Algebra dla informatyków

Jacek Michałowski, Piotr Latanowicz

15 kwietnia 2014

Zadanie 1

Zadanie 1

Niech $n \in \mathbb{N}$, $n > 1$, będzie dowolną liczbą naturalną. Wówczas:

a) $\text{nwd}(n, n+3) = n$

b) $\text{nwd}(n, n+3) = 3$

c) $\text{nwd}(n, n+3) = 1$

Zadanie 1

Definicja

Liczbę d nazywamy *największym wspólnym dzielnikiem* $a, b \in \mathbb{Z}$ jeśli:

- d jest wspólnym dzielnikiem:

$$d|a \wedge d|b$$

- d jest największe:

$$\forall_c \begin{cases} c|a \\ c|b \end{cases} \implies c|d$$

Oznaczamy nwd(a, b) lub (a, b).

Zadanie 1

Próbujemy znaleźć kontrprzykłady.
Niech $n = 2$, wtedy:

$$\text{nwd}(2, 5) = 1$$

$1 \neq n$, odpowiedź a: **Nie**. $1 \neq 3$, odpowiedź b: **Nie**.

Niech $n = 3$, wtedy:

$$\text{nwd}(3, 6) = 3 \neq 1$$

Odpowiedź c: **Nie**.

Zadanie 2

Niech m będzie liczbą naturalną taką, że $m|b$ i $m|a+b$, gdzie $a, b \in \mathbb{Z}$. Wówczas:

a) $m|ab$

b) $m|a$

c) $m|ax+by$

Zadanie 2

Definicja

Niech $a, b \in \mathbb{Z}, a \neq 0$. Mówimy że a jest *dzielnikiem* b (b jest podzielne przez a), wtedy i tylko wtedy gdy istnieje $c \in \mathbb{Z}$, że $b = ac$. Oznaczamy $a|b$.

Na podstawie definicji podzielności istnieją takie $p, q \in \mathbb{Z}$, że:

$$\begin{cases} m|b \\ m|a+b \end{cases} \Leftrightarrow \begin{cases} b & = mp \\ a+b & = mq \end{cases}$$

$$\begin{aligned} a + mp &= mq \\ a &= mq - mp \\ a &= m(q-p) \end{aligned}$$

Zatem $m|a$. Odpowiedź b: **Tak**.

Zadanie 2

$$\begin{aligned} ab &= m(q-p)mp \\ &= m^2(q-p) \end{aligned}$$

Czyli $m|ab$. Odpowiedź a: **Tak**.

$$\begin{aligned} ax+by &= m(q-p)x+mpy \\ &= m\left((q-p)x+py\right) \end{aligned}$$

Więc $m|ax+by$. Odpowiedź c: **Tak**.

Zadanie 3

Równanie $45x - 69y = 24$

a) nie ma rozwiązań całkowitych

b) ma dokładnie jedno rozwiązanie całkowite

c) ma nieskończenie wiele rozwiązań całkowitych

Zadanie 3

Twierdzenie

Równanie $ax + by = c$, $a, b, c \in \mathbb{Z}$ ma rozwiązanie $x, y \in \mathbb{Z}$ wtedy i tylko wtedy gdy $\text{nwd}(a, b)|c$. Wszystkie rozwiązania w $\mathbb{Z}$ dane są wzorami:

$$x = x_0 + b_1, \qquad y = y_0 - a_1 t$$

gdzie $t \in \mathbb{Z}$, $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$, $d = \text{nwd}(a, b)$.

$$\begin{aligned} 45x - 69y &= 24 \quad / : 3 \\ 15x - 23y &= 8 \end{aligned}$$

Jest to równanie diofantyczne. Warunkiem istnienia rozwiązania jest $\text{nwd}(15, -23)|8$. Ponieważ $1|8$, równanie ma rozwiązania i jest ich nieskończenie wiele. Odpowiedzi: a: **Nie**, b: **Nie**, c: **Tak**.

