Rozwiązanie Zadania 4

Zadanie 4 (13 punktów) Dana jest grupa $(G, \cdot)$ taką, że każdy jej element jest rzędu 2. Pokazać, że $(G, \cdot)$ jest grupą abelową. Znajdź element odwrotny do $x = 43$ w ciele $(\mathbb{Z}_{79}, +, \cdot)$.

Część 1: Pokazać, że grupa $(G, \cdot)$ jest grupą abelową, jeśli każdy jej element jest rzędu 2.

Aby grupa $(G, \cdot)$ była grupą abelową (przemienną), musi spełniać cztery warunki: łączność, istnienie elementu neutralnego, istnienie elementu odwrotnego oraz przemienność. Trzy pierwsze warunki są spełnione z definicji grupy. Pozostaje wykazać warunek przemienności.

Z założenia, każdy element $g \in G$ ma rząd 2. Oznacza to, że jeśli element g pomnożymy przez samego siebie, otrzymamy element neutralny e. Możemy to zapisać jako: $g \cdot g = e$

Pokażmy teraz, że w tej grupie każdy element jest swoim własnym elementem odwrotnym, tzn. $g = g^{-1}$.

1. Zaczynamy od definicji rzędu 2 dla elementu g: $g \cdot g = e$
2. Mnożymy obie strony równania z lewej strony przez element odwrotny do g, czyli g^{-1}. (Mnożenie z lewej jest ważne dla poprawności przekształceń w grupach): $g^{-1} \cdot (g \cdot g) = g^{-1} \cdot e$
3. Stosujemy własność **łączności** działania $\cdot$ w grupie, czyli $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. Tutaj $a = g^{-1}$, $b = g$, $c = g$: $(g^{-1} \cdot g) \cdot g = g^{-1} \cdot e$
4. Stosujemy **definicję elementu odwrotnego**, która mówi, że iloczyn elementu i jego elementu odwrotnego daje element neutralny ($g^{-1} \cdot g = e$). Podstawiamy e za $g^{-1} \cdot g$ po lewej stronie równania: $e \cdot g = g^{-1} \cdot e$
5. Stosujemy **definicję elementu neutralnego**, która mówi, że pomnożenie dowolnego elementu przez element neutralny (z lewej lub prawej strony) daje ten sam element ($e \cdot x = x$ oraz $x \cdot e = x$). Stosujemy to zarówno po lewej ($e \cdot g = g$), jak i po prawej ($g^{-1} \cdot e = g^{-1}$) stronie równania: $g = g^{-1}$

Zatem, wykazaliśmy, że w grupie, gdzie każdy element jest rzędu 2, każdy element jest swoim własnym elementem odwrotnym.

Teraz przejdźmy do warunków grupy abelowej, skupiając się na przemienności:

1. **Łączność (Asocjatywność):** Dla każdego $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. Ten warunek jest spełniony z definicji grupy $(G, \cdot)$.
2. **Element neutralny:** Istnieje element $e \in G$ taki, że dla każdego $a \in G$, $a \cdot e = e \cdot a = a$. Ten warunek jest spełniony z definicji grupy $(G, \cdot)$.
3. **Element odwrotny:** Dla każdego $a \in G$ istnieje element $a^{-1} \in G$ taki, że $a \cdot a^{-1} = a^{-1} \cdot a = e$. Ten warunek jest spełniony z definicji grupy $(G, \cdot)$. Co więcej, jak wykazano powyżej, dla tej grupy każdy element jest swoim własnym elementem odwrotnym, tzn. $a^{-1} = a$.
4. **Przemienność (Komutatywność):** Dla każdych dowolnych elementów $a, b \in G$, musimy pokazać, że $a \cdot b = b \cdot a$.
   - Weźmy dowolne elementy $a, b \in G$.
   - Z definicji grupy, jeśli $a \in G$ i $b \in G$, to również ich iloczyn $a \cdot b \in G$ (własność zamkniętości).
   - Ponieważ każdy element w grupie G ma rząd 2, element $(a \cdot b)$ również musi mieć rząd 2. Zatem: $(a \cdot b)^2 = e$ co jest równoważne: $(a \cdot b) \cdot (a \cdot b) = e$
   - Wiemy, że element odwrotny do iloczynu dwóch elementów w grupie jest iloczynem ich elementów odwrotnych w odwróconej kolejności (jedna z podstawowych własności grup): $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$
   - Z wcześniejszych ustaleń (punkt 4 dowodu), wiemy, że w tej grupie każdy element jest swoim własnym elementem odwrotnym. Zatem, możemy podstawić $a^{-1} = a$ i $b^{-1} = b$: $b^{-1} \cdot a^{-1} = b \cdot a$
   - Z drugiej strony, ponieważ $(a \cdot b)$ jest elementem rzędu 2 (jak wyżej), to również jest swoim własnym elementem odwrotnym: $(a \cdot b)^{-1} = a \cdot b$
   - Porównując te dwa wyrażenia na $(a \cdot b)^{-1}$, otrzymujemy: $a \cdot b = b \cdot a$

