# Lista 12

**Zadanie 1** (* Nie liczy się do podstawy). *Typem* $t$ permutacji $\sigma \in S_n$ nazywamy ciąg $t = (n_1, \ldots, n_n)$, gdzie $n_i$ to liczba cykli długości $i$ w rozkładzie $\sigma$ na cykle rozłączne. Dla danego typu $t$ oraz $H \leq S_n$ niech $|H|_t$ będzie liczbą permutacji typu $t$ w $H$.

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

Niech $H \leq G \leq S_n$. Załóżmy, że dla każdego typu permutacji $t$ zachodzi $|H|_t \in \{0, |G|_t\}$, tj. podgrupa $H$ albo nie ma permutacji typu $t$ albo ma wszystkie permutacje typu $t$ z $G$. Pokaż, że $H \trianglelefteq G$.

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 2.** 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).

**Zadanie 3.** Załóżmy, że $H$ jest podgrupą $G$, a $N$ podgrupą normalną $G$. Pokaż, że wtedy

$$HN = \{hn \,:\, h \in H,\, n \in N\}$$

jest podgrupą $G$.

Załóżmy, że grupy $N_1, N_2$ są normalne w $G$. Pokaż, że $N_1N_2$ jest podgrupą normalną.

**Zadanie 4.** Wykonaj poniższe obliczenia modulo $3, 5, 15$. 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 którąś z liczb zmniejsza się o połowę.

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

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

**Zadanie 7.** Pokaż, że dla dodatnich całkowitych liczb $a, b$ 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:* Wydzielaj 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 $p_1, p_2, \ldots, p_k$—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.** Pokaż, że dla $p$-pierwszego oraz $a$-względnie pierwszego z $p$ liczba $a^{p-2}$ jest odwrotnością $a$ w $\mathbb{Z}_p$. Skonstruuj wydajny (tj. wielomianowy od $\log p$ oraz $\log a$) algorytm obliczania tej liczby.

*Wskazówka:* Małe twierdzenie Fermat'a.