Zadanie 4

Niech $\varphi : \mathbb{N} \to \mathbb{N}$ oznacza funkcję Eulera. Wówczas:

a) $\varphi(315) = \varphi(45)\varphi(7)$

b) $\varphi(315) = \varphi(15)\varphi(21)$

c) $\varphi(315) = \varphi(9)\varphi(35)$

Zadanie 4

Definicja

Funkcję arytmetyczną (czyli $\mathbb{N} \to \mathbb{N}$) f nazywamy *multiplikatywną* gdy:

$$\begin{cases} f(1) = 1 \\ f(mn) = f(m)f(n) \quad \forall_{m,n} \text{ nwd}(m,n) = 1 \end{cases}$$

Przykładem funkcji multiplikatywnej jest funkcja φ Eulera. Wyraża liczbę liczb względnie pierwszych i nie większych od danej.

Twierdzenie

Dla dowolnego $n \in \mathbb{N}$, $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $\alpha_i \geq 1$, p_i są liczbami pierwszymi, mamy:

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

Zadanie 4

$$\begin{aligned}\varphi(315) &= \varphi(3^2 5^1 7^1) \\ &= 315(1-\tfrac{1}{3})(1-\tfrac{1}{5})(1-\tfrac{1}{7}) \\ &= 315 \cdot \tfrac{2}{3}\tfrac{4}{5}\tfrac{6}{7} \\ &= 144\end{aligned}$$

a:

$$\varphi(45)\varphi(7) = \varphi(3^2 5^1)\varphi(7^1) = 45 \cdot \frac{2}{3}\frac{4}{5} \cdot 7 \cdot \frac{6}{7} = 144$$

b:

$$\varphi(15)\varphi(21) = \varphi(3^1 5^1)\varphi(3^1 7^1) = 15 \cdot \frac{2}{3}\frac{4}{5} \cdot 21 \cdot \frac{2}{3}\frac{6}{7} = 96 \neq 144$$

c:

$$\varphi(9)\varphi(35) = \varphi(3^2)\varphi(5^1 7^1) = 9 \cdot \frac{2}{3} \cdot 35 \cdot \frac{4}{5}\frac{6}{7} = 144$$

Odpowiedzi: a: **Tak**, b: **Nie**, c: **Tak**.

Zadanie 5

Dana jest kongruencja liniowa: $4x \equiv 5 \pmod{13}$. Wówczas:

a) liczba $x = 24$ jest jej rozwiązaniem.

b) każde dwa rozwiązania różnią się o wielokrotność modułu.

c) klasa reszt $[11]_{13}$ wyczerpuje zbiór wszystkich rozwiązań kongruencji.

Zadanie 5

Definicja

Niech $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$. Mówimy, że a przystaje do b modulo n jeśli n, dzieli $a - b$:

$$a \equiv b \,(\mathrm{mod}\ n) \qquad \Leftrightarrow \qquad n | a - b$$

Taką relację nazywamy *kongruencją*.

Własności kongruencji

$$\begin{cases} a \equiv b \,(\mathrm{mod}\ n) \\ c \equiv d \,(\mathrm{mod}\ n) \end{cases} \Rightarrow \begin{cases} a \pm c \equiv b \pm d \,(\mathrm{mod}\ n) \\ ac \equiv bd \,(\mathrm{mod}\ n) \end{cases}$$

$$ac \equiv bc \,(\mathrm{mod}\ n) \qquad \Leftrightarrow \qquad a \equiv b \left(\mathrm{mod}\ \frac{n}{\mathrm{nwd}(n, c)}\right)$$

Kongruencje można więc dodawać i mnożyć stronami oraz dzielić przez c o ile $\mathrm{nwd}(n, c) = 1$.

Zadanie 5

$$\begin{aligned} 4x &\equiv 5 \pmod{13} \\ (4 + 2 \cdot 13)x &\equiv 5 \pmod{13} \\ 30x &\equiv 5 \pmod{13} \\ 6x &\equiv 1 \pmod{13} \end{aligned}$$

Elementem odwrotnym do 6 w $\mathbb{Z}_{13}$ jest 11, zatem:

$$x \equiv 11 \pmod{13}$$

Odp c: **Tak**. Relacja kongruencji dzieli $\mathbb{Z}$ na rozłączne niepuste klasy abstrakcji. Elementy każdego z niej różnią się o wielokrotność modułu (Odp b: **Tak**), zatem $11 + 13 = 24 \in [11]_{13}$ (Odp a: **Tak**).

