

Kolokwium 1

Poniżej przedstawiono zadania z jednej wersji kolokwium. Zadania z innych zestawów można rozwiązać analogicznie. Jedynym wyjątkiem jest Zadanie 3, które jest zadaniem bardziej teoretycznym. W związku z tym jego rozwiązanie jest również zaprezentowane.

Zadanie 1 (3 punkty). *Korzystając z zasady indukcji matematycznej wykaż, że dla dowolnej liczby naturalnej n liczba $3^{2n-1} + 7^{2n-1}$ jest podzielna przez 10.*

Rozwiązanie:

1. Sprawdzenie dla $n = 1$: $3 + 7 = 10$. OK
2. Założenie indukcyjne dla $n = k$: $10 | 3^{2k-1} + 7^{2k-1}$
3. Teza indukcyjna: $10 | 3^{2(k+1)-1} + 7^{2(k+1)-1}$
4. Krok indukcyjny:

$$\begin{aligned} 3^{2(k+1)-1} + 7^{2(k+1)-1} &= 3^{2k+1} + 7^{2k+1} = 3^2 \cdot 3^{2k-1} + 7^2 \cdot 7^{2k-1} \\ &= 9 \cdot 3^{2k-1} + 49 \cdot 7^{2k-1} = 10 \cdot 3^{2k-1} - 3^{2k-1} + 50 \cdot 7^{2k-1} - 7^{2k-1} \\ &\equiv -(3^{2k-1} + 7^{2k-1}) \stackrel{\text{zał.ind.}}{\equiv} 0 \pmod{10} \end{aligned}$$

Zatem, na mocy indukcji matematycznej $10 | 3^{2n-1} + 7^{2n-1}$ dla dowolnego $n \in \mathbb{N}$.

□

Zadanie 2 (3 punkty). *Znajdź dwie ostatnie cyfry liczby 22^{222} .*

Rozwiązanie:

Wystarczy znaleźć najmniejszą liczbę naturalną x taką, że $22^{222} \equiv x \pmod{100}$. Ponieważ $\text{NWD}(22, 100) > 1$, więc nie możemy od razu skorzystać z twierdzenia Eulera. Z Chińskiego Twierdzenia o Resztach wiemy, że

$$22^{222} \equiv x \pmod{100} \iff \begin{cases} x \equiv 22^{222} \pmod{25} \\ x \equiv 22^{222} \pmod{4} \end{cases}$$

Łatwo zauważyć, że $22^{222} \equiv 0 \pmod{4}$. Z drugiej strony, na mocy tw. Eulera, skoro $\varphi(25) = 20$:

$$22^{222} = 22^{220} \cdot 22^2 \equiv 1 \cdot 22^2 \equiv (-3)^2 = 9 \pmod{25}.$$

Stąd:

$$\begin{cases} x \equiv 9 \pmod{25} \\ x \equiv 0 \pmod{4} \end{cases}$$

Liczbę x znajdujemy korzystając z metody przedstawionej w dowodzie Chińskiego Twierdzenia o Resztach:

$$x \equiv 9 \cdot 4 \cdot x_1 + 0 \pmod{100},$$

gdzie x_1 jest dowolną liczbą spełniającą kongruencję $4x_1 \equiv 1 \pmod{25}$, a więc np. $x_1 = 4^{-1} = 19$ (4^{-1} w $\mathbb{Z}_{25}$ można obliczyć z uogólnionego algorytmu Euklidesa, zob. Zadanie 4). Mamy więc:

$$x \equiv 9 \cdot 4 \cdot x_1 + 0 \equiv 36 \cdot 19 = 720 - 36 \equiv 84 \pmod{100}.$$

□

Zadanie 3 (3 punkty, dwie wersje).

1. Niech x, y będą względnie pierwszymi liczbami naturalnymi, które spełniają równanie $xy = a^2$ dla pewnego $a \in \mathbb{N}$. Wykaż, że x i y są kwadratami pewnych liczb naturalnych.
2. Niech x, y będą względnie pierwszymi liczbami naturalnymi. Wykaż, że $\text{NWD}(x + y, xy) = 1$.

