

Wstęp do Teorii Liczb

na podstawie wykładu dr. Bartosza Żrałka

Michał Posiadała, Kinga Klaudia Werońska, Filip Nogaj

Data ostatniej aktualizacji: 12 listopada 2024

1

Definicja 1.1: Podzielność

Niech $d, a \in \mathbb{Z}$. Mówimy, że d DZIELI/jest WIELOKROTNOŚCIĄ a , jeśli $a = dc$ dla pewnego $c \in \mathbb{Z}$.

Ozn. (d) - zbiór wszystkich wielokrotności d .

Twierdzenie 1.1

Niech $d, a_1, a_2, k \in \mathbb{Z}$.

- (i) Jeśli $d|a_1$ i $d|a_2$ to $d|a_1 + a_2$.
- (ii) Jeśli $d|a_1$, to $d|ka_1$.

Dowód:

- (i) Jeśli $a_1 = dc_1, a_2 = dc_2$, to $a_1 + a_2 = d(c_1 + c_2)$.
- (ii) Jeśli $a_1 = dc$, to $ka_1 = dkc$.

Definicja 1.2: Ideał pierścienia \mathbb{Z}

IDEAŁEM PIERŚCIENIA \mathbb{Z} nazywamy niepusty podzbiór I zbioru \mathbb{Z} spełniający:

- (i) $\forall_{a_1, a_2 \in I} a_1 + a_2 \in I$,
- (ii) $\forall_{k \in \mathbb{Z}, a \in I} ka \in I$.

Ozn. $I \triangleleft \mathbb{Z}$

Twierdzenie 1.2: Dzielienie z resztą w \mathbb{Z}

Niech $a, b \in \mathbb{Z}, b \neq 0$. Wtedy istnieje dokładnie jedna para liczb całkowitych (q, r) spełniająca

$$a = bq + r, \quad 0 \leq r < |b|.$$

Dowód:

Założmy, że $b > 0$ i rozważmy $W = \{bx : x \in \mathbb{Z}, bx \leq a\}$ i poczynimy kilka obserwacji:

- $W \subset \mathbb{Z}$
- W jest ograniczone z góry (przez a)
- $W \neq \emptyset$

Niech $bq = \max W$. Weźmy $r = a - bq$. Skoro $bq \in W$, to $bq < a$, czyli $\frac{r}{a-bq} \geq 0$. Ponadto $b(q+1) = bq + b > bq$, a skoro $bq = \max W$, to $b(q+1) \notin W$. Innymi słowy $b(q+1) > a$ tzn. $b > \underbrace{a - bq}_r$.

Założmy, że $b < 0$. Najpierw dzielimy a przez $-b$:

$$a = -b \cdot \tilde{q} + \tilde{r} \text{ dla } \tilde{q}, \tilde{r} \in \mathbb{Z}, 0 \leq \tilde{r} < -b$$

$$a = b \cdot (-\tilde{q} + \tilde{r})$$

$$q := -\tilde{q} \quad r := \tilde{r} \quad 0 \leq r < |b|$$

Pozostaje wykazać jednoznaczność pary (q, r) .

Założmy, że są dwie takie pary $(q_1, r_1), (q_2, r_2) \in \mathbb{R}^2$ które spełniają

$$a = bq_i + r_i, \quad 0 \leq r_i \leq |b| \text{ dla } i = 1, 2$$

$$\begin{aligned} bq_1 + r_1 &= q_2 + r_2 \\ |b(q_1 - q_2)| &= |r_2 - r_1| < |b| \\ |b(q_1 - q_2)| &< |b| \end{aligned}$$

Jako że $b \neq 0$, dzielimy przez $|b|$:

$$|q_1 - q_2| < 1$$

Skoro $q_1, q_2 \in \mathbb{Z}$, to z tego wynika, że $q_1 = q_2$, a z tego wynika, że $r_1 = r_2$, udowodniliśmy więc jednoznaczność.

Twierdzenie 1.3

Niech $I \triangleleft \mathbb{Z}$. Wtedy $I = (d)$ dla pewnego d .

Dowód:

Możemy założyć, że $I \neq (0)$. Wtedy $I \cap \mathbb{N} \neq \emptyset$, bo istnieje $a \in I, a \neq 0$. Z własności ideału, $(\pm 1) \cdot a \in I$.

Niech $d = \min(I \cap \mathbb{N})$. Pozostaje uzasadnić, że $I = (d)$.

- Inkluzja $(d) \subseteq I$ jest oczywista, bo $d \in I$.
- Niech $a \in I$. Chcemy pokazać, że $a \in (d)$. Mamy

$$r = \underbrace{a}_{\in I} - \underbrace{dq}_{\in I}$$

Z def. d otrzymujemy $r = 0$, tzn. $a = dq \in (d)$.

Definicja 1.3: Ideał generowany

Dla $a_1, \dots, a_k \in \mathbb{Z}$ zdefiniujemy

$$(a_1, \dots, a_k) := \{l_1 a_1 + \dots + l_k a_k, l_i \in \mathbb{Z}\}$$

Jest to najmniejszy (w sensie inkluzji) ideał zawierający a_1, \dots, a_k . Nazywamy go IDEAŁEM GENEROWANYM.