Zadanie 6

Reszta z dzielenia liczby $a = 8^{62}$ przez 13 jest równa.

a) 5

b) 8

c) 12

Zadanie 6

Twierdzenie Eulera

Jeżeli $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $\text{nwd}(a, n) = 1$, to

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Należy rozwiązać kongruencję:

$$x \equiv 8^{62} \pmod{13}$$

$$x \equiv 2^{186} \pmod{13}$$

Z twierdzenia Eulera wiemy, że:

$$1 \equiv 2^{\varphi(13)} \equiv 2^{12} \pmod{13}$$

Z powyższego oraz z $\varphi(n)$ okresowości potęgowania modulo n mamy:

$$x \equiv 2^{186} \equiv 2^{12 \cdot 15 + 6} \equiv 2^6 \equiv 4 \cdot 13 + 12 \equiv 12 \pmod{13}$$

Odpowiedzi: a: **Nie**, b: **Nie**, c: **Tak**

Zadanie 7

Niech $d = 45 \in \mathbb{Z}_{64}$. Wówczas:

a) d jest elementem odwracalnym w pierścieniu $\mathbb{Z}_{64}$

b) d jest dzielnikiem zera w pierścieniu $\mathbb{Z}_{64}$

c) $-d = 19$

Zadanie 7

Definicja

Dla danej liczby całkowitej a takiej, że $\text{nwd}(a, n) = 1$ określamy *element odwrotny* do a modulo n jako każde rozwiązanie $ax \equiv 1 \pmod{n}$.

Definicja

Niech P to pierścień przemienny z jedynką. Element $a \in P \setminus \{0\}$ nazywamy *dzielnikiem zera* gdy istnieje $b \in P \setminus \{0\}$ takie że $a \cdot b = 0$.

Element $a \in P$ nazywamy *odwracalnym* gdy istnieje $c \in P$ że $a \cdot c = 1$.

Twierdzenie

W pierścieniu skończonym z jedynką każdy element $a \neq 0$ jest albo dzielnikiem zera albo elementem odwracalnym.

Zadanie 7

Ponieważ $\text{nwd}(45, 64) = 1$ więc kongruencja $45x \equiv 1 \pmod{64}$ ma rozwiązanie, zatem 45 posiada element odwrotny. Odp. a: **Tak**.

Skoro 45 jest odwracalne to nie jest dzielnikiem zera. Odp. b: **Nie**.

$-d$ to element przeciwny do elementu d. To znaczy, że $d + (-d) \equiv 0 \pmod{64}$. Stąd $-d = 19$, a zatem odpowiedź c: **Tak**.

Zadanie 8

Dany niżej zbiór jest podgrupą grupy $\mathbb{Z}_{28}$

a) $\{0, 4, 7, 11\}$

b) $\{0, 7, 14, 21\}$

c) $\{0, 6, 12, 18, 24\}$

Zakładamy, że chodzi o grupę $(\mathbb{Z}_{28}, +)$.

Zadanie 8

Definicja

Niech $(G, \cdot)$ to grupa, $H \subset G$, $H \neq \varnothing$. H to *podgrupa* grupy G jeśli dla dowolnych elementów $a, b \in H$ zachodzi $ab^{-1} \in H$. Oznaczenie $H < G$.

Stwierdzenie

Następujące warunki są równoważne:

- $H < G$
- $H \subset G$ oraz

$$\forall_{a,b \in H} \begin{cases} ab \in H \\ ab^{-1} \in H \end{cases}$$

- $\left(H, \cdot \Big/ H\right)$

Zadanie 8

Podgrupa to zbiór elementów danej grupy, który sam tworzy grupę z działaniem grupy wyjściowej a także zawiera jej element neutralny. Liczba elementów podgrupy musi być dzielnikiem liczby wszystkich elementów grupy. Ponadto dla każdej pary elementów podgrupy H musi zachodzić $ab \in H$. Podgrupa może mieć w tym przypadku 1, 2, 4, 7, 14 lub 28 elementów.

a. W tej podgrupie są 4 elementy, ale nie zachodzi warunek, że $ab \in H$, bo na przykład $11 + 7 = 18$, a tego elementu nie ma w tej podgrupie, stąd odpowiedź: **Nie**.

c. W tej podgrupie jest 5 elementów, czyli rozpatrywanie tego przypadku nie ma w ogóle sensu. Odpowiedź: **Nie**.

