

## Algebra — Lista 13

**Zadanie 1** Wykonaj następujące obliczenia modulo 4 oraz modulo 7:

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

**Zadanie 2** Wykonaj poniższe obliczenia modulo 3 oraz 5. Oznaczenie  $62^{-1}$  oznacza element odwrotny do 62 mod 3 w  $\mathbb{Z}_3$  (analogicznie w  $\mathbb{Z}_5$ ).

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

**Zadanie 3** Rozpatrz działanie algorytmu Euklidesa na dwóch kolejnych liczbach Fibonacciego. Jak wygląda para liczb trzymanyh po  $k$ -tym kroku? Udowodnij, że dla pary liczb  $(F_{n+1}, F_{n+2})$  algorytm wykonuje przynajmniej  $n$  kroków.

**Zadanie 4** 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 5** Pokaż, że dla liczb całkowitych  $a, b > 0$  są dokładnie dwie pary liczb całkowitych  $(x, y)$ , takich że:

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

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

*Wskazówka:* Wydziel najpierw przez  $\gcd(a, b)$ .

**Zadanie 6** Oblicz gcd 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  $\varphi(nm) = \varphi(n) \cdot \varphi(m)$ .

**Zadanie 8** Ile wynosi  $\varphi(p^k)$ , gdzie  $p$  jest liczbą pierwszą a  $k \geq 1$ ? Używając poprzedniego zadania, określ, ile wynosi  $\varphi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k})$  dla  $p_1, p_2, \dots, p_k$  — różnych liczb pierwszych.

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

**Zadanie 10** 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.