Twierdzenie 1.4

Niech $a, b \in \mathbb{Z}$. Wtedy

1. $a|b \iff (b) \subseteq (a)$
2. $(a) = (b) \iff a = \pm b$

Dowód:

$$(i) \quad (b) \subseteq (a) \iff b \in (a) \iff \exists_{c \in \mathbb{Z}} b = ac \iff a|b$$

(ii)

$$\begin{aligned} (a) = (b) &\iff \begin{cases} (a) \subseteq (b) \\ (b) \subseteq (a) \end{cases} \iff \begin{cases} b|a \\ a|b \end{cases} \iff b = ka = klb, \quad k, l \in \mathbb{Z} \iff \\ &\iff b(kl - 1) = 0 \end{aligned}$$

Z czego wynika, że $a = \pm b$.

Definicja 1.4: Największy Wspólny Dzielnik

Niech $a_1, \dots, a_k \in \mathbb{Z}$. Niech $d \in \mathbb{Z}_{\geq 0}$ spełnia:

- (i) $d|a_1, \dots, d|a_k$,
- (ii) jeśli $d' \in \mathbb{Z}_{\geq 0}$ spełnia $d'|a_1, \dots, d'|a_k$ to $d'|d$.

Wtedy nazywamy d **NAJWIĘKSZYM WSPÓLNYM DZIELNIKIEM** i oznaczamy

$$d = NWD(a_1, \dots, a_k).$$

Twierdzenie 1.5

Dla ustalonego zestawu $a_1, \dots, a_k \in \mathbb{Z}$, $NWD(a_1, \dots, a_k)$ istnieje i jest wyznaczone jednoznacznie.

Dowód:

1. Istnienie

Rozważmy $I = (a_1, \dots, a_k)$. Na podstawie Twierdzenia 1.1 wiemy, że istnieje takie $n \in \mathbb{N}$, że $I = (n)$. Weźmy $d = |n|$. Chcemy pokazać, że d spełnia założenia NWD .

- (i) $(a_i) \subseteq (a_1, \dots, a_k) = (d)$,
więc z twierdzenia 1.4 $d|a_i$ dla $i = 1, \dots, k$
- (ii) Niech $d' \in \mathbb{Z}_{\geq 0}$, $d'|a_i$ dla $i = 1, \dots, k$. Zatem $a_i \in (d')$, więc $(d) = (a_1, \dots, a_k) \subseteq (d')$
czyli $d'|d$ z twierdzenia 1.4.

2. Jedyność

Jeśli d_1 i d_2 spełniają definicję NWD , to

$$\left. \begin{array}{l} d_1|d_2 \\ d_1|d_2 \end{array} \right\} \implies d_1 = d_2$$

Wniosek 1.1

Niech $a_1, \dots, a_k \in \mathbb{Z}$. Wtedy istnieją x_1, \dots, x_k takie, że $NWD(a_1, \dots, a_k) = x_1a_1 + \dots + x_ka_k$.

Dowód:

$NWD(a_1, \dots, a_k)$ jest nieujemnym generatorem ideału (a_1, \dots, a_k) , którego każdy element jest wyżej wymienionej postaci.

2

Twierdzenie 2.1: istnienie i jedyność NWW liczb całkowitych

Niech $a_1, \dots, a_k \in \mathbb{Z}$. Istnieje dokładnie jedna liczba $m \in \mathbb{Z}_{\geq 0}$ taka, że:

- (i) $a_1|m, \dots, a_k|m$,
- (ii) jeśli $m' \in \mathbb{Z}_{\geq 0}, a_1|m', \dots, a_k|m'$, to $m|m'$.

Liczbę m nazywamy NAJMNIEJSZĄ WSPÓLNĄ WIELOKROTNOŚCIĄ i oznaczamy $NWW(a_1, \dots, a_k)$.

Dowód:

Istnienie:

Weźmy m - nieujemny generator ideału $(a_1) \cap \dots \cap (a_k)$.

- (i) $m \in (a_1) \cap \dots \cap (a_k) \subset (a_i)$, więc $a_i|m$ dla $i = 1, \dots, k$
- (ii) Załóżmy, że $a_1|m', \dots, a_k|m'$. Innymi słowy $m' \in (a_1), \dots, m' \in (a_k)$. Zatem $m' \in (a_1) \cap \dots \cap (a_k) = (m)$. Stąd $m|m'$.

Jedyność:

Jeśli m_1, m_2 spełniają warunki (i) i (ii), to $m_1|m_2$ i $m_2|m_1$, więc $m_1 = m_2$.

Definicja 2.1: liczby względnie pierwsze

Liczby całkowite a, b nazywamy WZGLĘDNIIE PIERWSZYMI, jeśli $NWD(a, b) = 1$.

Twierdzenie 2.2: Bachet

Weźmy $a, b, c \in \mathbb{Z}$. Niech a i b będą względnie pierwsze oraz niech $a|bc$. Wtedy $a|c$.

Dowód:

Z wniosku 1.1 możemy napisać $xa + yb = 1$ dla pewnych $x, y \in \mathbb{Z}$. Stąd $c = xac + ybc$, co jest podzielne przez a .

Definicja 2.2: liczba pierwsza

Liczbę $p \in \mathbb{N}, p \geq 2$ nazywamy LICZBĄ PIERWSZĄ, jeśli jej jedynymi dzielnikami naturalnymi są 1 i p .

Ozn. \mathbb{P} - zbiór wszystkich liczb pierwszych

Lemat 2.1

Niech $p \in \mathbb{P}, a, b \in \mathbb{Z}$ i $p|ab$. Wtedy $p|a$ lub $p|b$.

Dowód:

Przypuśćmy, że $p \nmid a$. Wtedy $NWD(p, a) = 1$ (bo $NWD(p, a)|p$, więc $NWD(p, a) = 1$ lub $NWD(p, a) = p$, a jeśli $NWD(p, a) = p$, to $p = NWD(p, a)|a$).

