Lista 15

Zadanie 1. 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 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.

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 3. 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 $m_2 m_3 \cdots m_k$. Rekurencyjnie postępuj dla $m_2 m_3 \cdots m_k$.

Zadanie 4. 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: Wydziel najpierw przez $\mathrm{nwd}(a, b)$.

Zadanie 5. Pokaż, że dla liczb $m_1, \ldots, m_k$ istnieją $x_1, \ldots, x_k$ całkowite, takie że

$$\mathrm{nwd}(m_1, \ldots, m_k) = \sum_{i=1}^{k} x_i m_i$$

$$\sum_{i=1}^{k} |x_i| = \mathcal{O}\left(\left(\sum_{i=1}^{k} m_i\right)^2\right) .$$

Możesz w swoim rozwiązaniu skorzystać z Zadania 3, nawet jeśli nie umiesz go zrobić.

Wskazówka: Można na palcach, podobnie jak w Zadaniu 4. Można też przez dokładniejszą analizę algorytmu z Zadania 3.

Zadanie 6. Oblicz nwd dla następujących par liczb. Przedstaw je jako kombinację liniową (o współczynnikach całkowitych) tych liczb.

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

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

Zadanie 9 (* Nie liczy się do podstawy). 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 $\mathbb{Z}^*_{m_1} \times \mathbb{Z}^*_{m_2} \times \cdots \times \mathbb{Z}^*_{m_k}$.

Zadanie 10. Podaj dowolne rozwiązanie w liczbach naturalnych poniższych układów równań.

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

Zadanie 11. Wyznacz najmniejszą liczbę naturalną, która przy dzieleniu przez 2, 3, 5, 7, 11 daje odpowiednio reszty 1, 2, 4, 6 i 10.