Wstęp do Teorii Liczb

na podstawie wykładu dr. Bartosza Źrałka

Michał Posiadała, Kinga Klaudia Werońska, Filip Nogaj

Data ostatniej aktualizacji: 28 października 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) $\underset{a_1, a_2 \in I}{\forall} a_1 + a_2 \in I$,

(ii) $\underset{k \in \mathbb{Z}, a \in I}{\forall} ka \in I$.

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

Twierdzenie 1.2: Dzielenie z resztą w $\mathbb{Z}$

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

$$a = bq + r, \qquad 0 \leqslant r < |b|.$$

Dowód:
Załóżmy, że $b > 0$ i rozważmy $W = \{bx : x \in \mathbb{Z}, bx \leqslant a\}$ i poczyńmy 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 $\frac{r}{a-bq} \geqslant 0$. 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. $b > \underbrace{a - bq}_{r}$.

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

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

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

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

Pozostaje wykazać jednoznaczność pary (q, r).
Załóżmy, że są dwie takie pary $(q_1, r_1), (q_2, r_2) \in \mathbb{R}^2$ które spełniają

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

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

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 $I \lhd \mathbb{Z}$. 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 $a_1, ..., a_k \in \mathbb{Z}$ zdefiniujmy

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

Jest to najmniejszy (w sensie inkluzji) ideał zawierający $a_1, ..., a_k$. 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) $(b) \subseteq a \iff b \in (a) \iff \underset{c \in \mathbb{Z}}{\exists} b = ac \iff a|b$

(ii)

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

Z czego wynika, że $a = \pm b$.

Definicja 1.4: Największy Wspólny Dzielnik

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

(i) $d|a_1, ..., d|a_k$,

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

Wtedy nazywamy d Największym Wspólnym Dzielnikiem i oznaczamy

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

Twierdzenie 1.5

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

Dowód:

1. Istnienie
   Rozważmy $I = (a_1, ..., a_k)$. 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) $(a_i) \subseteq (a_1, ..., a_k) = (d)$,
   więc z twierdzenia 1.4 $d|a_i$ dla $i = 1, ..., k$

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

2. Jedyność
   Jeśli d_1 i d_2 spełniają definicję NWD, to

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

Wniosek 1.1

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

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

2

Twierdzenie 2.1: istnienie i jedyność NWW liczb całkowitych

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

(i) $a_1|m, ..., a_k|m$,

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

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

Dowód:
Istnienie:
Weźmy m - nieujemny generator ideału $(a_1) \cap ... \cap (a_k)$.

(i) $m \in (a_1) \cap ... \cap (a_k) \subset (a_i)$, więc $a_i|m$ dla $i = 1, ..., k$

(ii) Załóżmy, ż $a_1|m', ..., a_k|m'$. Innymi słowy $m' \in (a_1), ..., m' \in (a_k)$. Zatem $m' \in (a_1) \cap ... \cap (a_k) = (m)$. 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 WZGLĘDNIE 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 $p \in \mathbb{N}, p \geqslant 2$ 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 $p \in \mathbb{P}, a_1, ..., a_k \in \mathbb{Z}, p|a_1 \cdot ... \cdot a_k$. Wtedy $p|a_i$ dla pewnego $i = 1, .., k$.

Dowód:
Indukcja ze względu na k:

1. dla $k = 1$ oczywiste

2. Przypuśćmy, że wniosek zachodzi dla $k \in \mathbb{N}$.
   Niech $p \in \mathbb{P}, a_1, ..., a_{k+1} \in \mathbb{Z}$ oraz $p|a_1 \cdot (a_2 \cdot ... \cdot a_{k+1})$. Z lematu 2.1 $p|a_1$ lub $p|(a_2 \cdot ... \cdot a_{k+1})$. 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 szukanym 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.

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

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

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

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

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

(i) $d|a_1, ..., d|a_k$,

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

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

Twierdzenie 3.3: Najmniejsza Wspólna Wielokrotność w A

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

(i) $a_1|m, ..., a_k|m$,

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

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

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:
Niech γ będzie nierozkładalny w A i niech $a_1, ..., a_k \in A$ takie, że $\gamma|a_1 \cdot ... \cdot a_k$.
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 nierozkładalne.
  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 $p \in P$ rozkłada się w $\mathbb{Z}[i]$.

Uwaga ogólna:
Jeśli $a \in \mathbb{Z}[i], N(a) \in \mathbb{P}$ to a jest nierozkładalne 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 $p\alpha \cdot \beta$, 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 $\alpha\overline{\alpha} = p$, tzn $p = a^2 + b^2$
   Zauważmy, że $a^2 + b^2 \mod 4 \in \{, 1, 2\}$

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

   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 $p|(x^2+1) \iff p|(x-i)(x+i)$ w $\mathbb{Z}[i]$.
Zauważmy, że $NWD(p, x+i) \not\sim 1, p$

- $NWD(p, x+i) \not\sim 1$
  W.p.p z tw. Barcheta mielibyśmy $p|(x-i)$ SPRZECZNOŚĆ
- $NWD(p, x-i) \not\sim p$
  Analogicznie, w.p.p z tw. Barcheta mielibyśmy $p|(x+i)$ SPRZECZNOŚĆ

Napiszemy $NWD(p, x+i) \sim a + bi$.
Skoro $NWD(p, x+i) \not\sim 1$, to $a + ib \notin \mathbb{Z}[i]^*$
Stąd $N(a+ib) > 1$

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

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

  Jeśli $N(a+ib) = p^2$ to $N(\gamma) = 1$, czyli $\gamma \in \mathbb{Z}[i]^*$.
  Mielibyśmy $a + ib \sim p$,przez co $NWD(p, x+i) \not\sim p$.
  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 $a + ib \not\sim a - ib$
  W szczególności $a + ib|a - ib$
  Oczywiście $a + ib|a + ib$
  Stąd $a + ib|a - ib + (a + ib) = 2a$
  Bierzemy normy: $p = N(a+ib)|N(2a) = 4a^2$
  Podobnie $a + ib|(a+ib) - (a-ib) = 2ib, \qquad p|N(2ib) = 4b^2$
  Skoro $p \in \mathbb{P} \setminus \{2\}$ to $p|a \wedge p|b$ to

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

4

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. $p = a^2 + b^2$

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
$$a - a = 0 \in a \implies a \equiv a$$
- symetryczność
$$a \equiv b \iff a - b \in I \iff (-1)(b - a) \in I \iff b \equiv a$$
- przechodniość
$$\left.\begin{matrix} a \equiv b \\ b \equiv c \end{matrix}\right\} \implies \left.\begin{matrix} a - b \in I \\ b - c \in I \end{matrix}\right\} \implies a - b + b - c \in I \implies a - c \in I \iff a \equiv c$$