Wobec tego $p|b$ z twierdzenia 2.2.

Wniosek 2.1

Niech $p \in \mathbb{P}, a_1, \dots, a_k \in \mathbb{Z}, p|a_1 \cdot \dots \cdot a_k$. Wtedy $p|a_i$ dla pewnego $i = 1, \dots, k$.

Dowód:

Indukcja ze względu na k :

1. dla $k = 1$ oczywiste

2. Przypuśćmy, że wniosek zachodzi dla $k \in \mathbb{N}$.

Niech $p \in \mathbb{P}$, $a_1, \dots, a_{k+1} \in \mathbb{Z}$ oraz $p|a_1 \cdot (a_2 \cdot \dots \cdot a_{k+1})$. Z lematu 2.1 $p|a_1$ lub $p|(a_2 \cdot \dots \cdot a_{k+1})$.

Wobec tego, z założenia indukcyjnego, $p|a_1$ lub $p|a_2$ lub...lub $p|a_{k+1}$.

Twierdzenie 2.3

Każdą liczbę naturalną $n > 1$ można rozłożyć na iloczyn liczb pierwszych. Taki rozkład jest jednoznaczny (z dokładnością do kolejności czynników).

Dowód:

Istnienie - indukcja ze względu na n :

1. $n = 2 \in \mathbb{P}$

2. Załóżmy, że $n \in \mathbb{N}$, $n > 2$ oraz, że każda liczba naturalna m , $1 < m < n$ rozkłada się na iloczyn liczb pierwszych. Jeśli n jest pierwsze, to szukany rozkładem jest $n = n$. Załóżmy więc, że $n \notin \mathbb{P}$. Wtedy $n = n_1 n_2$, gdzie $n_1, n_2 \in \mathbb{N}$, $1 < n_1, n_2 < n$.

Z założenia indukcyjnego $n_1 = \prod_{p \in \mathbb{P}} p^{\alpha_p}$, $n_2 = \prod_{p \in \mathbb{P}} p^{\beta_p}$.

Wtedy $n = n_1 n_2 = \prod_{p \in \mathbb{P}} p^{\alpha_p + \beta_p}$.

Jednoznaczność - indukcja ze względu na n :

1. $n = 2$ - rozkład jednoznaczny w postaci iloczynu liczb pierwszych

2. Niech $n \in \mathbb{N}$, $n > 2$. Załóżmy, że rozkład na iloczyn liczb pierwszych każdej liczby naturalnej $1 < m < n$ jest jednoznaczny z dokładnością do kolejności czynników.

Założmy, że $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k} = p_1^{\beta_1} \cdot \dots \cdot p_k^{\beta_k}$, gdzie $p_i \in \mathbb{P}$, $p_i \neq p_j$ dla $i \neq j$ oraz $\alpha_i, \beta_i \in \mathbb{Z}_{\geq 0}$ (mogą być zerowe).

Skoro $n > 1$, to nie wszystkie $\alpha_1, \dots, \alpha_k$ są zerowe. BSO założmy, że $n_1 \geq 1$. Wtedy $p_1|n$.

Mamy zatem $p_1 | \underbrace{(p_1 \cdot \dots \cdot p_1)}_{\beta_1 \text{ czynników}} \cdot \dots \cdot \underbrace{(p_k \cdot \dots \cdot p_k)}_{\beta_k \text{ czynników}}$.

Z wniosku 2.1, gdyby $\beta_1 = 0$, to mielibyśmy $p_1|p_j$ dla $j \neq 1$, co daje $p_1 = p_j$, a to jest sprzeczność.

Zatem $\beta_1 \geq 1$. W takim razie $p_1^{\alpha_1-1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k} = \frac{n}{p_1} = p_1^{\beta_1-1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_k^{\beta_k}$.

Z założenia indukcyjnego ($\frac{n}{p_1} < n$) otrzymujemy:

$$\alpha_1 - 1 = \beta_1 - 1 \Leftrightarrow \alpha_1 = \beta_1,$$

$$\alpha_2 = \beta_2,$$

.

.

.

$$\alpha_k = \beta_k.$$

Uogólnienie dla pierścienia $A \in \{\mathbb{Z}, K[X], \mathbb{Z}[i]\}$:

- definicja podzielności pozostaje taka sama

- dzielenie z resztą w A :

Dla $a, b \in A$, $b \neq 0$ istnieją $q, r \in A$ spełniające $a = bq + r$ oraz $N(r) < N(b)$, gdzie dla $u \in A$

$$N(u) = \begin{cases} |u| & \text{dla } A = \mathbb{Z}, \\ |u|^2 = \bar{u}u & \text{dla } A = \mathbb{Z}[i], \\ 2^{\deg(u)} & \text{dla } A = K[X]. \end{cases}$$

3

Definicja 3.1

Elementy $a, b \in A$ nazywamy STOWARZYSZONYMI (co zapisujemy $a \sim b$), jeśli $a = ub$, gdzie $u \in A^*$ (grupy elementów odwracalnych pierścienia A).

Grupy elementów odwracalnych pierścienia $A \in \{\mathbb{Z}, K[X], \mathbb{Z}[i]\}$:

- $\mathbb{Z}^* = \{-1, 1\}$
- $K[X]^* = K^* = K$

- $\mathbb{Z}[i]^* = \{-i, i, -1, 1\}$

Zauważmy bowiem, że jeśli $a \in \mathbb{Z}[i]^*$ to $ab = 1$ dla pewnego $b \in \mathbb{Z}[i]$. Stąd $N(a)N(b) = N(1) = 1$. Jedynymi elementami $\mathbb{Z}[i]$ mającymi normę 1 są $-i, i, -1, 1$. Przy czym te elementy są odwracalne w $\mathbb{Z}[i]$. (Widzimy, że jeśli $N(a) = 1$ to $a^{-1} = \bar{a}$.)

