

Wykład 5

Liczby a i b nazywamy **względnie pierwszymi** jeśli $\text{NWD}(a, b) = 1$.

Twierdzenie 1 Liczby a i b są względnie pierwsze wtedy i tylko wtedy gdy istnieją liczby całkowite u, v , takie że $au + bv = 1$.

Twierdzenie 2 Równanie $a \cdot_n x = 1$ ma rozwiązanie w pierścieniu Z_n wtedy i tylko wtedy gdy liczby a i n są względnie pierwsze. Inaczej mówiąc liczba a jest odwracalna względem \cdot_n wtedy i tylko wtedy gdy liczby a i n są względnie pierwsze.

Dowód Jeśli $\text{NWD}(a, n) = 1$ to zgodnie z powyższym Twierdzeniem istnieją liczby całkowite u, v takie, że $au + bv = 1$ wtedy stosując funkcję f_n otrzymujemy: $f_n(au + bv) = f_n(1) = 1$, stąd $f_n(a) \cdot_n f_n(u) = 1$, a więc liczba a jest odwracalna modulo n . Jeśli teraz liczba a jest odwracalna modulo n to istnieje b , że $a \cdot_n b = 1$ i $a \cdot b - 1 = 0$ to oznacza, że $n | (ab - 1)$, a więc istnieje k , że $ab - 1 = kn$, zatem równanie $ax + ny = 1$ ma rozwiązanie, a to oznacza, że liczby a i n są względnie pierwsze. \square

Zadanie Znaleźć liczbę odwrotną do 15 w Z_{37} .

Rozwiązanie Ponieważ liczby 15 i 37 są względnie pierwsze to liczba 15 jest odwracalna w Z_{37} . Musimy rozwiązać równanie $15x + 37y = 1$, a więc skorzystamy z algorytmu Euklidesa:

$$\begin{aligned} 37 &= 2 \cdot 15 + 7 \\ 15 &= 2 \cdot 7 + 1 \\ 7 &= 7 \cdot 1 + 0 \end{aligned}$$

a więc mamy: $1 = 15 - 2 \cdot 7 = 15 - 2(37 - 2 \cdot 15) = 5 \cdot 15 - 2 \cdot 37$. To oznacza, że liczbą odwrotną do 15 w Z_{37} jest 5.

Element $x \in R$ nazywamy **dzielnikiem zera** jeśli $x \neq 0$ i istnieje $0 \neq y \in R$, że $x \odot y = 0$.

Przykład Pierścień $(\mathbb{Z}, +, \cdot)$ jest pierścieniem bez dzielników zera. Natomiast w pierścieniu $(Z_4, +_4, \cdot_4)$ element 2 jest dzielnikiem 0.

Element $u \in R$ pierścienia z jednością nazywamy **elementem odwracalnym** jeśli jest odwracalny względem \odot , a więc:

$$\exists u' \in R \quad u \odot u' = u' \odot u = 1.$$

Zbiór wszystkich elementów odwracalnych oznaczamy przez R^* .

Przykład W pierścieniu Z_8 elementy 1, 3, 5, 7 są odwracalne, bo $3 \cdot_8 3 = 1$, $5 \cdot_8 5 = 1$, $7 \cdot_8 7 = 1$.

Jak stwierdziliśmy powyżej, w pierścieniu Z_n , odwracalne są te elementy a dla, których $\text{NWD}(a, n) = 1$.

Twierdzenie 3 *Jeśli (R, \oplus, \odot) jest pierścieniem z jednością to (R^*, \odot) jest grupą.*

Pierścień (R, \oplus, \odot) przemienny z jednością nazywamy **ciałem** jeśli R ma co najmniej dwa elementy i $R^* = R - \{0\}$, tzn. każdy niezerowy element jest odwracalny.

Przykłady

1. $(\mathbb{Z}, +, \cdot)$ nie jest ciałem, bo $\mathbb{Z}^* = \{1, -1\}$,
2. $(\mathbb{R}, +, \cdot)$ jest ciałem,
3. $(\mathbb{Z}_2, +_2, \cdot_2)$ jest ciałem,
4. $(\mathbb{Z}_4, +_4, \cdot_4)$ nie jest ciałem, bo $\mathbb{Z}_4^* = \{1, 3\} \neq \mathbb{Z}_4 - \{0\}$.

Twierdzenie 4 *W ciele nie ma dzielników zera.*

Dowód Jeśli R jest ciałem i $a, b \in R$ są elementami, takimi że $a \neq 0$ i

$$ab = 0$$

to istnieje a^{-1} . Mnożąc równanie obustronnie przez a^{-1} otrzymujemy:

$$a^{-1}ab = 0$$

Stąd $b = 0$. ■

Niech $p \in \mathbb{Z}$, mówimy, że p jest liczbą pierwszą jeśli p jest podzielna tylko przez 1 i przez siebie.

Twierdzenie 5 *Jeśli n nie jest liczbą pierwszą to \mathbb{Z}_n nie jest ciałem.*

Dowód Jeśli n nie jest liczbą pierwszą to istnieją $k \neq 1, l \neq 1$, takie że $n = kl$. Wtedy k jest dzielnikiem zera w pierścieniu \mathbb{Z}_n . ■

Twierdzenie 6 *Pierścień $(\mathbb{Z}_n, +_n, \cdot_n)$ jest ciałem wtedy i tylko wtedy gdy n jest liczbą pierwszą.*