Zadanie 8

b. Aby sprawdzić czy $\{0, 7, 14, 21\}$ jest podgrupą sprawdzamy warunek

$$\forall_{a,b\in\{0,7,14,21\}}\ a - b \in \{0, 7, 14, 21\}$$

$a - b$	$-0 = 0$	$-7 = 21$	$-14 = 14$	$-21 = 7$
0	0	21	14	7
7	7	0	21	14
14	14	7	0	21
21	21	14	7	0

Widać teraz, że dla każdego a, b zachodzi $a - b \in H$. Zatem jest to podgrupa. Odpowiedź b: **Tak**.

Zadanie 9

Jądrem homomorfizmu $f : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ określonego wzorem $f(a) = 3a$ jest zbiór

a) $\{0, 4\}$

b) $\{0, 4, 8\}$

c) $\{0, 2, 4, 6, 8, 10\}$

Zadanie 9

Definicja

Homomorfizmem grup $(G, \otimes)$ i $(H, \star)$ nazywamy takie $f : G \to H$, że:

$$\forall_{a,b \in G}\ f(a \otimes b) = f(a) \star f(b)$$

Definicja

Jądrem homomorfizmu $f : G \to H$ nazywamy zbiór elementów G zmapowanych na element neutralny H.

$$\ker f = \{a \in G : f(a) = e_H\}$$

Zadanie 9

Trzeba obliczyć równanie w $\mathbb{Z}_{12}$:

$$f(a) = 0$$

$$3a = 0$$

$$a \in \{0, 4, 8\}$$

Stąd tylko odpowiedź b **Tak**.

Zadanie 10

Permutacja

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 6 & 3 & 1 \end{pmatrix} \in S_6$$

Wówczas:

a) a jest permutacją parzystą

b) a jest cyklem

c) $\mathrm{rz}a = 3$

Zadanie 10

Definicja

Permutację $f \in S_n$ nazywamy *cyklem* rzędu $k \leq n$, gdy istnieje podzbiór $I = \{i_i, i_2, \ldots, i_k\}$ zbioru $J = \{1, 2, \ldots, n\}$, taki że:

$$\begin{cases} f(i_1) = i_2 \\ f(i_2) = i_3 \\ \ldots \\ f(i_k) = i_1 \\ f(j) = j \qquad \forall_{j \in J \setminus I} \end{cases}$$

Twierdzenie

Każda permutacja $f \in S_n$ jest cyklem albo złożeniem cykli rozłącznych (cykle $(i_1, \ldots, i_k)$ i $(j_1, \ldots, j_s)$ są rozłączne jeśli $\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_s\} = \varnothing$).

Zadanie 10

Twierdzenie

Jeśli w pewnym rozkładzie permutacji $f \in S_n$ na iloczyn transpozycji liczba transpozycji jest parzysta (nieparzysta) to w każdym innym rozkładzie f liczba transpozycji jest również parzysta (nieparzysta).

a. Rozkładamy a na transpozycje:

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 6 & 3 & 1 \end{pmatrix} = (1,4,6) \circ (2,5,3) = (1,6) \circ (1,4) \circ (2,3) \circ (2,5)$$

a jest parzysta. Odpowiedź a: **Tak**.
b. Permutacja rozkłada się na dwa rozłączne cykle więc nie jest cyklem.
Odpowiedź b: **Nie**.
c. Rząd elementu a to najmniejsza liczba naturalna n taka że $a^n = e$. W naszym przypadku $n = 3$ (odpowiedź c: **Tak**):

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 6 & 3 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