W tym wykładzie A zawsze oznacza jeden z trzech wymienionych powyżej pierścieni. Jeśli dowody twierdzeń są pominięte, oznacza to, że są analogiczne do dowodu dla \mathbb{Z} .

Lemat 3.1

Niech $a, b \in A$. Wówczas:

- (i) $a|b \Leftrightarrow (b) \subset (a)$
- (ii) $(a) = (b) \Leftrightarrow a \sim b$

Twierdzenie 3.1

W pierścieniu A każdy ideał jest główny. Mówimy, że A jest PIERŚCIENIEM IDEAŁÓW GŁÓWNYCH (w skrócie po polsku PIG).

Dowód:

Niech $I \triangleleft A$. Jeśli $I \neq (0)$ to pokazujemy, że element o najmniejszej dodatniej normie w I jest generatorem I .

Twierdzenie 3.2: Największy Wspólny Dzielnik w A

Niech $a_1, \dots, a_k \in A$. Istnieje dokładnie jeden element $d \in A$, z dokładnością do stowarzyszenia pierścienia A , spełniający:

- (i) $d|a_1, \dots, d|a_k$,
- (ii) jeśli $d' \in A$ spełnia $d'|a_1, \dots, d'|a_k$ to $d'|d$.

Ten element d oznaczamy $NWD(a_1, \dots, a_k)$.

Twierdzenie 3.3: Najmniejsza Wspólna Wielokrotność w A

Niech $a_1, \dots, a_k \in A$. Z dokładnością do stowarzyszenia istnieje dokładnie jeden element $m \in A$ taki, że:

- (i) $a_1|m, \dots, a_k|m$,
- (ii) jeśli $m' \in A, a_1|m', \dots, a_k|m'$, to $m|m'$.

Ten element m oznaczamy $NWW(a_1, \dots, a_k)$.

Twierdzenie 3.4

Niech $a, b \in A, a|bc, NWD(a, b) \sim 1$. Wówczas $a|c$.

Definicja 3.2

Element $a \in A, a \neq 0, a \notin A^*$ nazywamy NIEROZKŁADALNYM jeśli jedynymi (z dokładnością do stowarzyszenia) dzielnikami a są 1 i a .

Twierdzenie 3.5

Niech γ będzie elementem nierozkładalnym pierścienia $A, a, b \in A, \gamma|ab$. Wtedy:
 $\gamma|a$ lub $\gamma|b$

Uwaga 1:

Element $\gamma \in A, \gamma \neq 0, \gamma \notin A^*$ spełniający warunek: $\forall a, b \in A : \gamma|ab \Rightarrow \gamma|a \vee \gamma|b$ nazywamy elementem pierwszym. Zatem powyższe twierdzenie można sformułować tak:

Każdy element nierozkładalny pierścienia A jest pierwszy.

Uwaga 2:

W dowolnej dziedzinie całkowitości każdy niezerowy element pierwszy jest nierozkładalny. W szczególności w naszym pierścieniu A zbiór wszystkich elementów nierozkładalnych to zbiór wszystkich elementów pierwszych.

Niech γ będzie pierwszy w dziedzinie całkowitości $D, \gamma = ab$, gdzie $a, b \in D$. Z definicji $\gamma|a \vee \gamma|b$. Przypuśćmy, że $\gamma|a \Rightarrow a = \gamma c$, gdzie $c \in D$. Wówczas:
 $\gamma = \gamma cb \Rightarrow 1 = cb$

Wniosek 3.1

Niech γ będzie nierozkładalny w A i niech $a_1, \dots, a_k \in A$ takie, że $\gamma|a_1 \cdot \dots \cdot a_k$.
 Wtedy $\gamma|a_i$ dla pewnego i .

Twierdzenie 3.6: Jednoznaczność rozkładu w A

Niech $a \in A, a \neq 0, a \notin A^*$. Element a można zapisać jednoznacznie z dokładnością do kolejności czynników i ich stowarzyszenia w postaci iloczynu elementów nierozkładalnych.

Dowód:

Dowód przebiega analogicznie do dowodu tego twierdzenia dla $A = \mathbb{Z}$, z indukcją ze względu na $N(a)$.

- W \mathbb{Z} zbiór wszystkich elementów nierozkładalnych to $\{\pm p : p \in \mathbb{P}\}$

- Opiszmy zbiór wszystkich elementów nierozkładalnych w $\mathbb{Z}[i]$.

Niech $\gamma \in \mathbb{Z}[i]$ będzie nierozkładalny.

Zauważmy, że $\gamma|\gamma\bar{\gamma} = N(\gamma)$ przy tym: $N(\gamma) \in \mathbb{N}, N(\gamma) > 1$. $N(\gamma)$ możemy rozłożyć w \mathbb{Z} na iloczyn liczb pierwszych. Wobec tego $\gamma|p$ dla pewnego $p \in \mathbb{P}$. Zauważmy, że γ nie może dzielić dwóch różnych $p, q \in \mathbb{P}$. Mielibyśmy bowiem: $\gamma|NWD(p, q) = 1$. Pozostaje opisać jak $p \in \mathbb{P}$ rozkłada się w $\mathbb{Z}[i]$.

