w jednej z tych par $x$ jest dodatnie, a $y$ niedodatnie, zaś w drugiej odwrotnie.

*Wskazówka:* Wydziel najpierw przez $\mathrm{nwd}(a, b)$.

**Zadanie 8.** Oblicz nwd dla następujących par liczb. Przedstaw je jako kombinację liniową (o współczynnikach całkowitych) tych liczb.

$$\{743, 342\}, \{3812, 71\}, \{1234, 321\}.$$

**Zadanie 9.** Pokaż, że jeśli $n, m$ są względnie pierwsze, to $\varphi(nm) = \varphi(n) \cdot \varphi(m)$.

Ile wynosi $\varphi(p^k)$, gdzie $p$ jest liczbą pierwszą a $k \geq 1$? Określ, ile wynosi $\varphi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k})$ dla $p_1, p_2, \dots, p_k$—różnych liczb pierwszych.

*Wskazówka:* Pierwsza część: najprościej z Chińskiego Tw. o resztach; da się też "na palcach", ale nie jest to takie łatwe.

**Zadanie 10.** Oblicz $\varphi$ dla następujących liczb: $7, 9, 27, 77, 143, 105$. Możesz skorzystać z Zadania 9.

**Zadanie 11.** Podaj dowolne rozwiązanie w liczbach naturalnych poniższych układów równań.

$$\begin{cases} x \bmod 7 = 1 \\ x \bmod 5 = 4 \end{cases} \quad \begin{cases} x \bmod 9 = 8 \\ x \bmod 11 = 3 \end{cases} \quad \begin{cases} x \bmod 13 = 3 \\ x \bmod 17 = 11 \end{cases} \quad .$$