Zadanie 11

W ciele $\mathbb{Z}_3[x]\Big/_{(x^2+1)}$, gdzie $I = (x^2+1)$ oznacza ideał generowany przez wielomian $f(x) = x^2 + 1$, zachodzi równość:

a) $[x+1]^{-1} = [2x+2]$

b) $[x+1]^{-1} = [x+2]$

c) $-[x+1] = [2x+2]$

Zadanie 11

Definicja

Niech $(P, +, \cdot)$ będzie pierścieniem przemiennym i niech $I \subset P$ będzie ideałem pierścienia P. Mówimy, że $a, b \in P$ *przystają modulo ideał* I, gdy $a - b \in I$ co zapisujemy:

$$a \equiv_I b \qquad \text{lub} \qquad a \equiv b \,(\mathrm{mod}\ I)$$

Definicja

Klasy abstrakcji relacji $\equiv_I$ nazywamy *warstwami*, a zbiór wszystkich klas abstrakcji oznaczamy $P \Big/ I$ i nazywamy *zbiorem ilorazowym*.

Zadanie 11

Twierdzenie

Zbiór $P\Big/_I$ z działaniami dodawania i mnożenia warstw określonymi:

$$[a] \oplus [b] = [a + b], \qquad [a] \odot [b] = [a \cdot b]$$

jest pierścieniem. Nazywamy go pierścieniem ilorazowym pierścienia P przez ideał I. Zerem pierścienia jest $[0] = 0 + I = I$.

Obliczamy z definicji operacji na warstwach:

$$[x + 1][2x + 2] = [2x^2 + 4x + 2] = [x] \neq [1]$$

$$[x + 1][x + 2] = [x^2 + 3x + 2] = [1]$$

$$-[x + 1] = [-(x + 1)] = [2x + 2]$$

Zatem odpowiedź a: **Nie**, b: **Tak**, c: **Tak**.

Zadanie 12

Niech $a = 7 \in \Phi(18)$. Wówczas:

a) $\mathrm{rz}a = 3$

b) $\mathrm{rz}a = 6$

c) $H = \{1, 7, 13\}$ jest podgrupą grupy $\Phi(18)$

Zadanie 12

Definicja

Niech $a \in G$. jeśli $\exists_{n \in \mathbb{N}}\ a^n = e$ to najmniejszą z tych liczb nazywamy *rzędem* elementu a i oznaczamy $\mathrm{rz}a$.

Twierdzenie

Niech $\mathrm{rz}a < \infty$. Wtedy zbiór:

$$H = \{a^0, a^1, a^2, \ldots, a^{\mathrm{rz}a-1}\}$$

jest podgrupą G i $|H| = \mathrm{rz}a$.

Zadanie 12

$$\Phi(18) = \{1, 5, 7, 11, 13, 17\}$$

Parę slajdów temu ustaliliśmy, że liczba elementów podgrupy jest podzielna przez liczbę elementów grupy. Z rzędami jest tak samo, dlatego będziemy sprawdzać tylko potęgę 1, 2, 3 i 6 siódemki:

$$7^1 = 7 \neq 1$$

$$7^2 = 13 \neq 1$$

$$7^3 = 1$$

Zatem 3 jest rzędem 7. Odpowiedzi a: **Tak**, b: **Nie**. Szczęśliwym zbiegiem okoliczności z elementu $a = 7$ wygenerowaliśmy podgrupę z punktu c, a każda podgrupa wygenerowana przez element należący do $\Phi(18)$ jest podgrupą $\Phi(18)$, stąd odpowiedź c: **Tak**.

Zadanie 13

W ciele $\mathbb{Z}_{23}$ zachodzi równość:

a) $-11 = 12$

b) $5^{-1} = 13$

c) $10^{-1} = 7$

Zadanie 13

a. Szukamy elementu przeciwnego do 11 w $\mathbb{Z}_{23}$. Czyli

$$11 + x \equiv 0 \,(\text{mod } 23)$$

$$x \equiv 12 \,(\text{mod } 23)$$

odpowiedź a: **Tak**.

b. Ponieważ $5 \cdot 13 \equiv 19 \not\equiv 1 \,(\text{mod } 23)$, więc odpowiedź b: **Nie**.

c. Ponieważ $10 \cdot 7 \equiv 1 \,(\text{mod } 23)$, zatem odpowiedź c: **Tak**.