Uwaga ogólna:

Jeśli $a \in \mathbb{Z}[i], N(a) \in \mathbb{P}$ to a jest nierozkładalny w $\mathbb{Z}[i]$.

$$a = bc$$

$$\mathbb{P} \ni N(a) = N(b)N(c) \Rightarrow N(b) = 1 \vee N(c) = 1$$

Czyli:

$$b \in A^* \vee c \in A^*$$

- $2 = i(1 - i)^2$, gdzie $i \in \mathbb{Z}[i]^*$
 $(1 - i)$ jest nierozkładalne w $\mathbb{Z}[i]$ ponieważ $N(1 - i) = 2 \in \mathbb{P}$

Dowód:

Niech $p \in \mathbb{P} \setminus \{2\}$. Załóżmy, że $p \nmid \alpha \cdot \beta$, gdzie α nierozkładalne. Wtedy

$$\underbrace{N(p)}_{p^2} = \underbrace{N(\alpha)}_{\neq 1} \cdot N(\beta)$$

Zatem są dwie możliwości

1. Albo $N(\alpha) = p^2, N(\beta) = 1$ co oznacza, że $\beta \in \mathbb{Z}[i]^*$ czyli $p \sim \alpha$. W szczególności p nierozkładalne
2. Albo $N(\alpha) = p$
Niech $\alpha = a + ib, a, b \in \mathbb{Z}$
Otrzymujemy $\alpha \bar{\alpha} = p$, tzn $p = a^2 + b^2$
Zauważmy, że $a^2 + b^2 \pmod{4} \in \{1, 2\}$

$$0^2 \equiv 0(4) \quad 1^2 \equiv 1(4) \quad 2^2 \equiv 0(4) \quad 3^2 \equiv 1(4)$$

Mamy, że dla $p \equiv 3(4)$ zachodzi przypadek 1), czyli takie p jest nierozkładalne w $\mathbb{Z}[i]$.

Pozostaje przypadek $p \equiv 1(4)$. Zauważmy że zachodzi następujące twierdzenie:

Twierdzenie 3.7

Dla każdego $p \in \mathbb{P}, p \equiv 1(4)$ istnieje $x \in \mathbb{Z}$ spełniający

$$x^2 \equiv -1(p)$$

Zaaplikujmy powyższe twierdzenie do $p \equiv 1(4)$. Weźmy $x \in \mathbb{Z}, x^2 \equiv -1(p)$. Innymi słowy $p \mid (x^2 + 1) \iff p \mid (x - i)(x + i)$ w $\mathbb{Z}[i]$.

Zauważmy, że $NWD(p, x + i) \nmid 1, p$

- $NWD(p, x + i) \nmid 1$
W.p.p z tw. Barcheta mieliśmy $p \mid (x - i)$ SPRZECZNOŚĆ
- $NWD(p, x - i) \nmid p$
Analogicznie, w.p.p z tw. Barcheta mieliśmy $p \mid (x + i)$ SPRZECZNOŚĆ

Napiszemy $NWD(p, x + i) \sim a + bi$.

Skoro $NWD(p, x + i) \nmid 1$, to $a + ib \notin \mathbb{Z}[i]^*$

Stąd $N(a + ib) > 1$

- $a + ib \mid p, p = (a + ib) \cdot \gamma, \quad \gamma \in \mathbb{Z}[i]$
Zatem $N(a + ib) \mid N(p) = p^2$. Pozostają dwie możliwości:

$$N(a + ib) = p \vee N(a + ib) = p^2$$

Jeśli $N(a + ib) = p^2$ to $N(\gamma) = 1$, czyli $\gamma \in \mathbb{Z}[i]^*$.

Mieliśmy $a + ib \sim p$, przez co $NWD(p, x + i) \nmid p$.

Pokazaliśmy więc, że $N(a + ib) = p$. Oznacza to, że $p = (a + ib)(a - ib)$, a skoro $N(a + ib) = p \in \mathbb{P}$, to $a - ib$ oraz $a + ib$ są nierozkładalne.

Zauważmy jeszcze, że $a + ib \nmid a - ib$

W szczególności $a + ib \nmid a - ib$

Oczywiście $a + ib \mid a + ib$

Stąd $a + ib \mid a - ib + (a + ib) = 2a$

Bierzemy normy: $p = N(a + ib) \mid N(2a) = 4a^2$

Podobnie $a + ib \mid (a + ib) - (a - ib) = 2ib, \quad p \mid N(2ib) = 4b^2$

Skoro $p \in \mathbb{P} \setminus \{2\}$ to $p \mid a \wedge p \mid b$ to

$$a + ib = p(a' + ib')$$

$$a - ib = p(a' - ib')$$

$$p = p^2(a' + ib')(a' - b'i)$$

$$1 = p(a'^2 + b'^2)$$

Wniosek 4.1

Każdą liczbę $p \in \mathbb{P}, p \equiv 1(4)$ można zapisać jako $a^2 + b^2$ dla pewnych $a, b \in \mathbb{Z}$. To przedstawienie jest jedyne, z dokładnością do znaku i permutacją a z b .

Wynika to z jednoznaczności rozkładu $(a + bi)(a - ib)$ z dokładnością do kolejności czynników nierozkładalnych i ich stowarzyszenia, czyli z dokładnością do $\pm 1, \pm i$.

