# Algebra Abstrakcyjna i Teoria Kodowania

Egzamin - termin I

Zadania oraz ich przykładowe rozwiązania

Jacek Cichoń
Politechnika Wrocławska
WPPT

1 lipca 2017

Podane rozwiązania są przykładowe - każde zadanie można (oczywiście) rozwiązać na wiele sposobów. Taka ogólna uwaga: przed podaniem końcowej odpowiedzi powinniście sprawdzić, czy znalezione rozwiązanie jest prawidłowe (np. w brudnopisie).

**Zadanie 1.** Wyznacz moc zbioru generatorów grupy $C_{11} \times C_{101}$.

*Rozwiązanie.* Z tego, że liczby 11 i 101 są pierwsze (i różne) wynika, że są względnie pierwsze. Z Chińskiego Twierdzenia o resztach wynika, że $C_{11} \times C_{101} \cong C_{11\cdot 101} = C_{1111}$. W grupie $C_n$ element $a$ jest generatorem wtedy i tylko wtedy, gdy $nwd(a,n) = 1$. Zatem liczba generatorów grupy $C_{1111}$ wynosi

$$\phi(1111) = \phi(11 \cdot 101) = \phi(11) \cdot \phi(101) = 10 \cdot 100 = 1000 \ .$$

□

**Zadanie 2.** Oblicz $5^{4036} \mod 2017$.

*Rozwiązanie.* Liczba 2017 jest pierwsza (to wiemy np. z Listy Zadań). Zatem dla dowolnej liczby $a$ mamy $a^{2017} \equiv a \mod 2017$ (wniosek z Małego Twierdzenia Fermata). Następie mamy $4036 = 2 \cdot 2017 + 2$. Zatem

$$5^{4036} = 5^{2\cdot 2017+2} = (5^{2017})^2 \cdot 5^2 \equiv_5 5^2 \cdot 5^2 = 625 \ .$$

□

**Zadanie 3.** Znajdź najmniejszą liczbę naturalną $x$ taką, że

$$\begin{cases} 2x + 1 \equiv 2 \mod 3 \\ x + 2 \equiv 1 \mod 5 \\ 3x + 2 \equiv 1 \mod 7 \end{cases}$$

*Rozwiązanie.* Rozważany układ równań jest równoważny układowi

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 4 \mod 5 \\ x \equiv 2 \mod 7 \end{cases}$$

Zajmujemy się dwoma pierwszymi dwoma równaniami. Mamy $2\cdot 3+(-1)\cdot 5 = 1$. Bierzemy liczbę $z = 2 \cdot 3 \cdot \mathbf{4} + (-1) \cdot 5 \cdot \mathbf{2} = 14$. Rozważamy teraz układ

$$\begin{cases} x \equiv 14 \mod 15 \\ x \equiv 2 \mod 7 \end{cases}$$

Mamy $1 \cdot 15 + (-2) \cdot 7 = 1$. Rozważamy więc liczbę $x_0 = 1 \cdot 15 \cdot \mathbf{2} + (-2) \cdot 7 \cdot \mathbf{14} = -166$. Liczba $x_0$ jest jednym z całkowitych rozwiązań rozważanego układu. Najmniejsze dodatnie $x$ spełniające rozważany układ spełniać musi warunek $3\cdot 5\cdot 7|(x-x_0)$ oraz $0 \leq x < 3\cdot 5\cdot 7$. Taką liczbą jest $x = -166+2\cdot(3\cdot 5\cdot 7) = \mathbf{44}$. To jest szukane $x$. □

**Zadanie 4.** Niech $K$ będzie rozszerzeniem ciała $\mathbb{Z}_3$ o taki element $j$, że $j^2 + 1 = 0$. Rozwiąż w ciele $K$ układ równań

$$\begin{cases} jx + y = 1 \\ 2x + y = j \end{cases}$$

*Rozwiązanie.* Zauważamy, że $j^2 = 2$. Zaczynamy rozwiązywać ten układ równań metodą wyznacznikową. Mamy

$$\Delta = \det \begin{bmatrix} j & 1 \\ 2 & 1 \end{bmatrix} = j - 2 = 1 + j \neq 0$$

Następnie

$$\Delta_y = \det \begin{bmatrix} j & 1 \\ 2 & j \end{bmatrix} = j^2 - 2 = 2 - 2 = 0$$

Zatem $y = \Delta_y/\Delta = 0$. Z pierwszego równania otrzymujemy $jx = 1$. Zatem $j^2x = j$, czyli $2x = j$, więc $x = 2j$. Rozwiązaniem jest więc para $(x, y) = (2j, 0)$. □

**Zadanie 5.** Niech $d(n)$ będzie liczbą różnych dzielników liczby $n$ (np. d(6) = |{1,2,3,6}| = 4). Pokaż, że jeśli $n = \prod_{p|n} p^{\alpha_n(p)}$ to $d(n) = \prod_{p|n}(1 + \alpha_n(p))$.

*Rozwiązanie.* Niech $n = \prod_{p|n} p^{\alpha_n(p)}$. Jeśli $d|n$ to istnieją liczby $(\beta(p))_{p|n}$ takie, że $0 \leq \beta(p) \leq \alpha_n(p)$ oraz $d = \prod_{p|n} p^{\beta(p)}$. Co więcej, zależność między dzielnikami liczby $n$ a elementami $\prod_{p|n}\{0, \ldots, \alpha_n(p)\}$ jest wzajemnie jednoznaczna. Zatem

$$d(n) = |\prod_{p|n}\{0, \ldots, \alpha_n(p)\}| = \prod_{p|n}(1 + \alpha_n(p)) \ .$$

□