Rozwiązanie:

1. Na mocy Zasadniczego Twierdzenia Arytmetyki, x, y, a mogą być jednoznacznie rozłożone na czynniki pierwsze, powiedzmy

$$x = p_1^{k_1} \cdot \dots \cdot p_s^{k_s}, \quad y = q_1^{l_1} \cdot \dots \cdot q_r^{l_r}, \quad a = a_1^{n_1} \cdot \dots \cdot a_t^{n_t}.$$

Ponieważ x, y są względnie pierwsze, więc zbiory $\{p_1, \dots, p_s\}$ i $\{q_1, \dots, q_r\}$ są rozłączne. Teraz, porównując wykładniki w iloczynie $xy = a^2$:

$$p_1^{k_1} \cdot \dots \cdot p_s^{k_s} \cdot q_1^{l_1} \cdot \dots \cdot q_r^{l_r} = a_1^{2n_1} \cdot \dots \cdot a_t^{2n_t}$$

widzimy, że liczby $k_1, \dots, k_s, l_1, \dots, l_r$ są parzyste. Zatem x i y są kwadratami pewnych liczb naturalnych.

2. Przypuśćmy, że $\text{NWD}(x + y, xy) = d > 1$. Wtedy istnieje liczba pierwsza p taka, że $p | \text{NWD}(x + y, xy)$. Z definicji NWD wynika, że $p | x + y$ i $p | xy$. Ale skoro x, y są względnie pierwsze, więc albo $p | x$ albo $p | y$. W pierwszym przypadku mamy: $p | x$ i $p | x + y$; co oznacza, że $p | y$, sprzeczność. W drugim przypadku również otrzymamy sprzeczność.

□

Zadanie 4 (3 punkty). Rozwiąż równanie $14x = 3$ w $\mathbb{Z}_{6007}$.
Jaki jest element odwrotny do 14 w $\mathbb{Z}_{6007}$?

Rozwiązanie:

Zauważmy, że w $\mathbb{Z}_{6007}$ równanie $14x = 3$ jest równoważne równaniu diofantycznemu

$$6007a + 14x = 3.$$

Rozwiązujemy je za pomocą uogólnionego algorytmu Euklidesa:

$$\begin{array}{ccc} [6007 & 1 & 0] \\ [14 & 0 & 1] \\ \hline [6007 - 14 \cdot 429 & 1 - 0 \cdot 429 & 0 - 1 \cdot 429] \\ \hline [1 & 1 & -429] \\ [0 & \star & \star] \end{array}$$

Odczytujemy:

$$6007 \cdot 1 + 14 \cdot (-429) = 1.$$

Stąd widać, że element odwrotny do 14 w $\mathbb{Z}_{6007}$ istnieje i wynosi -429 oraz

$$6007 \cdot 3 + 14 \cdot (-429 \cdot 3) = 3.$$

Zatem $x = -429 \cdot 3$.

□

Zadanie 5 (2 punkty). Oblicz w $\mathbb{Z}_{19}$: $(3^{-1} \cdot 7 - \sqrt{-3})^2$.

Rozwiązanie:

Liczbę 3^{-1} można wyznaczyć za pomocą uogólnionego algorytmu Euklidesa (zob. Zadanie 4) lub zauważyć że $3 \cdot 13 = 39 = 1$. Ponadto, $\sqrt{-3} = \sqrt{16} = \pm 4$. Stąd:

$$(3^{-1} \cdot 7 - \sqrt{-3})^2 = (13 \cdot 7 - \sqrt{16})^2 = (91 \pm 4)^2 = (-4 \pm 4)^2 = 0 \text{ lub } 64 = 0 \text{ lub } 7.$$

□

Zadanie 6 (2 punkty). Zapisz permutację

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 9 & 2 & 5 & 1 & 10 & 3 & 8 & 7 & 6 \end{pmatrix}$$

w postaci iloczynu cykli rozłącznych.

Czy jest to permutacja parzysta czy nieparzysta?