Metoda 4.1: wyznaczania $p = x^2 + y^2$

1. Znajdź $x \in \mathbb{Z}$, t. że $x^2 \equiv -1(p)$
2. Oblicz $NWD(p, x + i)$ w $\mathbb{Z}[i]$ za pomocą algorytmu Euklidesa.
3. $NWD(p, x + i) \sim a + ib$
4. $p = a^2 + b^2$

Konstrukcja pierścienia ilorazowego R/I :

Zakładamy, że R jest przemienny i z 1.

I - ideał pierścienia R ($I \triangleleft R$).

Stwierdzenie 4.1

Relacja \equiv w \mathbb{R} określona $a \equiv b \iff a - b \in I$ jest relacją równoważności. Klasę równoważności elementu a oznaczamy $[a]_I$.

Dowód:

- zwrotność

$$a - a = 0 \in I \implies a \equiv a$$

- symetryczność

$$a \equiv b \iff a - b \in I \iff (-1)(b - a) \in I \iff b \equiv a$$

- przechodność

$$\left. \begin{matrix} a \equiv b \\ b \equiv c \end{matrix} \right\} \implies \left. \begin{matrix} a - b \in I \\ b - c \in I \end{matrix} \right\} \implies a - b + b - c \in I \implies a - c \in I \iff a \equiv c$$

5

Stwierdzenie 5.1

Określmy następujące działania w R/I :

- $[a] + [b] = [a + b]$
- $[a] \cdot [b] = [ab]$
- $1_{R/I} = [1_R]$
- $0_{R/I} = [0_R]$

Tak określone działania są poprawne i czynią z R/I pierścień przemienny z 1.

Dowód:

1. Dodawanie w R/I jest dobrze określone, tzn. nie zależy od wyboru reprezentantów klas. Niech $a_1, a_2, b_1, b_2 \in R$, $[a_1] = [a_2]$, $[b_1] = [b_2]$. Chcemy pokazać, że $[a_1 + b_1] = [a_2 + b_2]$, tzn. że $a_1 + b_1 = a_2 + b_2$. Mamy $a_1 + b_1 - (a_2 + b_2) = a_1 - a_2 + b_1 - b_2$, gdzie $a_1 - a_2 \in I$ (bo $a_1 \equiv a_2$) oraz $b_1 - b_2 \in I$ (bo $b_1 \equiv b_2$). Zatem $a_1 + b_1 - (a_2 + b_2) \in I$.
2. Mnożenie w R/I jest dobrze określone. Niech $a_1, a_2, b_1, b_2 \in R$, $[a_1] = [a_2]$, $[b_1] = [b_2]$. Tym razem mamy pokazać, że $[a_1 b_1] = [a_2 b_2]$. Mamy $a_1 b_1 - a_2 b_2 = a_1(b_1 - b_2) + b_2(a_1 - a_2)$. Wiemy, że $b_1 - b_2 \in I$ (bo $b_1 \equiv b_2$) i analogicznie $a_1 - a_2 \in I$. Zatem $a_1(b_1 - b_2) \in I$ oraz $b_2(a_1 - a_2) \in I$. Czyli finalnie $a_1 b_1 - a_2 b_2 \in I$, a co za tym idzie $a_1 b_1 \equiv a_2 b_2$ tzn. $[a_1 b_1] = [a_2 b_2]$.

Stwierdzenie 5.2

Niech $n \in \mathbb{N}$. Moc $\mathbb{Z}/(n)$ (ozn. \mathbb{Z}_n) wynosi n .

Dowód:

Niech $\alpha \in \mathbb{Z}/(n)$, $\alpha = [a]$ dla pewnego $a \in \mathbb{Z}$.

Podzielmy a przez n z resztą ($n \neq 0$): $a = bn + r$, gdzie $b, r \in \mathbb{Z}$, $0 \leq r < n$.

Mamy $[a] = [bn + r] = [bn] + [r] = [0] + [r] = [0 + r] = [r]$ ($bn \in (n)$, więc $[bn] = [0]$).

Zatem $\mathbb{Z}/(n) = \{[0], [1], \dots, [n-1]\}$.

Niech $k, l \in \mathbb{Z}$, $0 \leq k < l \leq n-1$. Jest jasne, że $n \nmid l - k$ tzn. $(l - k) \notin (n)$, więc $l \not\equiv k$, tzn. $[l] \neq [k]$. Ostatecznie $|\mathbb{Z}/(n)| = n$.

Uwaga:

Niech $p \in \mathbb{P}$, $f \in \mathbb{Z}_p[X]$, $\deg(f) = d$, $f \neq 0$. Podobnie pokazujemy, że $|\mathbb{Z}_p[X]/(f)| = p^d$, przy czym $\mathbb{Z}_p[X]/(f) = \{[g] : g \in \mathbb{Z}_p[X], \deg(g) < d\}$, ($[h] = [qf + r] = [r]$, $\deg(r) < \deg(f) = d$, $h \in \mathbb{Z}_p[X]$).

Stwierdzenie 5.3

Niech $n \in \mathbb{N}$, $a \in \mathbb{Z}$. Wtedy $[a] \in \mathbb{Z}_n^* \Leftrightarrow NWD(a, n) = 1$.

Dowód:

” \Rightarrow ”

Przypuśćmy, że $[a] \in \mathbb{Z}_n^*$ tzn. że $[a][b] = 1$ dla pewnego $b \in \mathbb{Z}$.

Zatem $[ab] = 1$ tzn. $ab \equiv 1(n)$ tzn. $n \mid ab - 1$. Niech $d \in \mathbb{N}$, $d \mid a$, $d \mid n$. Wtedy $d \mid 1$ ($d \mid n \mid ab - 1$, $d \mid a \Rightarrow d \mid ab - 1 + ab$). Zatem $NWD(a, n) = 1$.