   Ponieważ warunek przemienności ($a \cdot b = b \cdot a$) został wykazany dla dowolnych elementów $a, b \in G$, grupa $(G, \cdot)$ jest grupą abelową.

Część 2: Znajdź element odwrotny do $x = 43$ w ciele $(\mathbb{Z}_{79}, +, \cdot)$.

W ciele $(\mathbb{Z}_{79}, +, \cdot)$ szukamy elementu odwrotnego do $x = 43$ względem mnożenia. Oznacza to, że poszukujemy takiej liczby całkowitej $y \in \{0, 1, \ldots, 78\}$, dla której spełnione jest równanie kongruencji: $43 \cdot y \equiv 1 \pmod{79}$

Do znalezienia elementu odwrotnego wykorzystamy rozszerzony algorytm Euklidesa. Chcemy znaleźć takie liczby całkowite y i k, dla których spełnione jest równanie: $43y + 79k = 1$

Kroki algorytmu Euklidesa dla NWD$(79, 43)$:

1. $79 = 1 \cdot 43 + 36$
2. $43 = 1 \cdot 36 + 7$
3. $36 = 5 \cdot 7 + 1$ (Reszta wynosi 1, co oznacza, że NWD$(79, 43) = 1$, a więc element odwrotny istnieje)
4. $7 = 7 \cdot 1 + 0$

Teraz, cofamy się w algorytmie (podstawiamy reszty z równań w górę), aby wyrazić 1 jako kombinację liniową 79 i 43: Z równania (3): $1 = 36 - 5 \cdot 7$

Z równania (2), podstawiamy $7 = 43 - 1 \cdot 36$:

$$\begin{aligned} 1 &= 36 - 5 \cdot (43 - 1 \cdot 36) \\ 1 &= 36 - 5 \cdot 43 + 5 \cdot 36 \\ 1 &= 6 \cdot 36 - 5 \cdot 43 \end{aligned}$$

Z równania (1), podstawiamy $36 = 79 - 1 \cdot 43$:

$$\begin{aligned} 1 &= 6 \cdot (79 - 1 \cdot 43) - 5 \cdot 43 \\ 1 &= 6 \cdot 79 - 6 \cdot 43 - 5 \cdot 43 \\ 1 &= 6 \cdot 79 - 11 \cdot 43 \end{aligned}$$

Otrzymaliśmy równanie diofantyczne $1 = -11 \cdot 43 + 6 \cdot 79$. Odczytując je modulo 79, otrzymujemy: $-11 \cdot 43 \equiv 1 \pmod{79}$

Elementem odwrotnym do 43 jest -11 w arytmetyce modulo 79. Aby przedstawić go jako liczbę dodatnią w zakresie od 0 do 78, dodajemy 79 do -11: $-11 + 79 = 68$

Zatem elementem odwrotnym do $x = 43$ w ciele $(\mathbb{Z}_{79}, +, \cdot)$ jest **68**.

Sprawdzenie: Aby upewnić się co do poprawności rozwiązania, wykonujemy mnożenie: $43 \cdot 68 = 2924$ Następnie sprawdzamy resztę z dzielenia 2924 przez 79: $2924 \div 79 = 37$ z resztą 1. Czyli, $2924 = 37 \cdot 79 + 1$, co oznacza $2924 \equiv 1 \pmod{79}$. Wynik jest poprawny.