Algebra - Lista 14

Zadanie 1 Wykonaj następujące obliczenia modulo 4 oraz modulo 7:

- $-(24 \cdot 5 + 3 \cdot (-2)) \cdot (82 - 13)$
- $1 + 2 + 3 + \ldots + 100$
- $1 \cdot 5 + 17 \cdot (-32) + 10 \cdot 4$

Zadanie 2 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.

Zadanie 3 Uogólnij algorytm Euklidesa dla większej ilości liczb $m_1, m_2, \ldots, m_k$. Pokaż, że można też z jego działania odtworzyć k ciągów współczynników, $x_1^{(1)}, x_2^{(1)}, \ldots, x_k^{(1)}$, $x_1^{(2)}, x_2^{(2)}, \ldots, x_k^{(2)}$, $\ldots$, $x_1^{(k)}, x_2^{(k)}, \ldots, x_k^{(k)}$, takich że:

$$\sum_j x_j^{(i)} m_j \mod m_i = 1 \quad \sum_j x_j^{(i)} m_j \mod m_{i'} = 0 \text{ dla } i \neq i'.$$

Wskazówka: Rozważ, co zwraca algorytm Euklidesa dla dwóch liczb m_1 oraz $m_2 m_3 \cdots m_k$. Rekurencyjnie postępuj dla $m_2 m_3 \cdots m_k$.

Zadanie 4 Pokaż, że dla liczb $a, b > 0$ są dokładnie dwie pary liczb (x, y), takich że:

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

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

Zadanie 5 Oblicz gcd dla następujących liczb. Przedstaw je jako kombinację liniową (o współczynnikach całkowitych) tych liczb.

$$\{743, 342\}, \{3812, 71\}, \{1234, 321\}, \{234, 11, 13\}.$$

Zadanie 6 Pokaż, że jeśli n, m są względnie pierwsze, to $\varphi(nm) = \varphi(n) \cdot \varphi(m)$.

Wskazówka: Możesz z Chińskiego tw. o resztach, ale da się też „na palcach”.

Zadanie 7 Oblicz, ile wynosi $\varphi(p^k)$, gdzie p jest liczbą pierwszą a $k \geq 1$. Używając poprzedniego zadania, 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.

Zadanie 8 Oblicz φ dla następujących liczb: $7, 9, 27, 77, 143, 105$.

Zadanie 9 Podaj dowolne rozwiązanie w liczbach naturalnych poniższych układów równań.

$$\begin{cases} x \mod 7 &= 2 \\ x \mod 5 &= 1 \end{cases} \quad \begin{cases} x \mod 7 &= 1 \\ x \mod 5 &= 4 \end{cases} \quad \begin{cases} x \mod 9 &= 5 \\ x \mod 11 &= 6 \end{cases} \quad \begin{cases} x \mod 9 &= 8 \\ x \mod 11 &= 3 \end{cases}$$

Zadanie 10 Przypomnijmy, że Chińskie twierdzenie o resztach mówi, że gdy $m_1, m_2, \ldots, m_k$ są parami względnie pierwsze, to naturalny homomorfizm z $\mathbb{Z}_{m_1 \cdot m_2 \cdots m_k}$ w $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$ jest izomorfizmem. Pokaż, że obrazem $\mathbb{Z}^*_{m_1 \cdot m_2 \cdots m_k}$ (czyli elementów odwracalnych w $\mathbb{Z}_{m_1 \cdot m_2 \cdots m_k}$) tego izomorfizmu jest $\mathbb{Z}^*_{m_1} \times \mathbb{Z}^*_{m_2} \times \cdots \times \mathbb{Z}^*_{m_k}$.