” \Leftarrow ”

Przypuśćmy, że $NWD(a, n) = 1$. Wtedy $xa + yn = 1$ dla pewnych $x, y \in \mathbb{Z}$.

$[xa + yn] = [1]$

$[x][a] = [1]$, co oznacza, że $[a] \in \mathbb{Z}_n^*$ ($[a]^{-1} = [x]$).

Uwaga:

Podobnie pokazujemy (przykładowo), że jeśli $p \in \mathbb{P}$, $f, g \in \mathbb{Z}_p[X]$, $f \neq 0$, to $[g] \in (\mathbb{Z}_p[X]/(p))^* \Leftrightarrow NWD(g, f) \sim 1$. To kryterium na odwracalność działa w dowolnej DIG.

Dążymy do sformułowania (algebraicznej wersji) chińskiego twierdzenia o resztach (CRT).
Potrzebne nam pojęcie izomorfizmu pierścieni.

Przykład (motywujący):

$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ - ciało

Niech $A_1 = \mathbb{Z}_7[x]/(x^2 - 5)$, $A_2 = \mathbb{Z}_7[x]/(x^2 - 6)$.

Zauważmy, że A_1 i A_2 to ciała (7^2 elementów) co wynika z:

Stwierdzenie 5.4

Niech D będzie DIG, $a \in D$, $a \neq 0$, $a \notin D^*$. Wówczas:

1. Jeśli a jest nierozkładalny, to $D/(a)$ jest ciałem.
2. Jeśli a jest rozkładalny, to $D/(a)$ nie jest dziedziną całkowitości, więc tym bardziej nie jest ciałem.

(przykład i dowód stwierdzenia do dokończenia na kolejnym wykładzie)

Dowód:

1. Załóżmy, że a jest nierozkładalny.

Niech $\beta \in D/(a)$, $\beta = [b]$ (klasa pewnego elementu $b \in D$)

Skoro D jest DIG to $(a, b) = (c)$ dla pewnego $c \in D$.

$c|a$ ponieważ $(a) \subset (a, b) = (c)$ więc $a \in (c)$

Ale a jest nierozkładalny, czyli $c \sim a \vee c \in D^*$

- Przypuśćmy, że $c \in D^*$.

Wtedy $(c) = D$, w szczególności $1 \in (c) = (a, b)$

Stąd $1 = xa + yb$ dla pewnych $x, y \in D$

Mamy $[1] = [x][a] + [y][b]$, $[a] = [0]$ w $D/(a)$

Zatem $[1] = [y][b]$

$[b] = \beta$ jest odwracalne w $D/(a)$

- Załóżmy, że $c \sim a$

Wtedy $(a, b) = (c) = (a)$

Otrzymujemy, że $a|b$ bo $b \in (a, b) = (a)$

to znaczy, że $b = da$ dla pewnego $d \in D$

Stąd $\beta = [b] = [d][a] = [0]$

Pokazaliśmy, że jeśli a jest nierozkładalne to albo β jest odwracalne albo $\beta = [0]$

2. Jeśli a jest rozkładalny czyli $a = a_1 a_2$ gdzie $a_1, a_2 \in D/D^*$

$[0] = [a] = [a_1][a_2]$

Pozostaje zauważyć, że $[a_1], [a_2] \neq [0]$

Przymuśmy, że $[a_1] = [0]$

To oznacza, że $a_1 \equiv 0 \pmod{a}$

$a_1 - 0 = a_1 \in (a)$

Innymi słowy $1|a_1$ czyli $a_1 = da$ dla $d \in D$

$a = a_1 a_2 = daa_2$

Skoro D jest dziedziną to możemy skrócić przez $a \neq 0$

$1 = da_2 \Rightarrow a_2$ jest odwracalny, co prowadzi do sprzeczności: $a_2 \in D^*$

Zatem $[a_1] \neq [0]$

Analogicznie dowodzimy $[a_2] \neq [0]$

6

Z tego stwierdzenia wynika następujący przykład:

Przykład 6.1

Zadanie 1. Pokaż, że pierścienie ilorazowe $A_1 = \mathbb{Z}_7[x]/(x^2 - 5)$ oraz $A_2 = \mathbb{Z}_7[x]/(x^2 - 6)$ są tymi samymi ciałami.

Rozwiązanie Zadania 1.

Z wspomnianego stwierdzenia wiemy, że oba są ciałami. Wiemy też, że mają po 7^2 elementów.

Uzasadnijmy, że są tym samym ciałem z dokładnością do nazwy elementów (bez powoływania się na teorię ciał skończonych).

Przyjrzyjmy się najpierw 7^2 elementowemu ciału $\mathbb{Z}_7[x]/(x^2 - 5)$

Mamy w nim $[x^2 - 5] = [0]$, więc $[x^2] = [5]$

Innymi słowy $[x]$ jest pierwiastkiem kwadratowym z $[5]$ w $\mathbb{Z}_7[x]/(x^2 - 5)$

Zamiast $[5]$ możemy pisać po prostu 5, bo $\mathbb{Z}_7[x]/(x^2 - 5)$ zawiera kopię ciała \mathbb{Z}_7 .

Formalnie: $\mathbb{Z}_7 \ni a \mapsto [a] \in \mathbb{Z}_7[x]/(x^2 - 5)$

W takiej sytuacji piszemy $[x] = \sqrt{5}$

$\mathbb{Z}_7[x]/(x^2 - 5) = \mathbb{Z}_7(\sqrt{5})$ (ciało $\mathbb{Z}_7[x]$ poszerzone o $\sqrt{5}$).