Rozwiązanie:

$$\begin{aligned} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 9 & 2 & 5 & 1 & 10 & 3 & 8 & 7 & 6 \end{pmatrix} &= (145)(2973)(610) \\ &= (15)(14)(23)(27)(29)(610) \end{aligned}$$

Jest to permutacja parzysta.

□

Zadanie 7 (4 punkty). Sprawdź, że zbiór $\mathbb{Q} \times \mathbb{Q}$ z działaniami

$$(a, b) + (c, d) = (a + c, b + d), \quad (a, b) \star (c, d) = (ac + 5bd, ad + bc)$$

jest ciałem (wskazówka: oblicz $(1, 0) \star (1, 0)$).

Wykaż, że to ciało jest izomorficzne z $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} : a, b \in \mathbb{Q}\}$ (działania w $\mathbb{Q}(\sqrt{5})$ to zwykłe dodawanie i mnożenie).

Rozwiązanie:

Przede wszystkim, dla dowolnych $a, b, c, d \in \mathbb{Q}$ mamy $(a, b) + (c, d) \in \mathbb{Q} \times \mathbb{Q}$ oraz $(a, b) \star (c, d) \in \mathbb{Q} \times \mathbb{Q}$, a więc rzeczywiście $+$ i $\star$ są działaniami w $\mathbb{Q} \times \mathbb{Q}$. Ustalmy teraz dowolne $a, b, c, d, e, f \in \mathbb{Q}$.

1. Łatwo pokazać, że $(\mathbb{Q} \times \mathbb{Q}, +)$ jest grupą abelową (na kolokwium wypada to trochę rozpisać, postępując podobnie jak poniżej to zrobimy dla $\star$).
2. $\star$ jest działaniem przemiennym:

$$(a, b) \star (c, d) = (ac + 5bd, ad + bc) = (ca + 5db, da + cb) = (c, d) \star (a, b)$$

3. $\star$ jest działaniem łącznym:

$$(a, b) \star ((c, d) \star (e, f)) = (a, b) \star (ce + 5df, cf + de) = \dots = ((a, b) \star (c, d)) \star (e, f)$$

4. Zachodzi rozdzielnosc $\star$ względem $+$:

$$\begin{aligned} ((a, b) + (c, d)) \star (e, f) &= (a + c, b + d) \star (e, f) \\ &= ((a + c)e + 5(b + d)f, (a + c)f + (b + d)e) \\ &= \dots \\ &= ((a, b) \star (e, f)) + ((c, d) \star (e, f)) \end{aligned}$$

5. Zauważmy, że $(a, b) \star (1, 0) = (a, b)$, co oznacza (skoro $\star$ jest przemienne), że $(1, 0)$ jest elementem neutralnym $\star$.
6. Załóżmy teraz, że $(a, b) \neq (0, 0)$. (c, d) jest elementem odwrotnym do (a, b) względem $\star$ wtedy i tylko wtedy gdy (skoro $\star$ jest przemienne) $(a, b) \star (c, d) = (1, 0)$. Dostajemy układ równań:

$$\begin{cases} ac + 5bd = 1 \\ ad + bc = 0 \end{cases}$$

Z drugiego równania wyznaczamy c , podstawiamy do pierwszego i w rezultacie dostajemy

$$c = \frac{a}{a^2 - 5b^2}, \quad d = -\frac{b}{a^2 - 5b^2},$$

co oznacza, że każdy element $\mathbb{Q} \times \mathbb{Q}$ różny od $(0, 0)$ ma element odwrotny.

Stąd $(\mathbb{Q} \times \mathbb{Q}, +, \star)$ jest ciałem.

Rozważmy teraz odwzorowanie

$$\varphi: \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}(\sqrt{5}), \quad \varphi(a, b) = a + b\sqrt{5}.$$

Łatwo sprawdzić, że spełnia ono wszystkie wymogi aby być izomorfizmem ciał.

Oczywiście, wszystkie luki w powyższym rozwiązaniu powinny być rozpisane na kolokwium.

□