Zadanie 14

Użytkownik systemu RSA podał klucz publiczny $K = (n, e) = (55, 7)$. Wówczas klucz deszyfrujący ma postać:

a) $K_D = (55, 48)$

b) $K_D = (40, 7)$

c) $K_D = (55, 23)$

Zadanie 14

Algorytm RSA

1) Wybieramy losowo dwie liczby pierwsze p i q.
2) $n = pq$.
3) Losujemy liczbę nieparzystą e taką że $\text{nwd}(e, \varphi(n)) = 1$.
4) Udostępniamy klucz $K = (n, e)$.
5) $K_D = (n, d)$, gdzie
$$ed \equiv 1 \pmod{\varphi(n)}$$
6) Szyfrowanie wiadomości M:
$$C \equiv f(M) \equiv M^e \pmod{n}$$
7) Deszyfrowanie szyfrogramu C:
$$M \equiv f^{-1}(C) \equiv C^d \pmod{n}$$

Zadanie 14

Pierwszą częścią klucza RSA zawsze będzie n. Wiemy, że:

$$d \equiv e^{-1} \pmod{\varphi(n)}$$

Ponieważ

$$\varphi(55) = 55(1 - \frac{1}{5})(1 - \frac{1}{11}) = 40$$

zatem szukamy elementu odwrotnego do $7 \pmod{40}$. Skoro

$$7 \cdot 48 \equiv 336 \equiv 36 \pmod{40}$$

odpowiedź a: **Nie**. Odpowiedź b w ogóle nie ma sensu - **Nie**.
W c mamy

$$7 \cdot 23 \equiv 161 \equiv 1 \pmod{40}$$

czyli 23 jest elementem odwrotnym do $7 \pmod{40}$, stąd odpowiedź c **Tak**.

Zadanie 15

Niech $I = (2x^2 + 1)$ będzie ideałem głównym. Wówczas:

a) I jest ideałem maksymalnym w pierścieniu $\mathbb{Z}_3[x]$

b) I jest ideałem maksymalnym w pierścieniu $\mathbb{Z}_2[x]$

c) I jest ideałem pierwszym w pierścieniu $\mathbb{Z}_2[x]$

Zadanie 15

Definicja

Ideał I pierścienia przemiennego z jedynką P nazywamy *ideałem pierwszym* gdy:

- $I \neq P$
- $\forall_{a,b \in P}\ ab \in I \Rightarrow a \in I \vee b \in I$

Definicja

Ideał I pierścienia przemiennego z jedynką P nazywamy *ideałem maksymalnym* gdy:

- $I \neq P$
- $\forall_{J \subset P}\ I \subset J \Rightarrow J = I \vee J = P$

Zadanie 15

a. Aby udowodnić, że $I = (2x^2 + 1)$ jest ideałem maksymalnym w $\mathbb{Z}_3[x]$ należy pokazać, że $f = 2x^2 + 1$ jest nierozkładalny.

Elementy odwracalne pierścienia $\mathbb{Z}_3[x]$ to $U = \{1, 2\}$. f jest rozkładalne o ile da się znaleźć takie $g, h \notin U$, że $f = gh$. Zatem $\deg g, \deg h \geq 1$.

Z twierdzenia Bézouta wiemy, że f posiada pierwiastki o ile $\exists_{c \in \mathbb{Z}_3} f(c) = 0$. Istotnie $f(1) = 0$. Stąd f jest rozkładalny:

$$f = 2x^2 + 1 = (x - 1)(2x + 2) = (x + 2)(2x + 2)$$

I nie jest masksymalny w $\mathbb{Z}_3[x]$. Odpowiedź a: **Nie**.

Zadanie 15

Podobnie dowodzimy, że $2x^2 + 1$ jest nierozkładalny w $\mathbb{Z}_2[x]$.

Pierścień $\mathbb{Z}_2[x]$ posiada jeden element odwracalny $U = \{1\}$. Tym razem nie da się znaleźć takich wielomianów $g, h \notin U$, że $f = gh$. Musiałyby mieć stopień 0 i nie należeć do U. Jedyna możliwość to $g = 0$ i $h = 0$, ale $gh \neq f$.

Zatem I musi być maksymalny w $\mathbb{Z}_2[x]$. Odpowiedź b: **Tak**.

Każdy ideał maksymalny jest pierwszy, stąd odpowiedź c: **Tak**.

Koniec

Dziękujemy za uwagę