Podobnie $\mathbb{Z}_7[x]/(x^2 - 6) = \mathbb{Z}_7(\sqrt{6})$, $[x] = [6]$

W $\mathbb{Z}_7[x]/(x^2 - 5)$:

$\sqrt{5}$ jest oznaczony $[x]_{x^2-5}$

$\sqrt{6} = 2\sqrt{5}$, bo $(2\sqrt{5})^2 = 6 \pmod{7}$ jest oznaczony $[2x]_{x^2-5}$

W $\mathbb{Z}_7[x]/(x^2 - 6)$:

$\sqrt{6}$ jest oznaczony $[x]_{x^2-6}$

$\sqrt{5} = 4\sqrt{6}$, bo $(4\sqrt{6})^2 = 5 \pmod{7}$ jest oznaczony $[4x]_{x^2-6}$

Innymi słowy $\mathbb{Z}_7[x]/(x^2 - 5)$ i $\mathbb{Z}_7[x]/(x^2 - 6)$ jest tym samym ciałem z dokładnością do nazwania elementów. Działania są takie same (mod 7).

Definicja 6.1

Niech R_1, R_2 będą pierścieniami przemiennymi z 1. Izomorfizmem R_1 na R_2 nazywamy bijekcję $f : R_1 \rightarrow R_2$ taką, że:

$$f(a + b) = f(a) + f(b)$$

$$f(ab) = f(a)f(b)$$

$$f(1_{R_1}) = 1_{R_2}$$

dla dowolnych $a, b \in R_1$

Do otrzymania definicji monomorfizmu, epimorfizmu i homomorfizmu trzeba zamienić w definicji izomorfizmu słowo "bijekcja" na odpowiednio "iniekcja", "surjekcja" i "funkcja".

Pokażemy formalnie, że $\mathbb{Z}_7[x]/(x^2 - 5) \simeq \mathbb{Z}_7[x]/(x^2 - 6)$ (są izomorficzne).
Przydadzą się stwierdzenia:

Stwierdzenie 6.1

Niech R_1, R_2 - pierścienie przemiennie z 1. $f : R_1 \rightarrow R_2$ jest homomorfizmem.

Wówczas: $\ker f = f^{-1}(\{0\}) \triangleleft R_1$ (jest ideałem R_1)

Stwierdzenie 6.2

Homomorfizm f pierścieni przemiennych z 1 jest monomorfizmem wtedy i tylko wtedy gdy $\ker f = \{0\}$

Dowód:

Dla $a \in R_1$: $g([a]) = 0 \Leftrightarrow f(a) = 0 \Leftrightarrow a \in \ker f \Leftrightarrow [a] = [0]$

Stwierdzenie 6.3: Twierdzenie o izomorfizmie

Niech R_1, R_2 - pierścienie przemiennie z 1. $f : R_1 \rightarrow R_2$ jest epimorfizmem.

Wtedy istnieje dokładnie jeden izomorfizm g , taki, że poniższy diagram jest przemienny.

$$\begin{array}{ccc} R_1 & \xrightarrow{f} & R_2 \\ \downarrow \Pi & \nearrow g & \\ R_1/\ker f & & \end{array}$$

gdzie Π to rzutowanie kanoniczne, $\Pi(a) = a + \ker f$

Dowód:

$g : R_1/\ker f \rightarrow R_2$ musi być określone wzorem $g([a]) = f(a)$

(i) g jest dobrze określone: założmy, że $a, b \in R_1, [a] = [b]$.

To oznacza, że $a - b \in \ker f$.

Stąd $f(a - b) = f(0) = 0$.

To znaczy: $f(a) - f(b) = 0, f(a) = f(b)$, czyli:

$g([a]) = g([b])$

(ii) g jest homomorfizmem.

Dla $a, b \in R_1$ mamy $g([a][b]) = g([ab]) = f(ab) = f(a)f(b) = g([a])g([b])$

Podobnie dla dodawania.

Wreszcie $g([1]) = f(1) = 1$

(iii) g jest izomorfizmem.

g jest "na" bo f jest "na".

g jest monomorfizmem bo $\ker g = [0]$.

Pokażemy teraz $\mathbb{Z}_7[x]/(x^2 - 5) \simeq \mathbb{Z}_7[x]/(x^2 - 6)$

Niech $f : \mathbb{Z}_7[x] \mapsto \mathbb{Z}_7[x]/(x^2 - 6)$

$x \mapsto [4x]$, tak by $\ker f = (x^2 - 5)$

f jest homomorfizmem, f jest "na".

Z twierdzenia o izomorfizmie $\mathbb{Z}_7[x]/(x^2 - 6) \simeq \mathbb{Z}_7[x]/\ker f$

Mamy $\ker f = (x^2 - 5)$

$(x^2 - 5) \mapsto [4x]^2 - [5] = [0]$

Niech $w \in \mathbb{Z}_7[x], f(w) = [0]$

$w = (x^2 - 5)Q + R, \text{ def } R < 2$

$[0] = f(w) = f(x^2 - 5)f(Q) + f(R) = [0]f(Q) + f(R) = f(R)$

Czyli: $f(R) = [0]$

Jako, że R jest postaci: $R = ax + b$

$[0] = f(R) = f(ax) + f(b) = [4ax] + [b]$

Stąd: $a = b = 0$

$x^2 - 6 \mid 4ax + b$ oraz $ax + b = 0$